ESET Internet Security

Používateľská príručka

Pre zobrazenie tohto dokumentu v online verzii kliknite sem

Digital Security
Progress. Protected.

ESET Internet Security bol vyvinutý spoločnosťou ESET, spol. s r. o.

Viac informácií nájdete na webovej stránke www.eset.sk.

Kontaktný formulár: https://www.eset.com/sk/podpora/kontakt/

REV. 12.4.2024

ESET Internet Security

ESET Internet Security predstavuje nový prístup k integrovanej počítačovej bezpečnosti. Najnovšia verzia skenovacieho jadra ESET LiveGrid® spolu s naším vlastným firewallom a antispamovým modulom prináša rýchlu a presnú ochranu pre váš počítač. Výsledkom je inteligentný systém, ktorý je neustále v pohotovosti pred útokmi či škodlivým softvérom predstavujúcim potenciálnu hrozbu pre váš počítač.

ESET Internet Security je komplexné bezpečnostné riešenie a je výsledkom dlhodobého úsilia spojiť maximálnu bezpečnosť s minimálnou záťažou systému. Naše pokročilé technológie založené na umelej inteligencii sú schopné proaktívne eliminovať preniknutie vírusov, spyvéru, trójskych koní, červov, advéru, rootkitov a ďalších hrozieb bez toho, aby brzdili výkon systému alebo spôsobili nefunkčnosť operačného systému počítača.

Vlastnosti a výhody

Prepracované používateľské rozhranie	Používateľské rozhranie v novej verzii bolo značne vylepšené a zjednodušené na základe výsledkov používateľského testovania. Všetky popisy a oznámenia boli dôkladne skontrolované a rozhranie teraz navyše poskytuje podporu pre jazyky písané sprava doľava, ako sú hebrejčina a arabčina. Online pomocník je teraz integrovaný do ESET Internet Security a poskytuje dynamicky aktualizovaný podporný obsah pre používateľov.
Tmavý režim	Rozšírenie, ktoré vám umožní rýchlo prepnúť obrazovku na tmavý motív. Preferovaný farebný motív si môžete vybrať v sekcii Prvky používateľského rozhrania.
Antivírusová a antispyvérová ochrana	Proaktívne deteguje a lieči známe i neznáme vírusy, červy, trójske kone a rootkity. Pokročilá heuristika odhaľuje dokonca aj doteraz neznáme hrozby a neutralizuje ich skôr, než môžu spôsobiť škodu vo vašom počítači. Ochrana prístupu na web a antiphishingová ochrana monitorujú komunikáciu prehliadačov internetových stránok so vzdialenými servermi (vrátane SSL). Ochrana e-mailových klientov zabezpečuje kontrolu e-mailovej komunikácie prijímanej prostredníctvom protokolov POP3(S) a IMAP(S).
Pravidelné aktualizácie	Pravidelné aktualizácie detekčného jadra (v predchádzajúcich verziách pod názvom „vírusová databáza“) a programových modulov sú základným predpokladom na zaistenie maximálnej úrovne zabezpečenia vášho počítača.
ESET LiveGrid® (cloudový reputačný systém)	Používateľ môže overiť reputáciu súborov a spustených procesov priamo v ESET Internet Security.
Správa zariadení	Všetky USB zariadenia, pamäťové karty, CD a DVD sú automaticky skontrolované pri vložení. Je možné blokovať vloženie USB a iných médií na základe typu média, výrobcu, veľkosti média alebo iných vlastností.
HIPS	Táto funkcia umožňuje nastavenie správania systému do posledného detailu: vytvorenie pravidiel pre systémové registre, aktívne procesy a aplikácie vo vašom počítači, ako aj vyladenie zabezpečenia.
Herný režim	Odďaľuje zobrazenie oznamovacích okien, vykonanie aktualizácií alebo iných systémovo náročných aktivít, aby mohli hry alebo iné aplikácie, ktoré sú spustené na celej obrazovke, naplno využiť výkon systému.

Funkcie zahrnuté v ESET Internet Security

Ochrana pri platbách a prehliadaní	Ochrana pri platbách a prehliadaní poskytuje zabezpečený prehliadač používaný na prístup k internetovému bankovníctvu alebo platobným bránam, čím sa zaistí, že všetky online transakcie sa uskutočnia v dôveryhodnom a bezpečnom prostredí.

Podpora pre sieťové podpisy	Sieťové podpisy umožňujú rýchlu identifikáciu a blokovanie škodlivej prichádzajúcej komunikácie z a do zariadenia, ako sú boty a exploit balíčky. Táto funkcia je vylepšením Ochrany pred botnetmi.
Inteligentný Firewall	Zabraňuje prístupu neoprávnených používateľov (hackerov) na váš počítač, aby nemohli zneužiť vaše osobné údaje.
Antispamová ochrana e□mailových klientov	Spam tvorí až 50 % všetkej e-mailovej komunikácie. Antispamová ochrana e□mailových klientov vás pred ním zabezpečí.
Anti-Theft	Anti-Theft je funkcia, ktorá rozširuje bezpečnosť na používateľskej úrovni v prípade straty alebo odcudzenia vášho počítača. Po inštalácii produktu ESET Internet Security a funkcie Anti-Theft bude počítač pridaný na zoznam zariadení používateľa vo webovom rozhraní. Webové rozhranie umožňuje používateľovi spravovať nastavenia služby Anti-Theft, ako aj spravovať funkcie Anti-Theft na zariadení.
Rodičovská kontrola	Chráni vašich blízkych pred potenciálne nevhodným obsahom tak, že blokuje vybrané kategórie internetových stránok.

Na využívanie funkcií ESET Internet Security musíte mať aktívne predplatné. Predplatné ESET Internet Security odporúčame obnoviť niekoľko týždňov pred blížiacim sa koncom jeho platnosti.

Čo je nové?

Aké novinky prináša ESET Internet Security 17.1

- Drobné vylepšenia funkcie Strážca siete
- Drobné vylepšenia funkcie Ochrana pri platbách a prehliadaní
- Ďalšie menšie opravy chýb a vylepšenia

> Ak chcete vypnúť zobrazovanie **oznámení o novinkách**, postupujte nasledovne:
> 1. Kliknite na Rozšírené nastavenia > **Oznámenia** > **Oznámenia na ploche**.
> 2. Kliknite na tlačidlo **Upraviť** vedľa položky **Oznámenia na ploche**.
> 3. Zrušte označenie možnosti **Zobrazovať oznámenia o novinkách** a kliknite na **OK**.
> Viac informácií nájdete v kapitole Oznámenia.

> Podrobný zoznam zmien v programe ESET Internet Security nájdete v protokole zmien pre ESET Internet Security.

Aký produkt mám nainštalovaný?

ESET ponúka s novými produktmi viaceré vrstvy ochrany, od účinného a rýchleho antivírusu až po všestranné bezpečnostné riešenie s minimálnym zaťažením systému:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**
- **ESET Security Ultimate**

Ak chcete zistiť, aký produkt máte nainštalovaný, otvorte hlavné okno programu a v hornej časti uvidíte názov produktu (bližšie informácie nájdete v tomto článku Databázy znalostí).

V tabuľke nižšie nájdete zoznam funkcií, ktoré sú dostupné pre jednotlivé produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekčné jadro	✔	✔	✔	✔
Pokročilé strojové učenie	✔	✔	✔	✔
Exploit Blocker	✔	✔	✔	✔
Ochrana proti skriptovým útokom	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Ochrana prístupu na web	✔	✔	✔	✔
HIPS (vrátane Ransomware Shield)	✔	✔	✔	✔
Antispam		✔	✔	✔
Firewall		✔	✔	✔
Strážca siete		✔	✔	✔
Ochrana webovej kamery		✔	✔	✔
Ochrana pred sieťovými útokmi		✔	✔	✔
Ochrana pred botnetmi		✔	✔	✔
Ochrana pri platbách a prehliadaní		✔	✔	✔
Ochrana súkromia v prehliadači		✔	✔	✔
Rodičovská kontrola		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Niektoré z vyššie uvedených produktov nemusia byť dostupné pre vašu krajinu/jazyk.

Systémové požiadavky

Aby ESET Internet Security pracoval správne, váš systém by mal spĺňať nasledujúce hardvérové a softvérové požiadavky:

Podporované procesory

Procesor Intel alebo AMD, 32-bitový (x86) s inštrukčnou súpravou SSE2 alebo 64-bitový (x64), 1 GHz alebo rýchlejší
Procesor založený na architektúre ARM64, 1 GHz alebo rýchlejší

Podporované operačné systémy

Microsoft® Windows® 11

Microsoft® Windows® 10

Inštalácia či aktualizácia produktov ESET vydaných po júli 2023 vyžaduje na všetkých operačných systémoch Windows podporu služby Azure Code Signing. Viac informácií

Operačný systém pravidelne aktualizujte.

Systémové požiadavky pre funkcie ESET Internet Security

Systémové požiadavky pre konkrétne funkcie ESET Internet Security sú uvedené v tabuľke nižšie:

Funkcia	Požiadavky
Intel® Threat Detection Technology	Pozrite si podporované procesory.
Ochrana pri platbách a prehliadaní	Pozrite si podporované webové prehliadače.
Priehľadné pozadie	Windows 10 vo verzii RS4 a novších.
Specialized Cleaner	Procesor nezalożený na architektúre ARM64.
Čistenie systému	Procesor nezalożený na architektúre ARM64.
Exploit Blocker	Procesor nezalożený na architektúre ARM64.
Hĺbková kontrola správania	Procesor nezalożený na architektúre ARM64.

Ostatné

Aktivácia a aktualizácia programu ESET Internet Security vyžaduje funkčné internetové pripojenie.

Používanie dvoch antivírusových programov súčasne na jednom zariadení nevyhnutne vedie ku konfliktu pri prístupe k systémovým prostriedkom, čo sa prejaví spomalením systému a môže vyústiť až do stavu, keď zariadenie prestane pracovať.

Neaktuálne verzie systému Microsoft Windows

O čo ide

- Chcete nainštalovať najnovšiu verziu produktu ESET Internet Security do počítača so systémom Windows 7, Windows 8 (8.1) alebo Windows Home Server 2011
- ESET Internet Security počas inštalácie zobrazí chybu **Neaktuálny operačný systém**

Podrobnosti

Najnovšia verzia produktu ESET Internet Security vyžaduje operačný systém Windows 10 alebo Windows 11.

Riešenie

Sú dostupné tieto riešenia:

Prechod na Windows 10 alebo Windows 11

Prechod na novšiu verziu je pomerne jednoduchý a väčšinou tak môžete urobiť bez rizika straty súborov. Pred prechodom na Windows 10:

1. Zálohujte dôležité dáta.

2. Prečítajte si článok spoločnosti Microsoft s najčastejšími otázkami týkajúcimi sa prechodu na Windows 10 alebo Windows 11 a aktualizujte svoj operačný systém Windows.

Inštalácia produktu ESET Internet Security 16.0

Ak nemôžete aktualizovať systém Windows, nainštalujte si ESET Internet Security vo verzii 16.0. Viac informácií nájdete v Online pomocníkovi pre ESET Internet Security 16.0.

Prevencia

Pri práci s počítačom, najmä pri prehliadaní internetu, majte na pamäti, že žiadny antivírusový systém na svete nedokáže úplne eliminovať riziko infiltrácií a vzdialených útokov. Na zaistenie maximálnej úrovne ochrany a pohodlia je nevyhnutné správne používať vaše antivírusové riešenie a dodržiavať niekoľko užitočných pravidiel:

Pravidelná aktualizácia

Podľa štatistík zo systému ESET LiveGrid® vznikajú denne tisíce nových unikátnych infiltrácií, ktoré sa snažia obísť existujúce bezpečnostné opatrenia a priniesť svojim tvorcom zisk na úkor ostatných používateľov. Vírusoví analytici spoločnosti ESET denne tieto hrozby analyzujú a vydávajú aktualizácie, ktoré zvyšujú úroveň ochrany používateľov antivírusového systému. Pri nesprávnom nastavení aktualizácie sa účinnosť antivírusového systému dramaticky znižuje. Pre podrobnejšie informácie o nastavení aktualizácie kliknite na nasledujúci odkaz: Nastavenie aktualizácie.

Sťahovanie bezpečnostných záplat

Tvorcovia malvéru s obľubou využívajú bezpečnostné zraniteľnosti a chyby v často používaných programoch, aby zvýšili účinnosť šírenia škodlivého kódu. Z toho dôvodu softvérové spoločnosti kladú dôraz na vyhľadávanie bezpečnostných zraniteľností vo svojich programoch a pravidelne vydávajú bezpečnostné záplaty, ktorými dané chyby opravujú a znižujú potenciálne riziko hrozby. Je dôležité tieto záplaty pravidelne inštalovať. Medzi takéto programy môžeme zaradiť napríklad operačný systém Microsoft Windows alebo internetový prehliadač Internet Explorer.

zálohujte dôležité dáta,

Tvorcovia malvéru väčšinou neberú ohľad na potreby používateľov a nimi vytvorené programy môžu často spôsobiť úplnú nefunkčnosť operačného systému alebo stratu či poškodenie dát. Preto je kľúčové pravidelne zálohovať citlivé a dôležité dáta na externé úložisko, napríklad na DVD alebo externý pevný disk. Záloha vám výrazne uľahčí a urýchli obnovu systému po útoku do pôvodného stavu.

Pravidelná kontrola počítača

Detekcia známych či menej známych vírusov, červov, trójskych koní a rootkitov je zabezpečená pomocou Rezidentnej ochrany súborového systému. To znamená, že pri každom prístupe alebo otvorení súboru prebehne kontrola na prítomnosť malvéru. Napriek tomu odporúčame, aby ste spustili kontrolu počítača aspoň raz mesačne, pretože malvér je rôzny, dynamický a detekčné jadro sa aktualizuje každý deň.

Dodržiavanie základných bezpečnostných pravidiel

Jedným z najužitočnejších a najúčinnejších bezpečnostných opatrení je obozretnosť používateľa. V súčasnosti mnoho infiltrácií vyžaduje priame spustenie a šírenie používateľom. Preto je veľmi dôležitá opatrnosť pri otváraní súborov. Ušetríte si tak mnoho problémov a čas strávený snahou o odstránenie infiltrácie z počítača. Medzi užitočné rady by sme mohli zahrnúť:

- Obmedziť návštevy podozrivých stránok, ktoré používateľa bombardujú otváraním okien s reklamnými ponukami a pod.
- Opatrnosť pri sťahovaní a inštalovaní voľne šíriteľných programov, kodekov atď. Používať iba overené programy a navštevovať len bezpečné internetové stránky.
- Opatrnosť pri otváraní príloh e□mailov, obzvlášť pri masovo posielaných e□mailoch alebo pri e□mailoch od neznámych odosielateľov.
- Nepoužívať na bežnú prácu s počítačom účet správcu.

Pomocník k programu

Vitajte v používateľskej príručke pre produkt ESET Internet Security. Veríme, že informácie obsiahnuté v tejto príručke vám pomôžu pri práci s vaším produktom a urobia váš počítač bezpečnejším.

Ako začať

Skôr ako začnete používať ESET Internet Security, oboznámte sa s rôznymi typmi infiltrácií a vzdialenými útokmi, s ktorými sa môžete pri práci s počítačom stretnúť. Vypracovali sme tiež zoznam nových funkcií produktu ESET Internet Security.

Začnite inštaláciou produktu ESET Internet Security. Ak už máte produkt ESET Internet Security nainštalovaný, prečítajte si kapitolu Práca s ESET Internet Security.

Ako používať Pomocníka programu ESET Internet Security

Online pomocník je rozdelený na niekoľko kapitol a podkapitol. Stlačením klávesu **F1** v programe ESET Internet Security zobrazíte informácie týkajúce sa aktuálne otvoreného okna.

Online pomocník vám umožňuje vyhľadávať kapitoly pomocníka podľa kľúčových slov alebo vyhľadávať obsah podľa slov a fráz. Rozdiel medzi týmito dvomi typmi vyhľadávania je ten, že kľúčové slová sa viažu k stránkam pomocníka logicky, pričom samotné kľúčové slovo sa v texte vôbec nemusí vyskytovať. Vyhľadávanie pomocou jednotlivých slov a slovných spojení vám vyhľadá všetky stránky pomocníka, kde sa hľadané slová alebo frázy nachádzajú priamo v texte.

Na zachovanie konzistencie a zabránenie zámene je terminológia použitá v tejto príručke založená na používateľskom rozhraní produktu ESET Internet Security. Používame tiež jednotnú súpravu symbolov na zvýraznenie kapitol, ktoré sú zvlášť dôležité alebo sú iným spôsobom významné.

Poznámka je len krátky postreh. Hoci poznámkam nemusí byť venovaná zvláštna pozornosť, môžu obsahovať cenné informácie, ako napr. špecifické funkcie alebo odkaz na súvisiacu kapitolu.

Tieto informácie si vyžadujú vašu pozornosť a neodporúča sa ich ignorovať. Zvyčajne nejde o mimoriadne závažné informácie, sú však podstatné.

Ide o informáciu, ktorá vyžaduje zvýšenú pozornosť a opatrnosť. Upozornenia sú umiestnené tak, aby vás včas varovali a zároveň vám pomohli predísť chybám, ktoré by mohli mať negatívne následky. Tieto informácie si dôkladne prečítajte, pretože sa týkajú mimoriadne citlivých systémových nastavení alebo upozorňujú na riziká.

Toto je prípad použitia alebo praktický príklad, ktorého cieľom je pomôcť vám lepšie porozumieť, ako využiť konkrétnu funkciu.

Konvencia	Význam
Tučné písmo	Pomenúva položky rozhrania, ako napr. polia a tlačidlá možností.
Kurzíva	Zástupné symboly pre údaje, ktoré máte poskytnúť. Napríklad filename alebo path znamená, že máte zadať konkrétnu cestu alebo názov súboru.
`Courier New`	Príklady kódov alebo príkazov.
Hypertextové prepojenie	Poskytuje rýchly a jednoduchý prístup k súvisiacim prepojeným kapitolám alebo externým webovým lokalitám. Hypertextové prepojenia sú zvýraznené modrou farbou a môžu byť podčiarknuté.
%ProgramFiles%	Systémový adresár Windows, kde sú uložené programy inštalované na operačnom systéme Windows.

Online pomocník je hlavným zdrojom pomocného obsahu. Pri pripojení na internet sa automaticky zobrazuje vždy najnovšia verzia Online pomocníka.

Inštalácia

Existuje niekoľko spôsobov, ako nainštalovať ESET Internet Security na počítač. Dostupnosť nižšie uvedených spôsobov inštalácie sa môže líšiť v závislosti od krajiny a spôsobu distribúcie inštalačného súboru:

- Live inštalátor – Live inštalátor si môžete stiahnuť z webovej stránky spoločnosti ESET alebo z CD/DVD. Tento inštalačný balík je univerzálny pre všetky jazyky (používateľ si môže zvoliť preferovaný jazyk). Zaberá málo miesta na disku a všetky potrebné súbory na inštaláciu programu ESET Internet Security sa stiahnu automaticky z internetu.

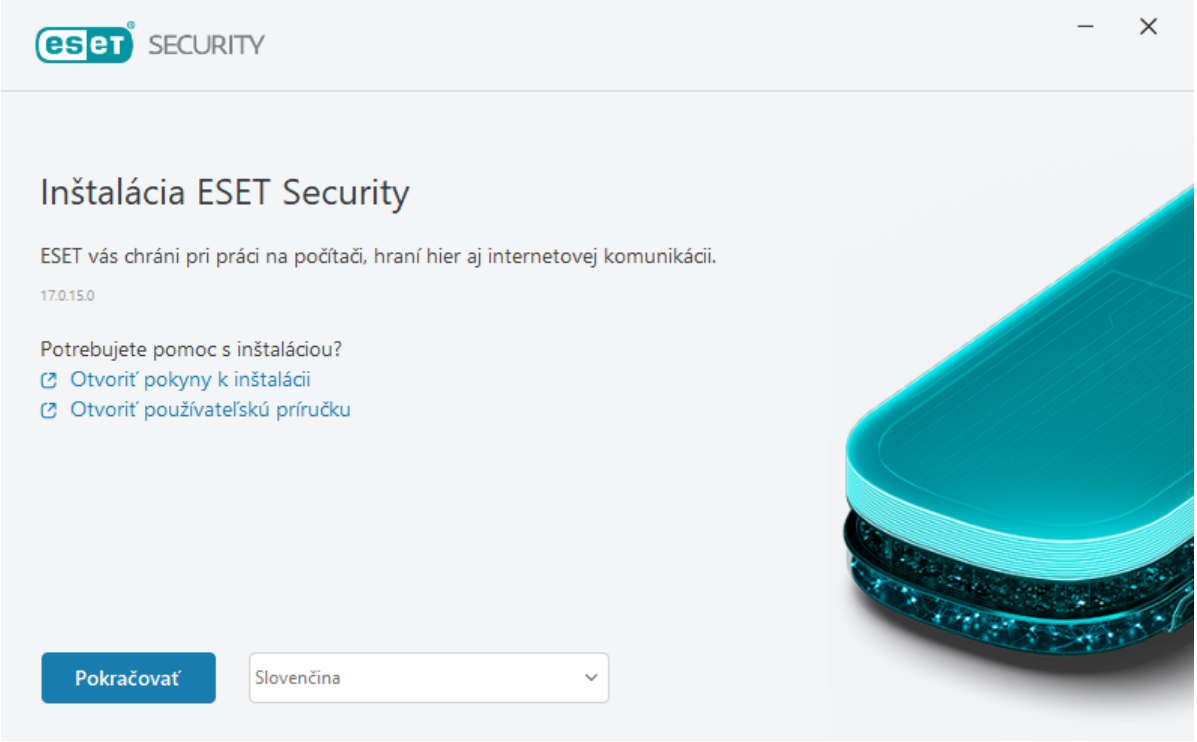
- Offline inštalácia – tento typ inštalácie sa vykonáva pomocou inštalačného súboru .exe, ktorý je väčší ako súbor Live inštalátora. Inštalácia si nevyžaduje internetové pripojenie a nie je potrebné sťahovať ďalšie súbory.

Predtým, ako začnete inštalovať ESET Internet Security sa uistite, že nemáte nainštalovaný antivírusový program od inej spoločnosti. Medzi dvoma antivírusovými programami môže dochádzať ku konfliktu. Odporúčame preto odinštalovať akýkoľvek iný antivírusový program zo systému. Viac informácií o odinštalovaní antivírusových programov nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Live inštalátor

Po stiahnutí inštalačného balíka Live inštalátora dvakrát kliknite na inštalačný súbor a postupujte podľa inštrukcií uvedených v sprievodcovi inštalácie.

Tento typ inštalácie je možné vykonať iba v prípade, ak ste pripojený na internet.



1. Z roletového menu vyberte preferovaný jazyk produktu a kliknite na **Pokračovať**.

Ak inštalujete novú verziu produktu cez staršiu verziu s nastaveniami chránenými heslom, zadajte príslušné heslo. Heslo na ochranu nastavení môžete nakonfigurovať v časti Nastavenia prístupu.

2. Zvoľte, ktoré z nasledujúcich funkcií chcete povoliť, prečítajte si Licenčnú dohodu s koncovým používateľom a Zásady ochrany osobných údajov a kliknite na **Pokračovať**. Kliknutím na **Povoliť všetko a pokračovať** môžete povoliť všetky funkcie:

- Systém spätnej väzby ESET LiveGrid®
- Potenciálne nechcené aplikácie
- Program zvyšovania spokojnosti zákazníkov

Kliknutím na **Pokračovať** alebo **Povoliť všetko a pokračovať** vyjadrujete súhlas s Licenčnou dohodou s koncovým používateľom a beriete na vedomie Zásady ochrany osobných údajov.

3. Pripojte svoje zariadenie k účtu ESET HOME, aby ste mohli aktivovať, spravovať a sledovať jeho zabezpečenie prostredníctvom portálu ESET HOME. Ak chcete pokračovať bez pripojenia zariadenia k účtu ESET HOME, kliknite na tlačidlo **Preskočiť prihlásenie**. Zariadenie môžete pripojiť k svojmu účtu ESET HOME aj neskôr.

4. Ak budete pokračovať bez pripojenia k účtu ESET HOME, vyberte si možnosť aktivácie. Ak inštalujete novú verziu produktu cez staršiu verziu nainštalovanú na vašom počítači, váš **aktivačný kľúč** bude vyplnený automaticky.

5. Sprievodca inštaláciou zvolí bezpečnostný produkt ESET na základe vášho predplatného. Predvolene ponúkne produktovú verziu, ktorá obsahuje najviac funkcií. Kliknutím na **Zmeniť produkt** si môžete vybrať a nainštalovať iný produkt. Kliknutím na tlačidlo **Pokračovať** spustite inštaláciu. Tento proces môže chvíľu trvať.

Ak zostali z minulých inštalácií produktov ESET na počítači po odinštalovaní nejaké zostávajúce súbory alebo priečinky, budete vyzvaný k tomu, aby ste povolili ich odstránenie. Pokračujte kliknutím na tlačidlo **Inštalovať**.

6. Kliknite na tlačidlo **Dokončiť** pre ukončenie sprievodcu inštaláciou.

Riešenie problémov pri inštalácii.

Po dokončení inštalácie a aktivácie produktu sa začne sťahovanie potrebných programových modulov. Prebieha inicializácia ochrany a niektoré funkcie ešte nemusia byť plne funkčné, pokým sa nedokončí sťahovanie modulov.

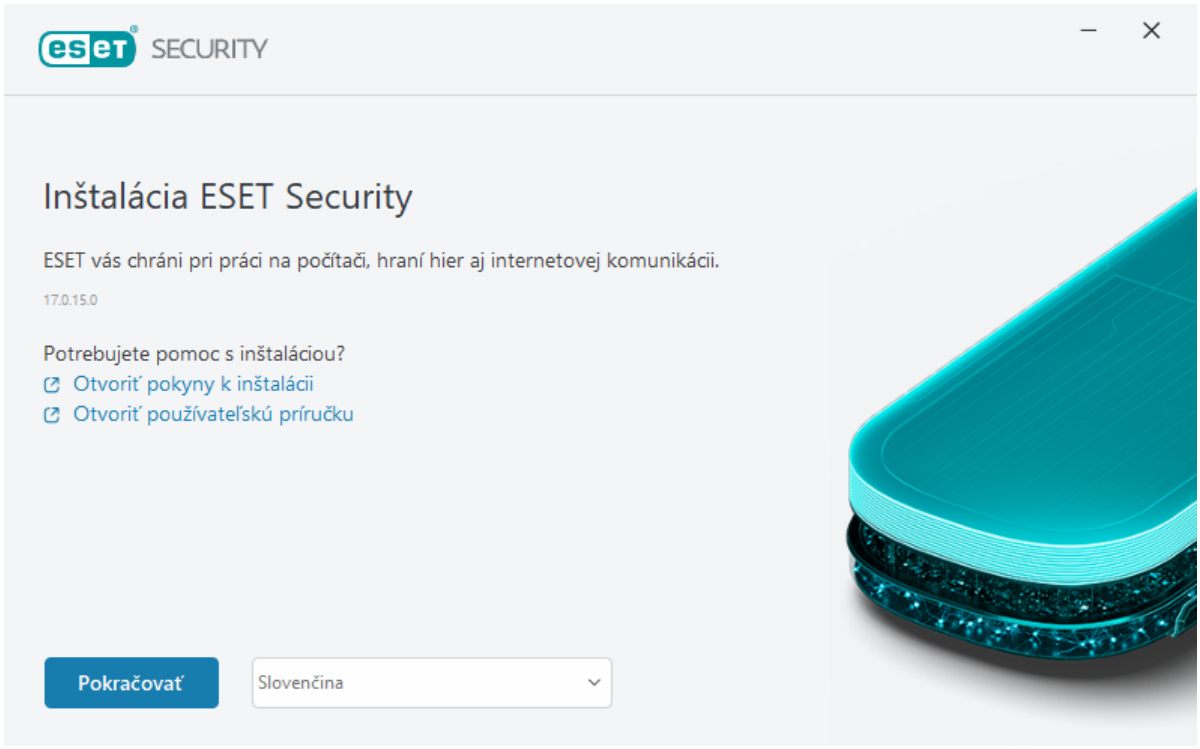
Offline inštalácia

Stiahnite si príslušný offline inštalátor (.exe) nižšie a nainštalujte si svoj bezpečnostný produkt ESET určený pre domácnosti s OS Windows. Vyberte, ktorú verziu produktu ESET pre domácnosti chcete stiahnuť (32-bitová, 64-bitová verzia alebo verzia pre zariadenia s procesorom ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Stiahnuť 64-bitovú verziu Stiahnuť 32-bitovú verziu Stiahnuť verziu ARM	Stiahnuť 64-bitovú verziu Stiahnuť 32-bitovú verziu Stiahnuť verziu ARM	Stiahnuť 64-bitovú verziu Stiahnuť 32-bitovú verziu Stiahnuť verziu ARM	Stiahnuť 64-bitovú verziu Stiahnuť 32-bitovú verziu Stiahnuť verziu ARM

Ak máte aktívne pripojenie na internet, nainštalujte si produkt ESET použitím Live inštalátora.

Po spustení offline inštalátora (.exe) vás sprievodca prevedie celým inštalačným procesom.



1. Z roletového menu vyberte preferovaný jazyk produktu a kliknite na **Pokračovať**.

Ak inštalujete novú verziu produktu cez staršiu verziu s nastaveniami chránenými heslom, zadajte príslušné heslo. Heslo na ochranu nastavení môžete nakonfigurovať v časti Nastavenia prístupu.

2. Zvoľte, ktoré z nasledujúcich funkcií chcete povoliť, prečítajte si Licenčnú dohodu s koncovým používateľom a Zásady ochrany osobných údajov a kliknite na **Pokračovať**. Kliknutím na **Povoliť všetko a pokračovať** môžete povoliť všetky funkcie:

- Systém spätnej väzby ESET LiveGrid®
- Potenciálne nechcené aplikácie
- Program zvyšovania spokojnosti zákazníkov

Kliknutím na **Pokračovať** alebo **Povoliť všetko a pokračovať** vyjadrujete súhlas s Licenčnou dohodou s koncovým používateľom a beriete na vedomie Zásady ochrany osobných údajov.

3. Kliknite na **Preskočiť prihlásenie**. Po pripojení na internet môžete zariadenie pripojiť k svojmu účtu ESET HOME.

4. Kliknite na **Preskočiť aktiváciu**. ESET Internet Security je potrebné po inštalácii dodatočne aktivovať, aby mohol byť plne funkčný. Aktivácia produktu si vyžaduje pripojenie na internet.

5. Sprievodca inštaláciou na základe stiahnutého offline inštalátora určí a zobrazí produkt ESET, ktorý bude nainštalovaný. Kliknutím na tlačidlo **Pokračovať** spustite inštaláciu. Tento proces môže chvíľu trvať.

Ak zostali z minulých inštalácií produktov ESET na počítači po odinštalovaní nejaké zostávajúce súbory alebo priečinky, budete vyzvaný k tomu, aby ste povolili ich odstránenie. Pokračujte kliknutím na tlačidlo **Inštalovať**.

6. Kliknite na tlačidlo **Dokončiť** pre ukončenie sprievodcu inštaláciou.

Riešenie problémov pri inštalácii.

Navýšenie úrovne predplatného

Toto oznámenie sa zobrazí, ak bolo predplatné, ktorým je aktivovaný váš produkt ESET, zmenené. Vaše zmenené predplatné vám umožňuje aktivovať produkt s väčším rozsahom bezpečnostných funkcií. Ak nebola vykonaná žiadna zmena, ESET Internet Security zobrazí okno s oznámením **Zmena na produkt s väčším počtom funkcií** s možnosťou zmeny na vyšší produktový rad.

Áno (odporúčané) – automaticky sa nainštaluje produkt s väčším rozsahom bezpečnostných funkcií.

Nie, ďakujem – nebudú vykonané žiadne zmeny a upozornenie sa viac nebude zobrazovať.

Ak chcete produkt zmeniť neskôr, prečítajte si náš článok Databázy znalostí spoločnosti ESET. Viac informácií o predplatnom ESET nájdete v našom článku s častými otázkami.

V tabuľke nižšie nájdete zoznam funkcií, ktoré sú dostupné pre jednotlivé produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekčné jadro	✔	✔	✔	✔
Pokročilé strojové učenie	✔	✔	✔	✔
Exploit Blocker	✔	✔	✔	✔
Ochrana proti skriptovým útokom	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Ochrana prístupu na web	✔	✔	✔	✔
HIPS (vrátane Ransomware Shield)	✔	✔	✔	✔
Antispam		✔	✔	✔
Firewall		✔	✔	✔
Strážca siete		✔	✔	✔
Ochrana webovej kamery		✔	✔	✔
Ochrana pred sieťovými útokmi		✔	✔	✔
Ochrana pred botnetmi		✔	✔	✔
Ochrana pri platbách a prehliadaní		✔	✔	✔
Ochrana súkromia v prehliadači		✔	✔	✔
Rodičovská kontrola		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Zmena na vyšší produktový rad

Stiahli ste si predvolený inštalátor a rozhodli ste sa zmeniť produkt, ktorý chcete aktivovať, alebo si želáte zmeniť váš nainštalovaný produkt na produkt s väčším rozsahom bezpečnostných funkcií.

Zmena produktu počas inštalácie.

V tabuľke nižšie nájdete zoznam funkcií, ktoré sú dostupné pre jednotlivé produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekčné jadro	✔	✔	✔	✔
Pokročilé strojové učenie	✔	✔	✔	✔
Exploit Blocker	✔	✔	✔	✔
Ochrana proti skriptovým útokom	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Ochrana prístupu na web	✔	✔	✔	✔
HIPS (vrátane Ransomware Shield)	✔	✔	✔	✔
Antispam		✔	✔	✔
Firewall		✔	✔	✔
Strážca siete		✔	✔	✔
Ochrana webovej kamery		✔	✔	✔
Ochrana pred sieťovými útokmi		✔	✔	✔
Ochrana pred botnetmi		✔	✔	✔
Ochrana pri platbách a prehliadaní		✔	✔	✔
Ochrana súkromia v prehliadači		✔	✔	✔
Rodičovská kontrola		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Zníženie úrovne predplatného

Toto dialógové okno sa zobrazí, ak bolo predplatné, ktorým je aktivovaný váš produkt ESET, zmenené. Vaše zmenené predplatné je možné používať len s iným produktom ESET, ktorý má menej bezpečnostných funkcií. Používaný produkt bol automaticky zmenený, aby sa predišlo strate ochrany.

Viac informácií o predplatnom ESET nájdete v našom článku s častými otázkami.

V tabuľke nižšie nájdete zoznam funkcií, ktoré sú dostupné pre jednotlivé produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekčné jadro	✔	✔	✔	✔
Pokročilé strojové učenie	✔	✔	✔	✔
Exploit Blocker	✔	✔	✔	✔
Ochrana proti skriptovým útokom	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Ochrana prístupu na web	✔	✔	✔	✔
HIPS (vrátane Ransomware Shield)	✔	✔	✔	✔
Antispam		✔	✔	✔
Firewall		✔	✔	✔
Strážca siete		✔	✔	✔
Ochrana webovej kamery		✔	✔	✔
Ochrana pred sieťovými útokmi		✔	✔	✔
Ochrana pred botnetmi		✔	✔	✔
Ochrana pri platbách a prehliadaní		✔	✔	✔
Ochrana súkromia v prehliadači		✔	✔	✔
Rodičovská kontrola		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Zmena na nižší produktový rad

Váš nainštalovaný produkt obsahuje viac bezpečnostných funkcií ako ten, ktorý sa chystáte aktivovať. Prídete tak o ochranu pri krádeži a o prístup k súvisiacim dátam uloženým na portáli ESET HOME.

V tabuľke nižšie nájdete zoznam funkcií, ktoré sú dostupné pre jednotlivé produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekčné jadro	✔	✔	✔	✔
Pokročilé strojové učenie	✔	✔	✔	✔
Exploit Blocker	✔	✔	✔	✔
Ochrana proti skriptovým útokom	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Ochrana prístupu na web	✔	✔	✔	✔
HIPS (vrátane Ransomware Shield)	✔	✔	✔	✔
Antispam		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Firewall		✔	✔	✔
Strážca siete		✔	✔	✔
Ochrana webovej kamery		✔	✔	✔
Ochrana pred sieťovými útokmi		✔	✔	✔
Ochrana pred botnetmi		✔	✔	✔
Ochrana pri platbách a prehliadaní		✔	✔	✔
Ochrana súkromia v prehliadači		✔	✔	✔
Rodičovská kontrola		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Riešenie problémov pri inštalácii

Ak sa počas inštalácie vyskytnú problémy, sprievodca inštaláciou ponúkne nástroj, ktorý sa pokúsi nájsť riešenie problému.

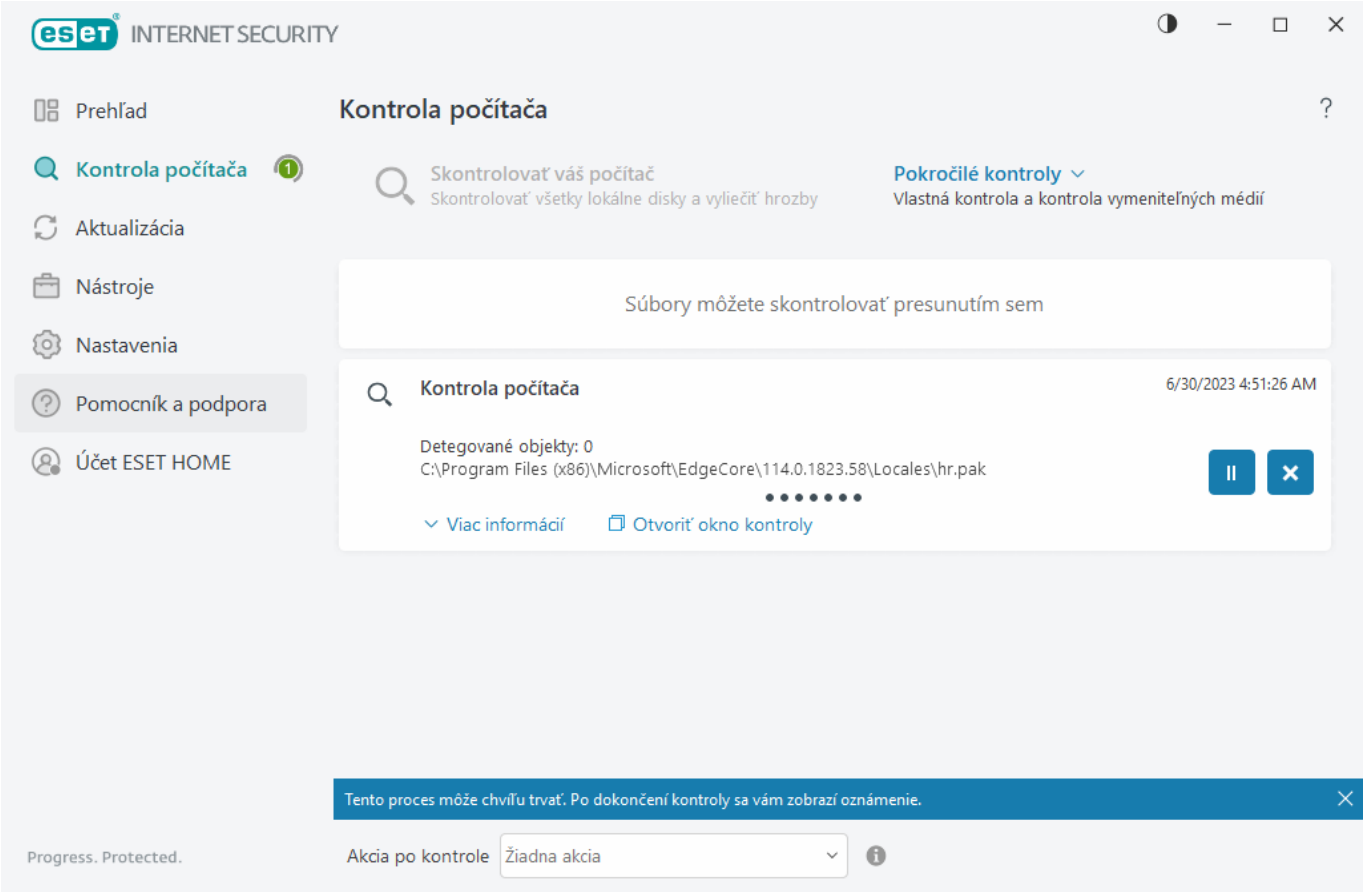
Po kliknutí na možnosť **Spustiť riešenie problémov** sa začne proces vyhľadania problému. Po jeho skončení sa zobrazí odporúčané riešenie, podľa ktorého je potrebné postupovať.

Ak problém pretrváva aj naďalej, pozrite si zoznam najbežnejších chýb pri inštalácii produktov ESET spolu s ich riešeniami.

Prvá kontrola po inštalácii

Keď po inštalácii produktu ESET Internet Security po prvýkrát prebehne aktualizácia, automaticky sa spustí kontrola počítača na prítomnosť malvéru.

Kontrolu počítača môžete spustiť aj manuálne z hlavného okna programu, a to kliknutím na **Kontrola počítača** > **Skontrolovať váš počítač**. Podrobnejšie informácie o kontrolách počítača nájdete v kapitole Kontrola počítača.



Prechod na novšiu verziu

Nové verzie ESET Internet Security sú vydávané kvôli zabudovaným vylepšeniam produktu a opravám chýb, ktoré nie je možné opraviť v rámci automatickej aktualizácie programových modulov. Je niekoľko spôsobov, ako prejsť na novšiu verziu produktu:

1. Automaticky prostredníctvom aktualizácie programu.
Keďže aktualizácia programu je posielaná všetkým používateľom daného produktu a môže mať významný dopad na konfiguráciu systému, je uvoľnená až po dlhom období testovania v rôznych konfiguráciách, aby sa zaistila úplná funkčnosť pre všetky možné systémové konfigurácie. Ak potrebujete prejsť na novšiu verziu hneď po jej vydaní, použite niektorú z nasledujúcich dvoch metód.
Uistite sa, že ste povolili **Aktualizácie programových funkcií** v sekcii Rozšírené nastavenia > **Aktualizácia** > **Profily** > **Aktualizácie**.

2. Manuálne, v hlavnom okne programu kliknite na **Overiť dostupnosť aktualizácií** v sekcii **Aktualizácia**.

3. Manuálne, stiahnutím a nainštalovaním novej verzie cez starú verziu programu pomocou inštalátora.

Dodatočné informácie a ilustrované inštrukcie nájdete na nasledujúcich odkazoch:

- Aktualizácia produktu ESET – overenie dostupnosti aktualizácií programových modulov
- Aké rozličné typy aktualizácií a vydaní produktov ESET existujú?

Automatická aktualizácia staršieho produktu

Vaša verzia produktu ESET už nie je podporovaná a váš produkt bol aktualizovaný na najnovšiu verziu.

Časté problémy inštalácie

Každá nová verzia produktov ESET obsahuje mnoho opráv chýb a vylepšení. Existujúci zákazníci s platným predplatným na produkt ESET môžu prejsť na najnovšiu verziu toho istého produktu zadarmo.

Na dokončenie inštalácie postupujte podľa nasledujúcich krokov:

1. Kliknite na **Prijať a pokračovať**, čím odsúhlasíte Licenčnú dohodu s koncovým používateľom a Zásady ochrany osobných údajov. Ak nesúhlasíte s Licenčnou dohodou s koncovým používateľom, kliknite na **Odinštalovať**. Nie je možné vrátiť sa k predchádzajúcej verzii.

2. Kliknite na **Povoliť všetko a pokračovať**, ak chcete povoliť Systém spätnej väzby ESET LiveGrid® aj Program zvyšovania spokojnosti zákazníkov. Ak sa programu nechcete zúčastniť, kliknite na **Pokračovať**.

3. Po aktivácii nového produktu ESET pomocou aktivačného kľúča sa zobrazí okno Prehľad. Ak sa nepodarí nájsť informácie o predplatnom, pokračujte využitím bezplatného skúšobného obdobia. Ak vaše predplatné používané v predchádzajúcom produkte nie je platné, prejdite k aktivácii produktu ESET.

4. Na dokončenie inštalácie sa vyžaduje reštart počítača.

ESET Internet Security bude nainštalovaný

Toto dialógové okno sa môže zobraziť:

- Počas inštalácie – kliknite na možnosť **Pokračovať** pre inštaláciu produktu ESET Internet Security.

- Pri zmene predplatného v rámci ESET Internet Security – kliknite na možnosť **Aktivovať** pre zmenu predplatného a aktiváciu produktu ESET Internet Security.

V závislosti od vášho predplatného si cez možnosť **Zmeniť produkt** môžete zvoliť aj iný produkt ESET určený pre domácnosti s OS Windows, ktorý vám predplatné povoľuje nainštalovať. Zoznam funkcií jednotlivých produktov nájdete v tejto kapitole.

Zmeniť na iný produktový rad

V závislosti od vášho predplatného si môžete zvoliť aj iný produkt ESET určený pre domácnosti s OS Windows, ktorý vám predplatné povoľuje nainštalovať. Zoznam funkcií jednotlivých produktov nájdete v tejto kapitole.

Registrácia

Zaregistrujte svoje predplatné zadaním príslušných údajov do registračného formulára a kliknutím na **Aktivovať**. Uistite sa, že ste vyplnili všetky polia označené ako povinné. Tieto informácie budú použité iba v súvislosti s vaším predplatným ESET.

Priebeh aktivácie

Aktivácia môže trvať niekoľko sekúnd (v závislosti od rýchlosti vášho internetového pripojenia alebo počítača).

Úspešná aktivácia

Proces aktivácie je dokončený. Na dokončenie nastavenia produktu ESET Internet Security postupujte podľa sprievodcu nastavením.

V priebehu niekoľkých sekúnd sa spustí aktualizácia modulov. Okamžite sa začnú pravidelné aktualizácie programu ESET Internet Security.

Prvá kontrola sa spustí automaticky do 20 minút po aktualizácii modulov.

Ak produkt nie je prepojený s účtom ESET HOME, môže dôjsť k prerušeniu aktivačného procesu. Prihláste sa do svojho účtu ESET HOME alebo si vytvorte nový účet.

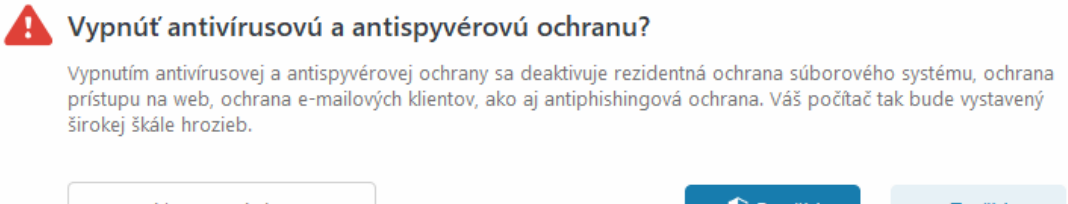
Ako začať

Táto kapitola poskytuje prvotný pohľad na ESET Internet Security a jeho základné nastavenia.

Ikona na paneli úloh

Niektoré dôležité nastavenia a funkcie sú dostupné v menu, ktoré sa zobrazí po kliknutí pravým tlačidlom na ikonu programu na paneli úloh (oblasť oznámení systému Windows).

Pozastaviť ochranu – zobrazí sa potvrdzovacie dialógové okno, pomocou ktorého vypnete detekčné jadro, ktoré chráni systém pred škodlivými útokmi tým, že kontroluje súbory, e-maily a internetovú komunikáciu. V roletovom menu **Časový interval** môžete nastaviť, ako dlho má byť ochrana vypnutá.



Pozastaviť firewall (povoliť všetku komunikáciu) – firewall sa prepne do neaktívneho režimu. Viac informácií nájdete v časti Sieť.

Blokovať všetku sieťovú komunikáciu – pomocou tejto možnosti môžete zablokovať všetku sieťovú komunikáciu. Obnoviť sieťovú komunikáciu môžete kliknutím na možnosť **Zastaviť blokovanie všetkej sieťovej komunikácie**.

Rozšírené nastavenia – otvorí sa okno s rozšírenými nastaveniami ESET Internet Security. Ak chcete rozšírené

nastavenia otvoriť z hlavného okna programu, stlačte F5 na klávesnici alebo kliknite na **Nastavenia** > **Rozšírené nastavenia**.

Protokoly – obsahujú informácie o dôležitých udalostiach v programe a poskytujú prehľad všetkých detekcií.

Otvoriť ESET Internet Security – otvorí sa hlavné okno programu ESET Internet Security.

Obnoviť rozmiestnenie okien – obnoví prednastavenú veľkosť a umiestnenie okna ESET Internet Security na obrazovke.

Farebný režim – otvoria sa nastavenia používateľského rozhrania, kde môžete zmeniť farbu grafického rozhrania.

Overiť dostupnosť aktualizácií – spustí sa aktualizácia modulu alebo produktu, ktorá zaistí vašu nepretržitú ochranu. ESET Internet Security kontroluje dostupnosť aktualizácií automaticky niekoľkokrát denne.

O programe – poskytuje informácie o systéme, podrobnosti o nainštalovanej verzii programu ESET Internet Security a nainštalovaných programových moduloch, ako aj informácie o operačnom systéme a systémových prostriedkoch.

Klávesové skratky

Pre rýchlejšiu navigáciu v programe ESET Internet Security je možné použiť aj nasledujúce klávesové skratky:

Klávesové skratky	Akcia
F1	otvorenie pomocníka
F5	otvorenie rozšírených nastavení
Šípka hore/šípka dole	navigácia v položkách roletového menu
TAB	presun na ďalší prvok grafického rozhrania v okne
Shift+TAB	presun na predchádzajúci prvok grafického rozhrania v okne
ESC	zatvorenie aktívneho dialógového okna
Ctrl+U	zobrazenie informácie o predplatnom ESET a vašom počítači (podrobnosti pre technickú podporu)
Ctrl+R	obnovenie prednastavenej veľkosti a umiestnenia okna programu na obrazovke
ALT + šípka doľava	prechod späť
ALT + šípka doprava	prechod vpred
ALT+Home	prechod na domovskú stránku

Môžete tiež použiť tlačidlá myši na navigáciu dozadu alebo dopredu.

Profily

Manažér profilov sa v ESET Internet Security používa na dvoch miestach – v sekcii **Manuálna kontrola** a v sekcii **Aktualizácia**.

Kontrola počítača

ESET Internet Security ponúka 4 prednastavené profily kontroly:

- **Smart kontrola** – toto je predvolený profil pokročilej kontroly. Profil Smart kontroly využíva technológiu Smart optimalizácie na vylúčenie súborov, ktoré boli počas predchádzajúcej kontroly vyhodnotené ako neškodné a odvtedy neboli zmenené. Vďaka tomu je čas kontroly kratší, pričom vplyv na bezpečnosť systému je minimálny.

- **Kontrola z kontextového menu** – kontrolu ľubovoľného súboru môžete spustiť manuálne z kontextového menu. Profil Kontroly z kontextového menu umožňuje nastaviť konfiguráciu kontroly, ktorá bude použitá pri spustení kontroly.

- **Hĺbková kontrola** – profil Hĺbkovej kontroly štandardne nevyužíva Smart optimalizáciu, čo znamená, že ak použijete tento profil, z kontroly nebudú vylúčené žiadne súbory.

- **Kontrola počítača** – toto je predvolený profil použitý pri štandardnej kontrole počítača.

Preferované nastavenia kontroly je možné uložiť do profilov pre budúce použitie. Odporúčame vám, aby ste vždy vytvorili nový profil (s rôznymi cieľmi kontroly, metódami kontroly a ďalšími parametrami) pre každú pravidelne používanú kontrolu.

Na vytvorenie nového profilu otvorte Rozšírené nastavenia > **Detekčné jadro** > **Detekcia malvéru** > **Manuálna kontrola** > **Zoznam profilov** > **Upraviť**. Otvorí sa okno **Manažér profilov**, v ktorom sa nachádza roletové menu **Aktívny profil** obsahujúce zoznam existujúcich profilov kontroly, ako aj možnosť vytvoriť nový profil kontroly. Pre objasnenie ako vytvoriť profil kontroly podľa vašich predstáv si pozrite kapitolu ThreatSense, ktorá obsahuje popis každého parametra kontroly.

> Povedzme, že chcete vytvoriť vlastný profil kontroly a čiastočne vám vyhovujú nastavenia predvoleného profilu používaného v prípade funkcie **Skontrolovať váš počítač**. Nechcete však kontrolovať runtime archívy či potenciálne nebezpečné aplikácie a chcete tiež použiť nastavenie **Vždy vyriešiť detekciu**. Zadajte názov nového profilu do okna **Manažér profilov** a kliknite na **Pridať**. Označte svoj nový profil v roletovom menu **Aktívny profil**, upravte ostatné parametre tak, aby vám vyhovovali, a profil uložte kliknutím na **OK**.

Aktualizácia

Editor profilov v rámci nastavení aktualizácie umožňuje používateľom vytvárať nové profily aktualizácie. Používanie iných profilov ako je štandardne nastavený **Môj profil** má význam v prípade, ak sa počítač pripája na aktualizačné servery viacerými spôsobmi.

Príkladom je notebook, ktorý sa pripája v domácej sieti na lokálny server – Mirror, avšak keď je mimo, na cestách, sťahuje si aktualizácie priamo zo serverov spoločnosti ESET. Vtedy je potrebné vytvoriť dva profily. Jeden sa bude pripájať na lokálny server, druhý, cestovný, na servery spoločnosti ESET. Po nakonfigurovaní profilov môžete v sekcii **Nástroje** > **Plánovač** upraviť parametre úlohy aktualizácie. Označte jeden profil ako primárny a druhý ako sekundárny.

Aktualizačný profil – profil, ktorý je momentálne používaný. Je možné ho zmeniť výberom iného profilu z roletového menu.

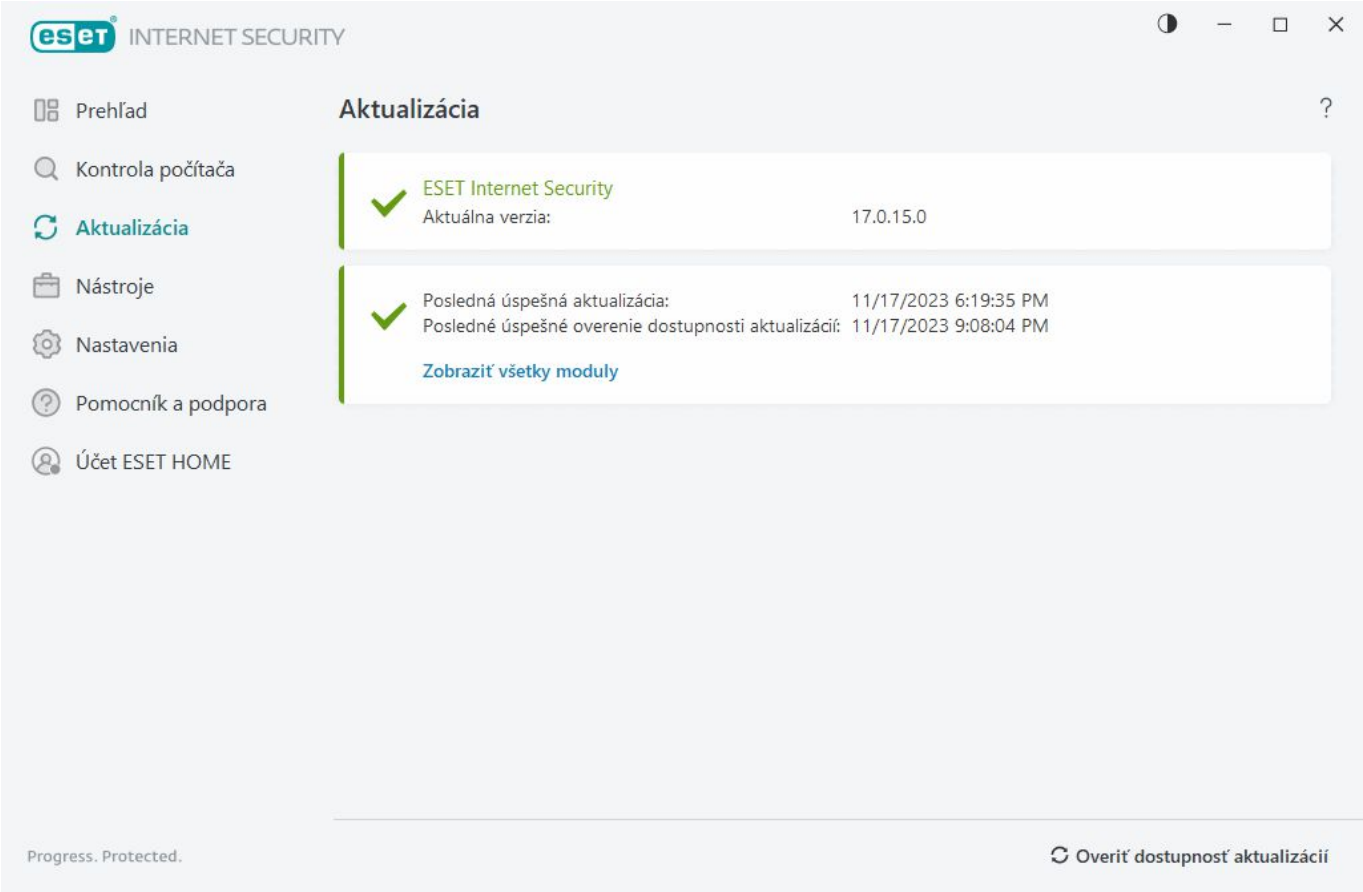
Zoznam profilov – vytvorte nový profil alebo zmeňte už existujúce profily.

Aktualizácie

Pravidelná aktualizácia programu ESET Internet Security je základným predpokladom pre zaistenie maximálnej úrovne ochrany vášho počítača. Modul aktualizácie zabezpečuje, aby bol program vždy aktuálny, a to z hľadiska programových modulov, ako aj systémových súčastí.

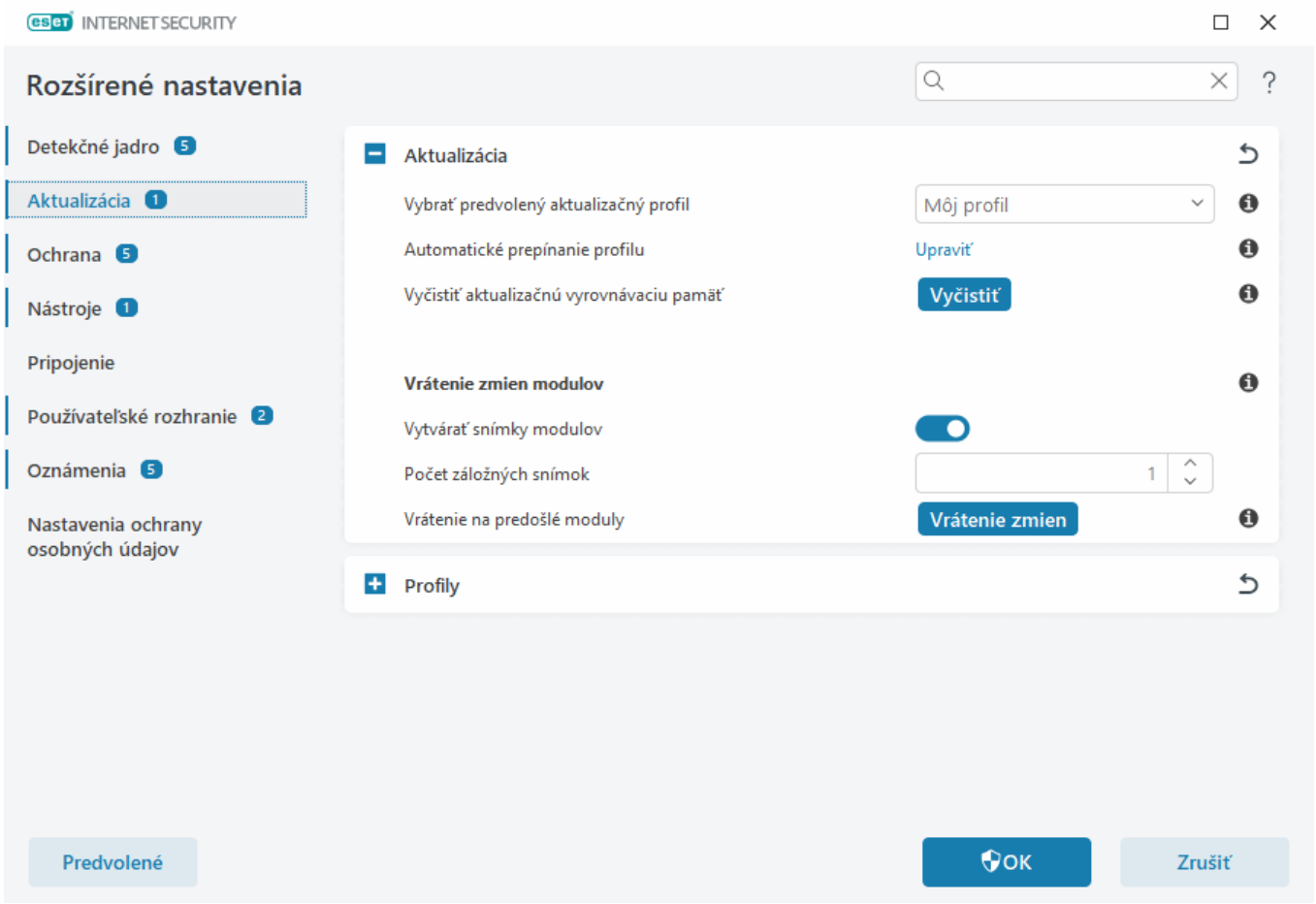
V sekcii **Aktualizácia** v hlavnom okne programu je zobrazený aktuálny stav aktualizácie vrátane informácie o dátume a čase poslednej úspešnej aktualizácie, prípadne aj o dostupnosti novej aktualizácie.

Popri automatických aktualizáciách môžete kedykoľvek použiť tlačidlo **Overiť dostupnosť aktualizácií** na manuálne spustenie aktualizácie.



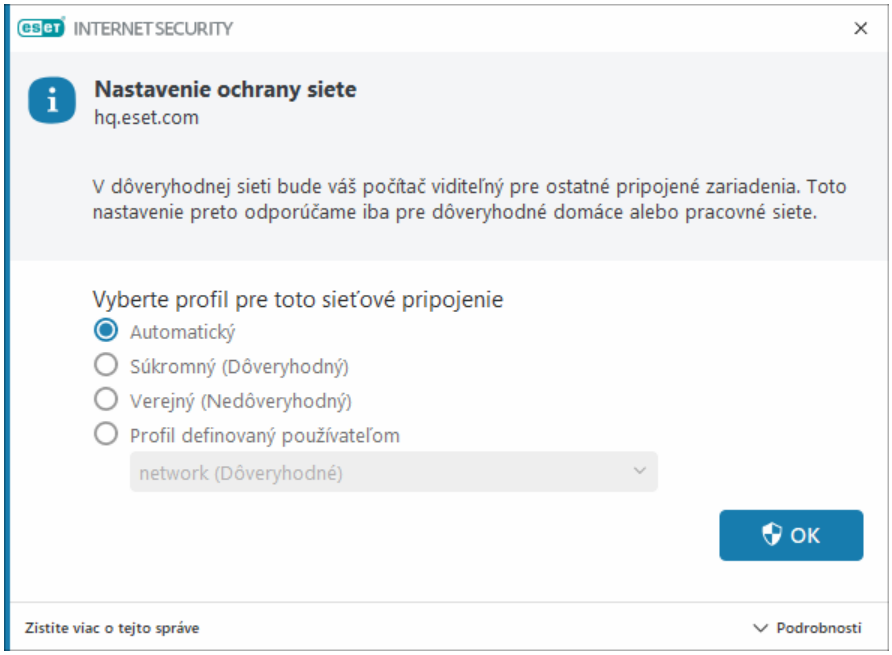
Sekcia Rozšírené nastavenia > **Aktualizácia** obsahuje dodatočné možnosti konfigurácie, napríklad režim aktualizácie, prístup k proxy serveru a LAN pripojenia.

V prípade problémov s aktualizovaním produktu kliknite na tlačidlo **Vyčistiť** a vyčistite vyrovnávaciu pamäť s aktualizačnými súbormi. Ak sa vám stále nedarí aktualizovať programové moduly, prečítajte si článok Čo robiť, ak aktualizácia modulov nebola úspešná a skončila chybou.



Nastavenie ochrany siete

Keď sa objaví nová sieť, ESET Internet Security pre ňu v predvolenom nastavení použije konfiguráciu zo systému Windows. Ak chcete, aby sa pri nájdení novej siete zobrazilo dialógové okno, nastavte priraďovanie profilu Ochrany siete na možnosť **Spýtať sa**. K nastaveniu ochrany siete budete vyzvaný vždy, keď sa váš počítač pripojí k novej sieti.



Môžete si vybrať z nasledujúcich profilov sieťového pripojenia:

Automatický – ESET Internet Security vyberie profil automaticky na základe aktivátorov nakonfigurovaných pre každý profil.

Súkromný – pre dôveryhodné siete (domácu alebo pracovnú sieť). Váš počítač a zdieľané súbory uložené na počítači budú viditeľné zo siete a systémové prostriedky budú dostupné pre ostatných používateľov v sieti (prístup k zdieľaným súborom a tlačiarňam, ako aj prichádzajúca RPC komunikácia budú povolené a služba zdieľania pracovnej plochy bude takisto dostupná). Toto nastavenie odporúčame použiť pri bezpečných lokálnych sieťach. Tento profil sa automaticky priradí k sieťovému pripojeniu, ak je v systéme Windows použitá konfigurácia domény alebo súkromnej siete.

Verejný – pre nedôveryhodné siete (verejné siete). Súbory a priečinky uložené vo vašom systéme nebudú zdieľané ani viditeľné pre ostatných používateľov v sieti a zdieľanie systémových prostriedkov bude deaktivované. Toto nastavenie odporúčame použiť pri pripojení k bezdrôtovým sieťam. Tento profil sa automaticky priradí ku každému sieťovému pripojeniu, ktoré nie je v systéme Windows nakonfigurované ako doména alebo súkromná sieť.

Profil definovaný používateľom – z roletového menu môžete vybrať vami vytvorený profil. Táto možnosť je k dispozícii len vtedy, ak ste vytvorili aspoň jeden vlastný profil.

Nesprávnym nastavením siete vystavujete počítač potenciálnemu bezpečnostnému riziku.

Zapnutie nástroja Anti-Theft

Pri každodennom cestovaní z domova do práce alebo iných verejných miest sú osobné zariadenia neustále vystavené riziku odcudzenia alebo straty. Anti-Theft je funkcia, ktorá výrazne zvyšuje zabezpečenie zariadenia v prípade jeho straty alebo krádeže. Anti-Theft vám umožní cez účet ESET HOME sledovať, či zariadenie niekto používa, a takisto vám ukáže polohu alebo IP adresy, z ktorých sa vaše zariadenie pripája na internet. Pomôže vám tak vystopovať zariadenie a ochrániť súkromné dáta.

Pomocou moderných technológií ako IP geolokácia, snímanie fotografií z webkamery, ochrana používateľských účtov a monitorovanie zariadenia dokáže Anti-Theft výrazne pomôcť pri hľadaní strateného zariadenia alebo pri odhalení krádeže. Cez ESET HOME môžete vidieť, aká aktivita prebieha na vašom počítači alebo zariadení.

Ak sa chcete dozvedieť viac informácií o funkcii Anti-Theft v rámci ESET HOME, pozrite si Online pomocníka pre ESET HOME.

Anti-Theft nemusí správne fungovať na počítačoch v doménach, a to z dôvodu obmedzení v správe používateľských účtov.

Ak chcete zapnúť Anti-Theft a zabezpečiť svoje zariadenie pre prípad straty alebo krádeže, použite jednu z nasledujúcich možností:

- V hlavnom okne programu v sekcii **Prehľad** kliknite na možnosť **Nastaviť** vedľa položky **Anti-Theft**.
- Ak v hlavnom okne programu v sekcii **Prehľad** vidíte správu „Anti-Theft je k dispozícii“, kliknite na **Zapnúť Anti-Theft**.
- V hlavnom okne programu kliknite na **Nastavenia** > **Bezpečnostné nástroje**. Pomocou prepínacieho tlačidla zapnite **Anti-Theft** a postupujte podľa pokynov na obrazovke.

Ak vaše zariadenie nie je pripojené k účtu ESET HOME, musíte postupovať nasledovne:
1. Pri zapínaní funkcie Anti-Theft sa prihláste do svojho účtu ESET HOME.
2. Nastavte názov zariadenia.

Anti-Theft nie je podporovaný na operačnom systéme Microsoft Windows Home Server.

Po zapnutí funkcie Anti-Theft môžete optimalizovať zabezpečenie svojho zariadenia v hlavnom okne programu v sekcii **Nastavenia** > **Bezpečnostné nástroje** > **Anti-Theft**.

Rodičovská kontrola

Ak ste už aktivovali rodičovskú kontrolu v programe ESET Internet Security, je potrebné ešte nastaviť príslušné používateľské účty, aby mohla rodičovská kontrola správne fungovať.

Ak je rodičovská kontrola aktívna, ale ešte nie sú nastavené používateľské účty, v programe ESET Internet Security bude na obrazovke **Prehľad** zobrazené oznámenie „Rodičovská kontrola nie je nastavená“. Kliknite na **Nastaviť pravidlá** a prečítajte si kapitolu Rodičovská kontrola, kde nájdete viac informácií.

Aktivácia produktu

Existuje niekoľko možností, ako aktivovať váš produkt ESET. Dostupnosť jednotlivých aktivačných možností sa môže líšiť v závislosti od krajiny a spôsobu distribúcie inštalačného súboru (CD/DVD, webová stránka spoločnosti ESET atď.):

- Ak ste si zakúpili krabicovú verziu produktu alebo ste informácie o predplatnom dostali na e‑mail, produkt aktivujte kliknutím na možnosť **Použiť zakúpený aktivačný kľúč**. Aby bola aktivácia úspešná, aktivačný kľúč je potrebné zadať presne v tom tvare, v akom je uvedený. Aktivačný kľúč je jedinečný reťazec znakov vo formáte XXXX-XXXX-XXXX-XXXX-XXXX alebo XXXX-XXXXXXXX, ktorý sa používa na identifikáciu vlastníka predplatného a na aktiváciu. Aktivačný kľúč zvyčajne nájdete vnútri alebo na zadnej strane balenia.

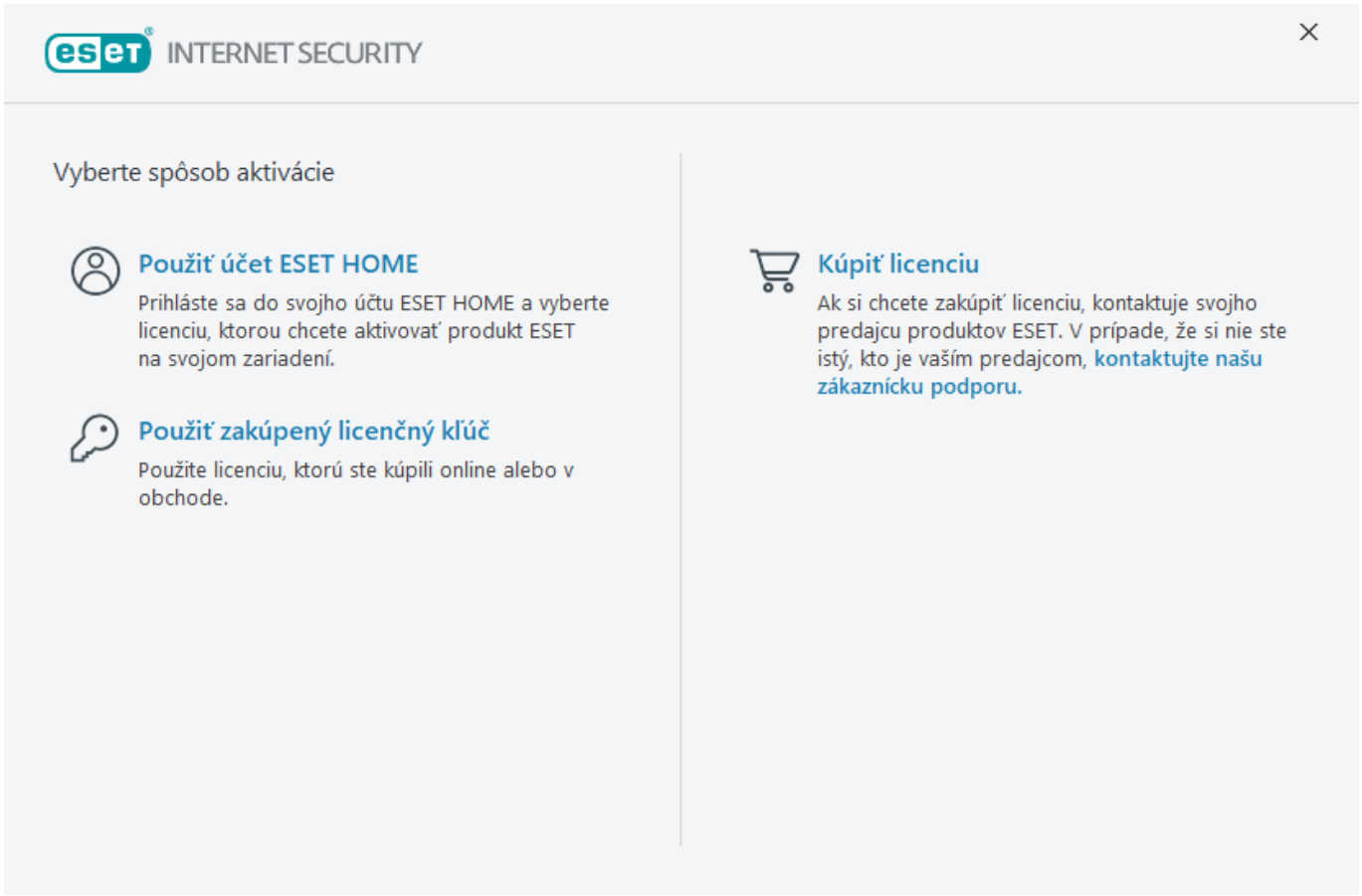
- Po zvolení možnosti Použiť účet ESET HOME sa zobrazí výzva na prihlásenie do účtu ESET HOME.

- Ak si chcete pred zakúpením predplatného produkt ESET Internet Security vyskúšať, zvoľte možnosť Vyskúšať bezplatnú verziu. Zadajte e‑mailovú adresu a krajinu, aby bolo možné aktivovať produkt ESET Internet Security na obmedzené časové obdobie. Na zadanú e‑mailovú adresu vám zašleme informácie o bezplatnej skúšobnej verzii. Každý zákazník môže skúšobnú verziu využiť len raz.

- Ak ešte nemáte predplatné a želáte si ho zakúpiť, kliknite na možnosť **Kúpiť predplatné**. Následne sa otvorí webová stránka lokálneho distribútora produktov ESET. Predplatné produktov ESET pre domácnosti s OS Windows nie je dostupné zdarma.

Svoje predplatné produktu môžete kedykoľvek zmeniť. V prípade, že chcete zmeniť predplatné, kliknite v hlavnom okne programu na **Pomocník a podpora** > **Zmeniť predplatné**. Uvidíte verejné identifikačné číslo, ktoré slúži na identifikáciu predplatného.

Neúspešná aktivácia produktu?



Zadanie aktivačného kľúča počas aktivácie

Pre úplnú funkčnosť programu sú dôležité pravidelné aktualizácie. ESET Internet Security bude automaticky dostávať aktualizácie len v tom prípade, že bol úspešne aktivovaný.

Je dôležité, aby ste **aktivačný kľúč** zadali presne v tom tvare, v akom je napísaný. Aktivačný kľúč je jedinečný reťazec znakov vo formáte XXXX-XXXX-XXXX-XXXX-XXXX, ktorý sa používa na identifikáciu vlastníka predplatného a aktiváciu predplatného.

Odporúčame vám aktivačný kľúč skopírovať z registračného e-mailu a vložiť ho do programu, aby ste tak mali istotu, že kľúč je zadaný v presnom tvare.

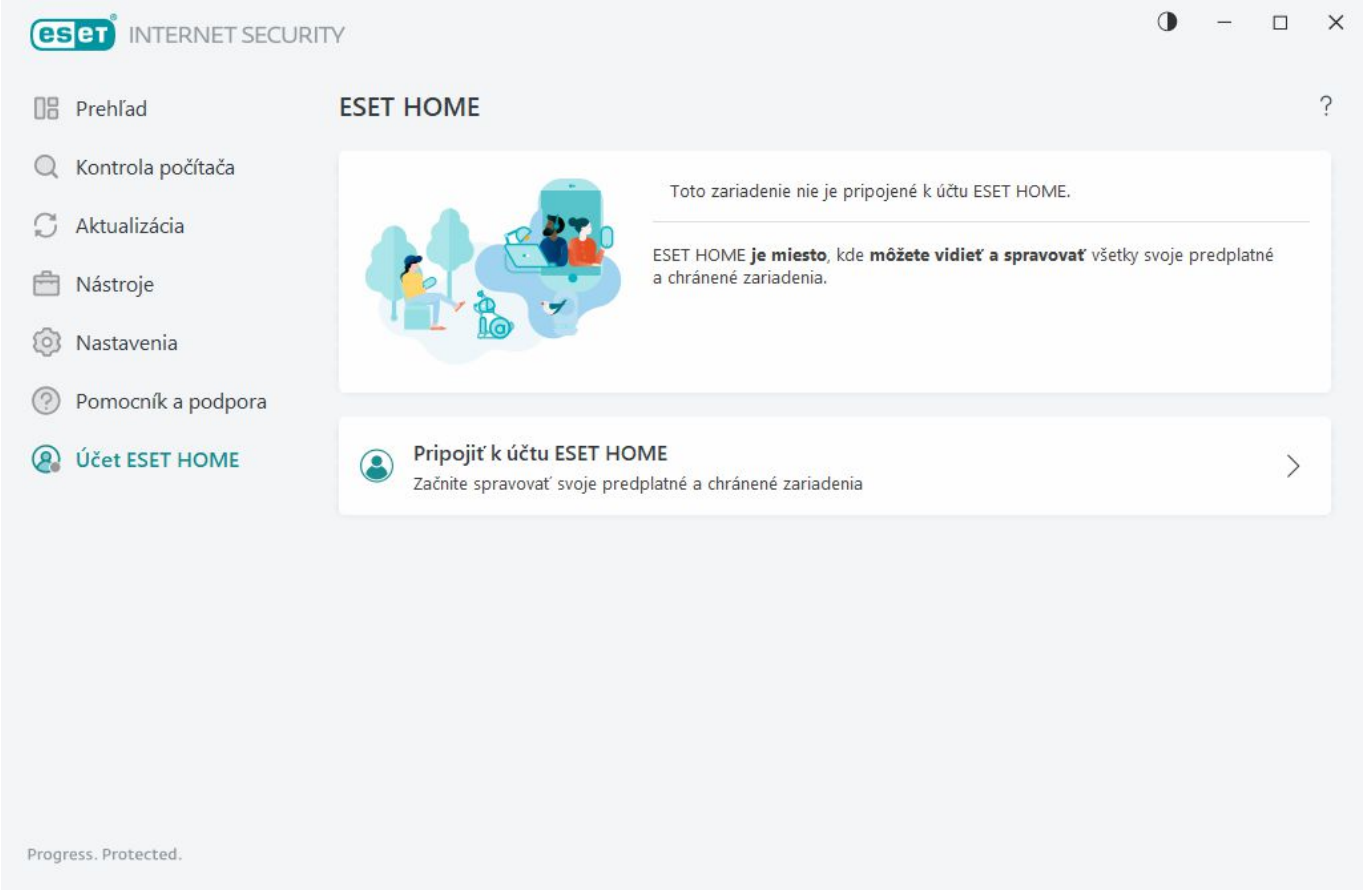
Ak ste nezadali aktivačný kľúč ihneď po inštalácii, produkt nie je aktivovaný a je teda potrebné ho dodatočne aktivovať. ESET Internet Security môžete aktivovať v hlavnom okne programu > **Pomocník a podpora** > **Aktivovať predplatné**.

Predplatné produktov ESET pre domácnosti s OS Windows nie je dostupné zdarma.

Použitie účtu ESET HOME

Pripojte svoje zariadenie k portálu ESET HOME, cez ktorý si môžete pozrieť a spravovať všetky svoje aktivované predplatné od spoločnosti ESET a chránené zariadenia. Predplatné si tu môžete jednoducho obnoviť, rozšíriť alebo zmeniť na vyšší produkt a tiež si môžete pozrieť dôležité informácie o predplatnom. V portáli na správu alebo mobilnej aplikácii ESET HOME môžete pridávať predplatné, sťahovať produkty do svojich zariadení a sledovať ich bezpečnostný stav, prípadne zdieľať predplatné s rodinou či priateľmi prostredníctvom e-mailu. Viac informácií

nájdete na stránkach Online pomocníka pre ESET HOME.



Po zvolení možnosti **Použiť účet ESET HOME** ako spôsobu aktivácie alebo pri pripájaní k účtu ESET HOME počas inštalácie postupujte nasledovne:

1. Prihláste sa do svojho účtu ESET HOME.

> Ak účet ESET HOME ešte nemáte, kliknite na možnosť **Vytvoriť účet** a zaregistrujte sa. Inštrukcie nájdete na stránke Online pomocníka ESET HOME.
> V prípade, že si neviete spomenúť na svoje heslo, kliknite na možnosť **Nepamätám si svoje heslo** a riaďte sa pokynmi na obrazovke, prípadne prejdite na stránku Online pomocníka ESET HOME.

2. Nastavte **Názov zariadenia**, ktorý sa bude používať naprieč všetkými službami ESET HOME, a následne kliknite na **Pokračovať**.

3. Zvoľte predplatné na aktivovanie produktu alebo pridajte nové predplatné. Kliknutím na **Pokračovať** aktivujte ESET Internet Security.

Aktivovať bezplatnú skúšobnú verziu

Na aktiváciu skúšobnej verzie ESET Internet Security zadajte do polí **E-mailová adresa** a **Potvrdenie e-mailovej adresy** platnú e-mailovú adresu. Po aktivácii sa vygeneruje predplatné ESET, ktoré bude zaslané na váš e-mail. Táto e-mailová adresa bude tiež slúžiť na prijímanie upozornení o končiacej sa platnosti predplatného a inú komunikáciu so spoločnosťou ESET. Bezplatnú skúšobnú verziu je možné aktivovať len raz.

Zvoľte svoju krajinu z roletového menu **Krajina** pre registráciu ESET Internet Security u vášho lokálneho distribútora, ktorý vám bude poskytovať technickú podporu.

Bezplatný aktivačný kľúč ESET

Predplatné produktu ESET Internet Security nie je zdarma.

Aktivačný kľúč od spoločnosti ESET predstavuje unikátny reťazec písmen a čísel oddelených pomlčkou, ktorý umožňuje legálne používanie produktu ESET Internet Security v súlade s Licenčnou dohodou s koncovým používateľom. Každý koncový používateľ je oprávnený používať aktivačný kľúč len do toho rozsahu, v akom má právo používať ESET Internet Security, a to na základe počtu licencií poskytnutých spoločnosťou ESET. Aktivačný kľúč sa považuje za dôverný údaj, ktorý nemožno zdieľať; možno však zdieľať predplatné cez portál ESET HOME.

Na internete nájdete rôzne zdroje, ktoré môžu ponúkať „bezplatné“ aktivačné kľúče k produktom ESET, no pamätajte si:

- Kliknutie na reklamu, ktorá ponúka „predplatné ESET zdarma“, môže viesť k narušeniu zabezpečenia a napadnutiu počítača či zariadenia malvérom. Malvér môže byť ukrytý v neoficiálnom webovom obsahu (napr. vo videách), na webových stránkach, ktoré zobrazujú reklamy s cieľom zarobiť na návštevnosti, atď. V týchto prípadoch je ponúkané predplatné zvyčajne iba návnadou.

- Spoločnosť ESET môže nelegálne používané predplatné deaktivovať, čo aj robí.

- Používanie nelegálne získaného aktivačného kľúča nie je v súlade s Licenčnou dohodou s koncovým používateľom, ktorej podmienky musíte prijať, aby ste si mohli produkt ESET Internet Security nainštalovať.

- Predplatné ESET si kupujte iba cez oficiálne predajné kanály, ako je stránka www.eset.com, naši distribútori či predajcovia (nekupujte predplatné z neoficiálnych webových stránok tretích strán ako eBay ani zdieľané predplatné tretích strán).

- Stiahnutie programu ESET Internet Security je bezplatné, no počas inštalácie sa vyžaduje aktivácia produktu platným aktivačným kľúčom od spoločnosti ESET (produkt si teda môžete stiahnuť a nainštalovať, no bez aktivácie nebude fungovať).

- Nezdieľajte svoje predplatné cez internet alebo sociálne médiá (mohlo by sa rozšíriť medzi veľký počet ľudí).

Ak chcete zistiť, ako identifikovať a nahlásiť nelegálne používané predplatné ESET, prečítajte si náš článok Databázy znalostí, v ktorom nájdete podrobné inštrukcie.

Ak s kúpou bezpečnostného produktu ESET ešte váhate, môžete si stiahnuť skúšobnú verziu a rozhodnúť sa na základe nej:

1. Aktivujte si bezplatnú skúšobnú verziu ESET Internet Security.

2. Pripojte sa k ESET Beta programu.

3. Ak používate mobilné zariadenie so systémom Android, nainštalujte si aplikáciu ESET Mobile Security, ktorá je dostupná aj ako bezplatná verzia.

Ak chcete získať zľavu/predĺžiť platnosť licencie, obnovte si licenciu ESET.

Aktivácia nebola úspešná – najčastejšie príčiny

Ak aktivácia produktu ESET Internet Security neprebehne úspešne, najčastejšie ide o niektorú z nasledujúcich príčin:

- Aktivačný kľúč sa už používa.
- Zadali ste neplatný aktivačný kľúč.
- Informácie v aktivačnom formulári chýbajú alebo sú neplatné.
- Zlyhala komunikácia s aktivačným serverom.
- Nie je dostupné alebo je vypnuté pripojenie k aktivačným serverom spoločnosti ESET.

Uistite sa, že ste zadali správny aktivačný kľúč a vaše internetové pripojenie je aktívne. Skúste produkt ESET Internet Security aktivovať znova. Ak chcete na aktiváciu použiť účet ESET HOME, prečítajte si informácie o správe predplatného v účte ESET HOME na stránkach Online pomocníka.

Ak sa zobrazí konkrétna chyba (napríklad pozastavené alebo prečerpané predplatné), postupujte podľa pokynov v kapitole Stav predplatného.

Ak sa vám stále nedarí aktivovať ESET Internet Security, náš sprievodca riešením problémov s aktiváciou vám poskytne odpovede na najčastejšie otázky, chyby a problémy týkajúce sa aktivácie a licencovania (dostupné v angličtine a niekoľkých ďalších jazykoch).

Stav predplatného

Vaše predplatné môže mať rôzne stavy. Informácie o stave svojho predplatného nájdete v účte ESET HOME. Ak chcete pridať svoje predplatné do účtu ESET HOME, prečítajte si kapitolu Pridanie predplatného.

Ak účet ESET HOME ešte nemáte, môžete si vytvoriť nový účet ESET HOME.

Ak je stav predplatného iný ako **Aktívny**, počas aktivácie sa zobrazí chyba alebo oznámenie v hlavnom okne programu.

Zobrazovanie oznámení o stave predplatného môžete vypnúť v sekcii Rozšírené nastavenia > **Oznámenia** > **Stavy aplikácie**. Kliknite na **Upraviť** vedľa položky **Stavy aplikácie**, rozbaľte **Licencovanie** a zrušte výber možnosti vedľa oznámenia, ktoré sa vám už nemá zobrazovať. Vypnutie zobrazovania oznámenia problém nevyrieši.

V nasledujúcej tabuľke nájdete popisy a odporúčania pre rôzne stavy predplatného:

Stav predplatného	Popis	Riešenie
Aktívne	Predplatné je platné a z vašej strany nie je potrebná žiadna interakcia. ESET Internet Security je možné aktivovať, pričom podrobnosti o predplatnom nájdete v hlavnom okne programu > **Pomocník a podpora**.	

Stav predplatného	Popis	Riešenie
Prečerpané	Toto predplatné používa viac zariadení, než je povolené. Zobrazí sa chyba pri aktivácii.	Viac informácií nájdete v kapitole Aktivácia nebola úspešná z dôvodu prečerpania predplatného.
Pozastavené	Vaše predplatné bolo pozastavené z dôvodu problémov s platbou. Ak chcete predplatné používať, uistite sa, že vaše platobné údaje v účte ESET HOME sú aktuálne, prípadne sa obráťte na svojho predajcu. Táto chyba sa môže zobraziť počas aktivácie alebo v hlavnom okne programu.	Nainštalovaný produkt – ak máte účet ESET HOME, v oznámení zobrazenom v hlavnom okne programu kliknite na možnosť **Spravujte svoje predplatné v účte ESET HOME** a skontrolujte svoje platobné údaje. V opačnom prípade sa obráťte na predajcu predplatného. Chyba pri aktivácii – ak máte účet ESET HOME, v okne upozorňujúcom na chybu pri aktivácii kliknite na možnosť **Otvoriť účet ESET HOME** a skontrolujte svoje platobné údaje. V opačnom prípade sa obráťte na predajcu predplatného.
Platnosť skončila	Vaše predplatné sa skončilo a nie je možné ho použiť na aktiváciu produktu ESET Internet Security. Táto chyba sa môže zobraziť počas aktivácie alebo v hlavnom okne programu. Ak už máte nainštalovaný produkt ESET Internet Security, váš počítač nie je chránený ani aktualizovaný.	Nainštalovaný produkt – v oznámení zobrazenom v hlavnom okne programu kliknite na možnosť **Obnoviť predplatné** a postupujte podľa pokynov v článku Obnovenie predplatného k produktu ESET, prípadne kliknite na možnosť **Aktivovať produkt** a vyberte spôsob aktivácie. Chyba pri aktivácii – v okne upozorňujúcom na chybu pri aktivácii kliknite na možnosť **Obnoviť predplatné** a postupujte podľa pokynov v článku Obnovenie predplatného k produktu ESET, prípadne zadajte nový alebo obnovený aktivačný kľúč a kliknite na **Obnoviť predplatné**.
Zrušené	Vaše predplatné bolo zrušené spoločnosťou ESET alebo predajcom predplatného.	Ak sa zobrazí chyba: Zrušené predplatné v hlavnom okne programu alebo počas aktivácie a vaše predplatné by malo fungovať správne, kontaktujte svojho predajcu predplatného.

Aktivácia nebola úspešná z dôvodu prečerpania predplatného

O čo ide

- Mohlo dôjsť k prečerpaniu alebo zneužitiu vášho predplatného
- Aktivácia nebola úspešná z dôvodu prečerpania predplatného

Riešenie

Toto predplatné používa viac zariadení, než je povolené. Je možné, že ste sa stali obeťou podvodu alebo softvérového pirátstva. Predplatné nie je možné použiť na aktiváciu ďalšieho produktu ESET. Ak ste si predplatné zakúpili z dôveryhodného zdroja alebo máte oprávnenie spravovať ho z účtu ESET HOME, môžete tento problém vyriešiť veľmi rýchlo. Ak účet ešte nemáte, založte si ho.

Ak ste vlastníkom predplatného, no nezobrazila sa vám výzva na zadanie e□mailovej adresy, postupujte takto:

1. Vo webovom prehliadači otvorte stránku https://home.eset.com, aby ste mohli spravovať svoje predplatné od spoločnosti ESET. Prejdite do sekcie ESET License Manager a odstráňte alebo deaktivujte licenčné jednotky. Viac sa dočítate v kapitole Čo robiť v prípade prečerpaného predplatného.

2. Pokyny, ako identifikovať a nahlásiť nelegálne používané predplatné ESET, nájdete v našom článku Identifikácia a nahlasovanie pirátskych predplatných ESET.

3. Ak máte pochybnosti, kliknite na **Späť** a kontaktujte technickú podporu spoločnosti ESET.

Ak predplatné nepatrí vám, kontaktujte vlastníka predplatného a informujte ho o tom, že predplatné je prečerpané a nie je možné ním aktivovať ďalší produkt ESET. Vlastník môže tento problém vyriešiť na portáli ESET HOME.

Ak sa vám zobrazí výzva na potvrdenie e□mailovej adresy (iba v niektorých prípadoch), zadajte adresu, ktorú ste použili pri kúpe alebo aktivácii produktu ESET Internet Security.

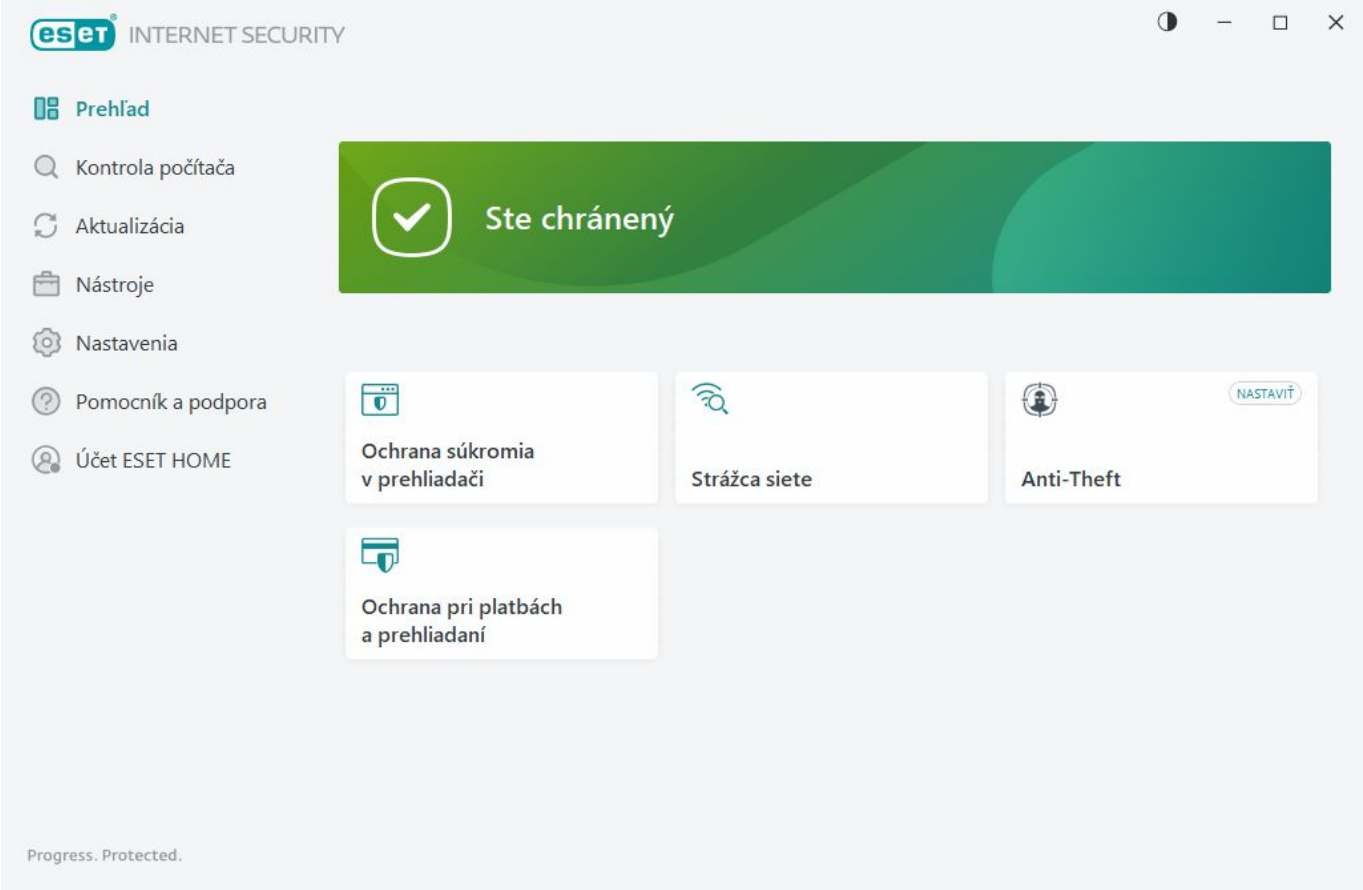
Práca s programom ESET Internet Security

Hlavné okno programu ESET Internet Security je rozdelené na dve časti. Časť vpravo zobrazuje informácie, ktoré podliehajú voľbe v hlavnom menu vľavo.

> **Ilustrované inštrukcie**
> Pozrite si náš článok Databázy znalostí s ilustrovanými inštrukciami o tom, ako otvoriť hlavné okno programu ESET pre Windows.

Farebný motív grafického rozhrania ESET Internet Security môžete vybrať v pravom hornom rohu hlavného okna programu. Kliknite na ikonu **farebného motívu** (ikona sa mení podľa aktuálne zvoleného farebného motívu) vedľa ikony **Minimalizovať** a z roletového menu vyberte farebný motív:

- **Rovnaký ako systémová farba** – farebný motív programu ESET Internet Security sa nastaví podľa operačného systému.
- **Tmavý** – ESET Internet Security bude mať tmavý motív (tmavý režim).
- **Svetlý** – ESET Internet Security bude mať štandardný svetlý motív.



Možnosti hlavného menu:

Prehľad – poskytuje informácie o stave ochrany počítača prostredníctvom programu ESET Internet Security.

Kontrola počítača – umožňuje nastaviť a spustiť kontrolu počítača a nakonfigurovať vlastnú kontrolu zodpovedajúcu požiadavkám používateľa.

Aktualizácia – zobrazuje informácie o aktualizáciách modulov a detekčného jadra.

Nástroje – poskytujú prístup k Strážcovi siete a iným funkciám, ktoré pomáhajú zjednodušiť správu programu a ponúkajú doplňujúce nastavenia pre pokročilých používateľov.

Nastavenia – umožňujú konfiguráciu funkcií ochrany v rámci produktu ESET Internet Security (Ochrana počítača, Ochrana internetu, Ochrana siete a Bezpečnostné nástroje) a prístup k rozšíreným nastaveniam.

Pomocník a podpora – zobrazuje informácie o vašom predplatnom, nainštalovanom produkte ESET a odkazy na stránky Online pomocníka, Databázu znalostí spoločnosti ESET a technickú podporu.

Účet ESET HOME – pripojte svoje zariadenie k účtu ESET HOME alebo skontrolujte stav pripojenia k účtu ESET HOME. Na zobrazenie a správu nastavení Anti-Theft, ako aj aktivovaných predplatných a zariadení použite účet ESET HOME.

Prehľad

V okne **Prehľad** sa zobrazujú informácie o aktuálnej ochrane počítača spolu s rýchlymi odkazmi na bezpečnostné funkcie produktu ESET Internet Security.

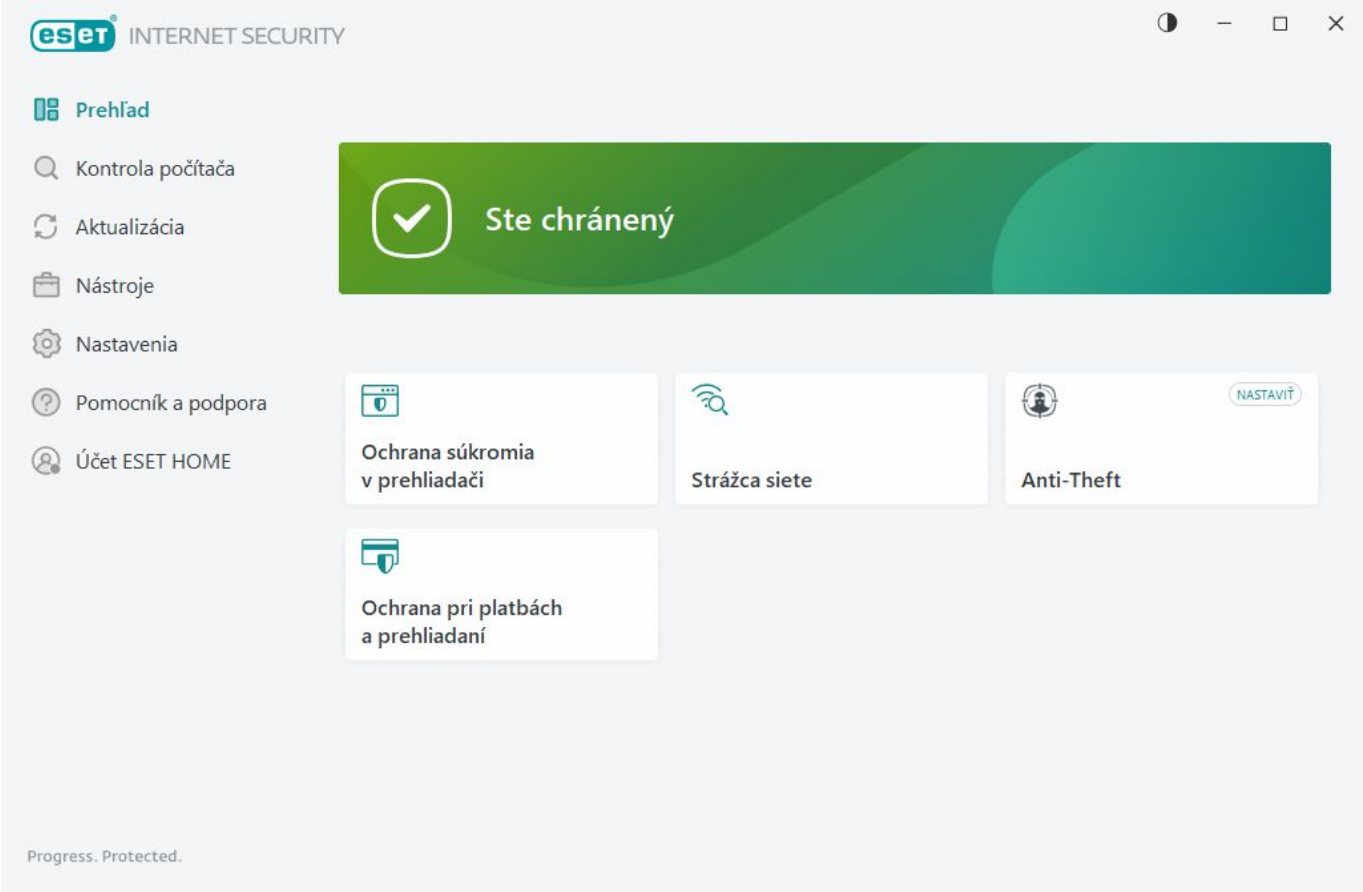
V okne **Prehľad** sa zobrazujú oznámenia s podrobnými informáciami a odporúčaniami na zvýšenie bezpečnosti

prostredníctvom produktu ESET Internet Security, zapnutie ďalších funkcií alebo zabezpečenie maximálnej ochrany. Ak je oznámení viac, kliknutím na tlačidlo **X ďalších oznámení** ich všetky rozbalíte.

Strážca siete – overí bezpečnosť vašej siete.

Ochrana pri platbách a prehliadaní – spustí prehliadač, ktorý je v systéme Windows nastavený ako predvolený, v zabezpečenom režime.

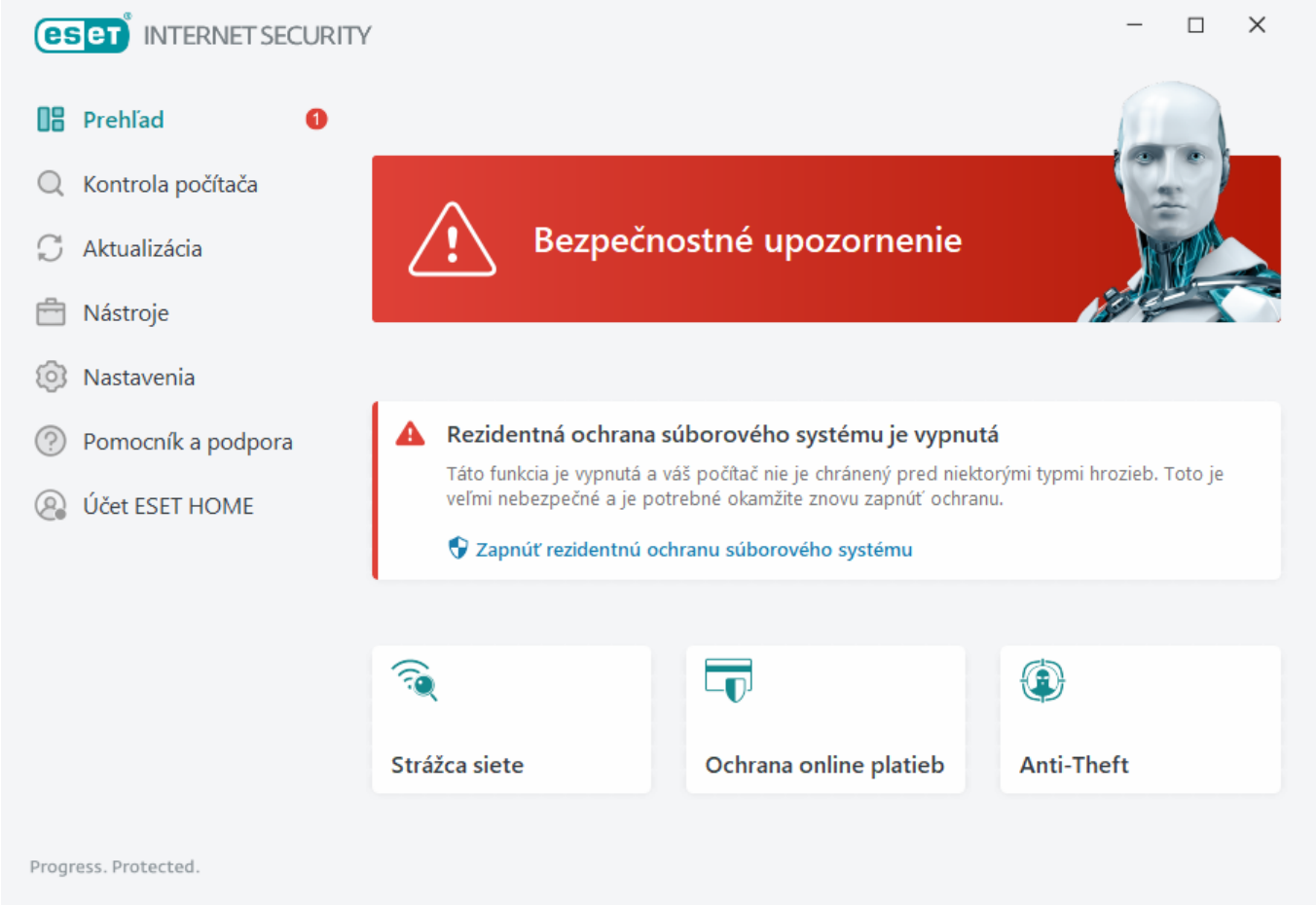
Anti-Theft – otvorí nastavenia funkcie Anti-Theft. Ak už máte funkciu Anti-Theft nastavenú, po kliknutí na rýchly odkaz sa otvorí okno Anti-Theft.



Zelená ikona a zelený nápis **Ste chránený** znamenajú, že je zaistená maximálna úroveň ochrany.

Čo robiť, ak program nepracuje správne?

Pri správnom fungovaní ochrany majú jednotlivé moduly zelenú ikonu stavu. Červený výkričník alebo oranžové upozornenie znamenajú, že ochrana vášho systému nie je zaručená v plnej miere. Podrobné informácie o stave ochrany jednotlivých modulov, ako aj odporúčané riešenia na obnovenie plnej ochrany sa zobrazujú ako oznámenia v okne **Prehľad**. Stav jednotlivých modulov je možné meniť v sekcii **Nastavenia** po označení požadovaného modulu.



Červená ikona a červený nápis **Bezpečnostné upozornenie** signalizujú kritické problémy. Možné príčiny sú:

- **Produkt nie je aktivovaný** alebo **Predplatné sa skončilo** – v tomto prípade ikona stavu ochrany zmení farbu na červenú. Po skončení predplatného nebude možné program aktualizovať. Ak chcete predplatné obnoviť, odporúčame postupovať podľa pokynov vo výstražnom okne.
- **Detekčné jadro je neaktuálne** – toto chybové hlásenie sa zobrazí po niekoľkých neúspešných pokusoch o aktualizáciu detekčného jadra. Odporúčame, aby ste skontrolovali nastavenia aktualizácie. Najčastejším problémom sú nesprávne zadané autorizačné údaje alebo nesprávne nakonfigurované nastavenia pripojenia.
- **Rezidentná ochrana súborového systému je vypnutá** – rezidentná ochrana bola deaktivovaná používateľom. Váš počítač nie je chránený pred hrozbami. Kliknite na **Zapnúť rezidentnú ochranu súborového systému** pre opätovné povolenie tejto funkcie.
- **Antivírusová a antispyvérová ochrana je vypnutá** – kompletnú ochranu môžete znova spustiť kliknutím na **Zapnúť antivírusovú a antispyvérovú ochranu**.
- **ESET Firewall je vypnutý** – tento problém je tiež signalizovaný notifikáciou na paneli oznámení vedľa ikony **siete**. Obnoviť funkciu firewallu môžete kliknutím na **Zapnúť firewall**.

Oranžová ikona signalizuje obmedzenú ochranu. Môžu sa napríklad vyskytnúť problémy s aktualizáciou programu alebo sa blíži dátum konca predplatného.
Možné príčiny sú:

- **Upozornenie optimalizácie Anti‑Theft** – zariadenie nie je optimalizované na používanie funkcie Anti-Theft. Napríklad Fantómový účet (účet, ktorý sa spustí automaticky, keď označíte zariadenie ako

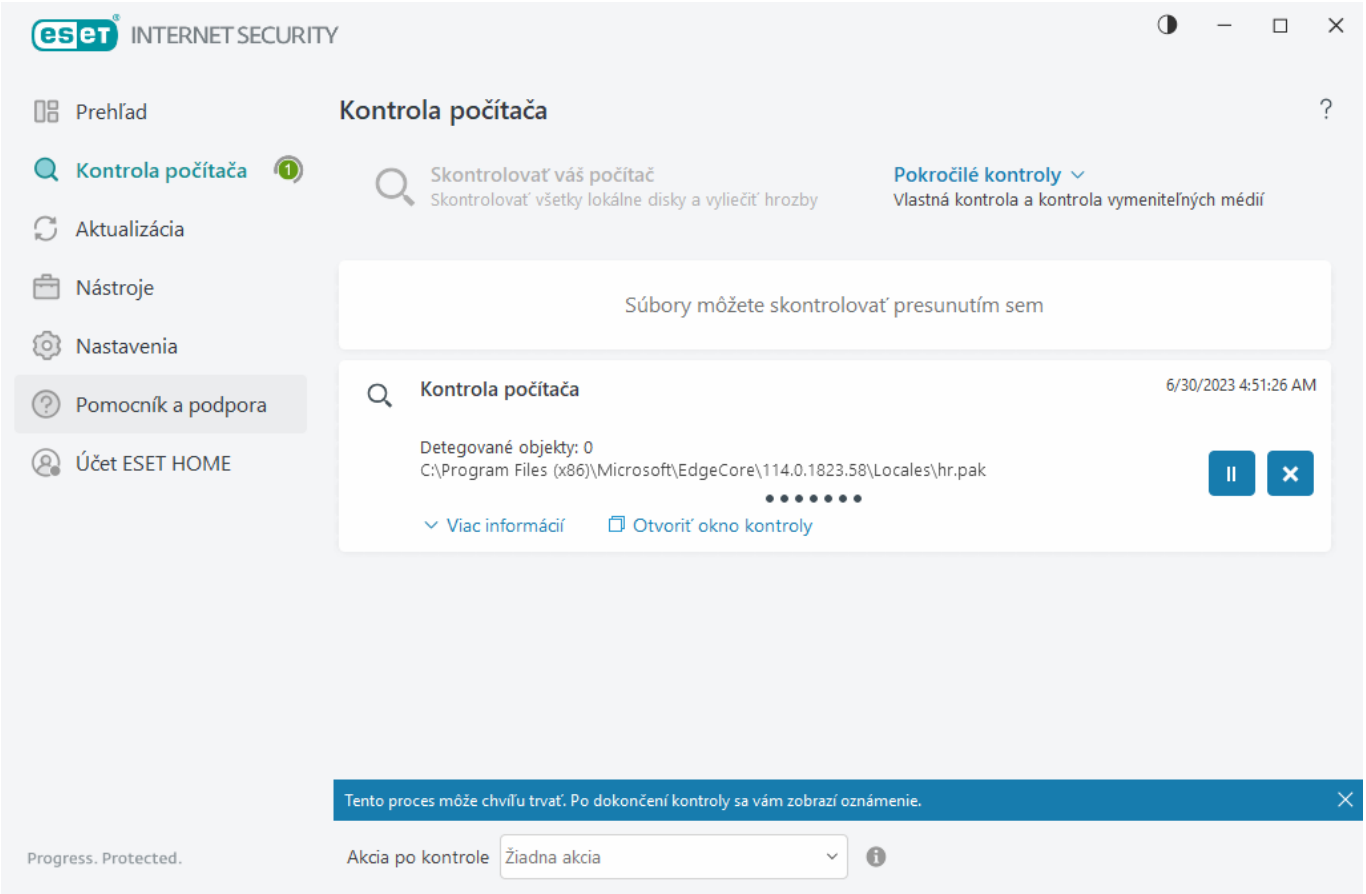
stratené) nie je vytvorený na vašom počítači. Fantómový účet môžete vytvoriť pomocou funkcie Optimalizácia vo webovom rozhraní Anti-Theft.

- **Herný režim je aktívny** – povolenie Herného režimu predstavuje potenciálne bezpečnostné riziko. Zapnutím herného režimu budú zakázané všetky oznámenia/upozornenia programu a úlohy plánovača.
- **Vaše predplatné sa čoskoro skončí/Vaše predplatné sa dnes skončí** – v tomto prípade sa ikona stavu ochrany zmení na výkričník zobrazený na paneli oznámení systému. Po skončení platnosti predplatného nebude možné program aktualizovať a ikona stavu ochrany bude mať červenú farbu.

Ak sa vám nepodarí problém vyriešiť pomocou navrhnutých riešení, je potrebné použiť časť **Pomocník a podpora** alebo vyhľadať informácie o danom probléme v Databáze znalostí spoločnosti ESET. Ak aj napriek tomu potrebujete pomoc, môžete kontaktovať technickú podporu spoločnosti ESET. Špecialisti technickej podpory spoločnosti ESET reagujú na problémy rýchlo a efektívne vám pomôžu s riešením vášho problému.

Kontrola počítača

Dôležitou súčasťou každého antivírusového programu je manuálna kontrola počítača. Umožňuje kontrolu diskov, jednotlivých priečinkov a súborov v počítači. Z bezpečnostného hľadiska je nevyhnutné, aby kontrola počítača bola spúšťaná nielen pri podozrení na infikované súbory, ale aj priebežne v rámci prevencie. HĺbkovúKontrolu počítača odporúčame vykonávať pravidelne, aby ste systém skontrolovali na prítomnosť vírusov, ktoré v čase zápisu na disk neboli zachytené pomocou Rezidentnej ochrany súborového systému. Takáto situácia môže nastať, ak bola rezidentná ochrana v danom čase vypnutá alebo bolo detekčné jadro neaktuálne, prípadne v čase zápisu na disk súbor nebol detegovaný ako vírus.



K dispozícii sú dva typy **kontroly počítača**. Možnosť **Skontrolovať váš počítač** slúži na rýchle spustenie kontroly počítača bez nastavovania ďalších parametrov kontroly. **Vlastná kontrola** (v časti Pokročilé kontroly) naopak

umožňuje vybrať si z prednastavených profilov kontroly zameraných na rozdielne umiestnenia v počítači, ako aj určiť konkrétne ciele kontroly.

Viac informácií nájdete v kapitole Priebeh kontroly.

> Na základe predvolených nastavení sa program ESET Internet Security pri kontrole počítača automaticky pokúsi o vyliečenie alebo vymazanie detegovaného objektu. V niektorých prípadoch, keď nie je možné vykonať žiadnu akciu, sa koncovému používateľovi zobrazí interaktívne upozornenie, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Zmenu úrovne liečenia a podrobnejšie informácie nájdete v kapitole Úrovne liečenia. Ak si chcete pozrieť predchádzajúce kontroly, kliknite na Protokoly.

Skontrolovať váš počítač

Možnosť **Skontrolovať váš počítač** slúži na rýchle spustenie kontroly počítača a vyliečenie infikovaných súborov, a to bez potreby interakcie zo strany používateľa. Hlavnou výhodou možnosti **Skontrolovať váš počítač** je jednoduché a rýchle spustenie bez nutnosti nastavovania parametrov kontroly. Skontrolujú sa všetky súbory na lokálnych diskoch, pričom nájdené infiltrácie budú automaticky vyliečené alebo odstránené. Úroveň liečenia je automaticky nastavená na predvolenú hodnotu. Podrobnejšie informácie o režimoch liečenia nájdete v kapitole Úrovne liečenia.

Môžete tiež manuálne spustiť **kontrolu konkrétneho súboru alebo priečinka jeho presunutím do okna programu (Drag & drop)** – kliknite na daný súbor alebo priečinok a podržte tlačidlo myši stlačené, následne presuňte kurzor myši do vyznačeného priestoru a uvoľnite prst z tlačidla myši. Aplikácia sa následne presunie do popredia.

V časti **Pokročilé kontroly** sú dostupné nasledujúce možnosti:

Vlastná kontrola

Vlastná kontrola je užitočná v prípade, že chcete vybrať konkrétne ciele a metódy kontroly. Výhodou **Vlastnej kontroly** je možnosť nastaviť si parametre kontroly podľa vlastných predstáv. Tieto nastavenia sa dajú uložiť do tzv. profilov. To je užitočné, najmä ak chcete vykonávať pravidelnú vlastnú kontrolu počítača s rovnakými nastaveniami.

Kontrola vymeniteľných médií

Funguje podobne ako funkcia **Skontrolovať váš počítač**, keďže vám umožňuje okamžite spustiť kontrolu vymeniteľných médií aktuálne pripojených do počítača (ako napr. CD/DVD/USB). Toto môže byť užitočné v prípade, ak pripojíte USB kľúč do počítača a želáte si skontrolovať jeho obsah na prítomnosť malvéru alebo iných potenciálnych hrozieb.

Tento typ kontroly je možné spustiť aj tak, že kliknete na možnosť **Vlastná kontrola**, z roletového menu **Ciele kontroly** vyberiete možnosť **Vymeniteľné médiá** a kliknete na **Kontrolovať**.

Opakovať poslednú kontrolu

Táto možnosť vám umožňuje rýchlo spustiť naposledy spustenú kontrolu s rovnakými nastaveniami.

V roletovom menu **Akcia po kontrole** môžete nastaviť akciu, ktorá sa má vykonať automaticky po dokončení kontroly:

- **Žiadna akcia** – po ukončení kontroly nebude vykonaná žiadna akcia.
- **Vypnúť** – počítač sa po ukončení kontroly vypne.
- **Reštartovať v prípade potreby** – počítač sa reštartuje, ak bude potrebné dokončiť liečenie zachytených hrozieb.
- **Reštartovať** – počítač po ukončení kontroly zatvorí všetky spustené programy a reštartuje sa.
- **Vynútiť reštart v prípade potreby** – počítač sa nútene reštartuje, ak bude potrebné dokončiť liečenie zachytených hrozieb.
- **Vynútiť reštart** – po ukončení kontroly sa bez interakcie s používateľom nútene zatvoria všetky spustené programy a počítač sa reštartuje.
- **Uspať** – vaša relácia bude uložená a počítač sa prepne do úsporného režimu, tak aby sa dal rýchlo zapnúť.
- **Prepnúť do režimu dlhodobého spánku** – bude uložená snímka stavu počítača a počítač sa vypne. Pri opätovnom zapnutí počítača sa načíta uložený stav.

> Možnosti **Uspať** a **Prepnúť do režimu dlhodobého spánku** sú dostupné v závislosti od nastavení napájania a režimu spánku v rámci operačného systému alebo od možností vášho počítača/laptopu. Berte na vedomie, že počítač v stave spánku je aj naďalej zapnutý. Takýto počítač má stále aktívne základné funkcie a naďalej spotrebúva elektrickú energiu, a to aj v prípade, že je napájaný z batérie. Pre šetrenie batérie, napríklad pri cestovaní mimo kancelárie, odporúčame použiť možnosť Prepnúť do režimu dlhodobého spánku.

Zvolená akcia sa spustí po dokončení všetkých prebiehajúcich kontrol. Ak ste zvolili akciu **Vypnúť** alebo **Reštartovať**, zobrazí sa dialógové okno s výzvou na potvrdenie akcie s 30sekundovým odpočítavaním, v rámci ktorého je možné plánované vypnutie/reštartovanie počítača zrušiť kliknutím na **Zrušiť**.

> Odporúčame, aby kontrola počítača prebehla aspoň raz za mesiac. Kontrola sa dá nastaviť ako jedna z plánovaných úloh v časti **Nástroje** > **Plánovač**. Ako naplánovať pravidelnú týždňovú kontrolu?

Spustenie vlastnej kontroly

Ak si želáte skontrolovať operačnú pamäť, sieťové jednotky alebo iba niektoré oblasti disku, môžete použiť nástroj Vlastná kontrola. Kliknite na **Pokročilé kontroly** > **Vlastná kontrola** a vyberte požadované ciele z adresárovej (stromovej) štruktúry.

Profil, s ktorým bude vykonaná kontrola zvolených cieľov, môžete vybrať z roletového menu **Profil**. Predvolený profil je **Smart kontrola**. Sú však dostupné aj ďalšie tri prednastavené profily: **Hĺbková kontrola**, **Kontrola z kontextového menu** a **Kontrola počítača**. Tieto profily používajú rôzne parametre ThreatSense. Dostupné možnosti nájdete v Rozšírených nastaveniach v sekcii **Detekčné jadro** > **Detekcia malvéru** > **Manuálna kontrola** > ThreatSense.

Adresárová (stromová) štruktúra tiež obsahuje konkrétne ciele kontroly.

- **Operačná pamäť** – skontrolujú sa všetky procesy a dáta aktuálne používané operačnou pamäťou.
- **Zavádzacie sektory/UEFI** – skontrolujú sa zavádzacie sektory a UEFI na prítomnosť malvéru. Viac o

kontrole UEFI sa dočítate v slovníku pojmov.

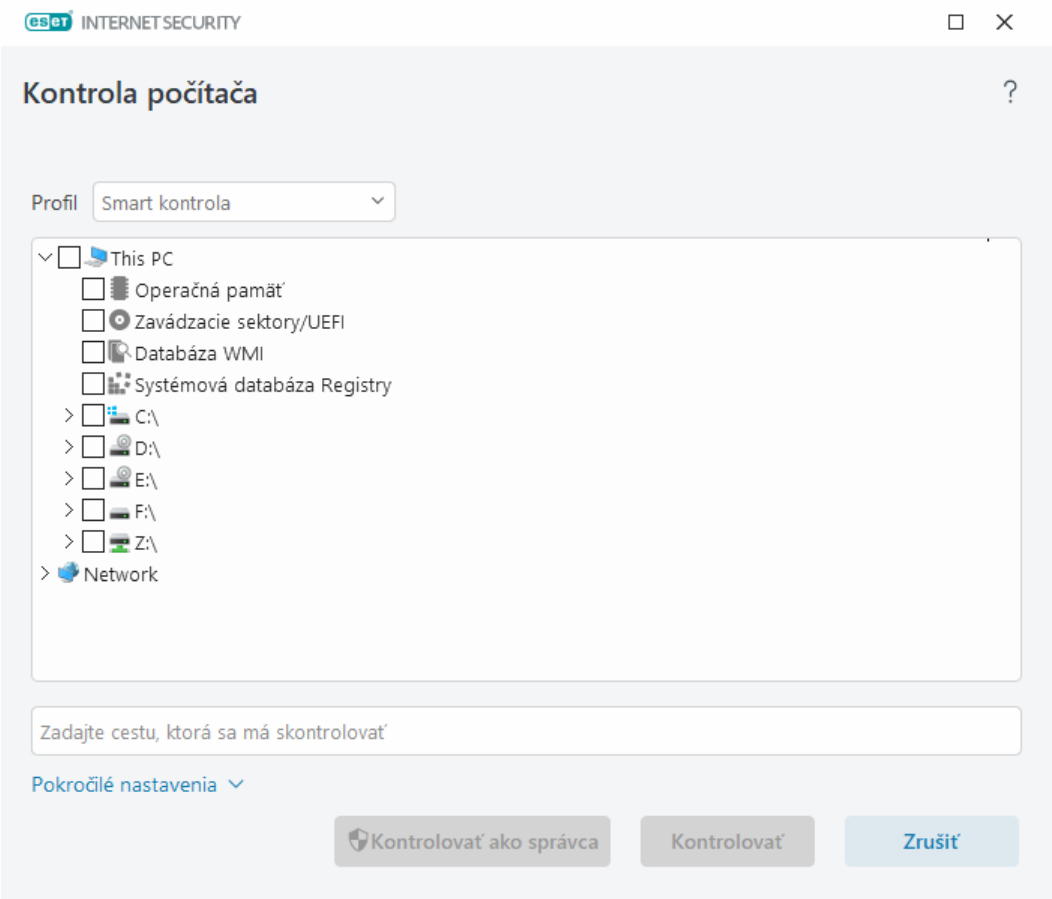
• **Databáza WMI** – skontroluje sa celá databáza služby Windows Management Instrumentation (WMI), všetky priestory názvov, inštancie triedy a vlastnosti. Vyhľadajú sa odkazy na infikované súbory alebo malvér vložený ako dáta.

• **Systémová databáza Registry** – skontroluje sa celá systémová databáza Registry, všetky kľúče a podkľúče. Vyhľadajú sa odkazy na infikované súbory alebo malvér vložený ako dáta. Pri liečení detekcie zostane v databáze Registry odkaz, aby sa zabránilo strate dôležitých dát.

Ak chcete rýchlo prejsť k požadovanému cieľu kontroly (súbor alebo priečinok), zadajte jeho cestu do textového poľa pod stromovou štruktúrou. V ceste sa rozlišujú veľké a malé písmená. Označením políčka v stromovej štruktúre pridáte daný cieľ do zoznamu cieľov, ktoré sa majú skontrolovať.

Ako naplánovať pravidelnú týždňovú kontrolu počítača

Ak chcete naplánovať pravidelnú úlohu, prečítajte si kapitolu Ako naplánovať pravidelnú týždňovú kontrolu počítača.



Parametre liečenia môžete pre danú kontrolu nastaviť v časti Rozšírené nastavenia > **Detekčné jadro** > **Detekcia malvéru** > **Manuálna kontrola** > **ThreatSense** > **Liečenie**. Na vykonanie kontroly bez liečenia kliknite na **Rozšírené nastavenia** a vyberte možnosť **Kontrolovať bez liečenia**. História kontrol sa zaznamenáva do protokolu kontroly.

Ak je vybraná možnosť **Ignorovať vylúčenia**, súbory s príponami, ktoré boli predtým vylúčené z kontroly, budú kontrolované bez výnimky.

Kliknutím na **Kontrolovať** spustíte kontrolu počítača s parametrami, ktoré ste nastavili.

Kontrolovať ako správca spúšťa kontrolu počítača pod účtom správcu. Túto možnosť je vhodné použiť, ak

prihlásený používateľ nemá dostatočné privilégia na prístup k príslušným súborom, ktoré sa majú kontrolovať. Táto možnosť nie je dostupná, ak daný používateľ nemôže vyvolať operácie UAC (kontroly používateľských kont) ako správca.

Po dokončení kontroly počítača môžete zobraziť protokol o kontrole kliknutím na Zobraziť protokol.

Priebeh kontroly

Okno priebehu kontroly ukazuje aktuálny stav kontroly a počet nájdených súborov, ktoré obsahujú škodlivý kód.

Je v poriadku, ak určité typy súborov, ako napríklad dáta chránené heslom alebo súbory využívané systémom (napr. *pagefile.sys* a niektoré súbory protokolov), nemôžu byť skontrolované. Viac informácií nájdete v našom článku Databázy znalostí.

Ako naplánovať pravidelnú týždňovú kontrolu počítača

Ak chcete naplánovať pravidelnú úlohu, prečítajte si kapitolu Ako naplánovať pravidelnú týždňovú kontrolu počítača.

Priebeh kontroly – indikátor priebehu zobrazuje stav prebiehajúcej kontroly.

Cieľ – názov aktuálne kontrolovaného súboru a jeho umiestnenie.

Počet detekcií – zobrazuje celkový počet skontrolovaných súborov, nájdených hrozieb či hrozieb vyliečených počas kontroly.

Kliknutím na položku Viac informácií sa zobrazia nasledujúce informácie:

- **Používateľ** – názov používateľského účtu, ktorý spustil kontrolu.
- **Skontrolované objekty** – počet už skontrolovaných objektov.
- **Trvanie** – uplynulý čas.

Ikona Pozastaviť – pozastavenie kontroly.

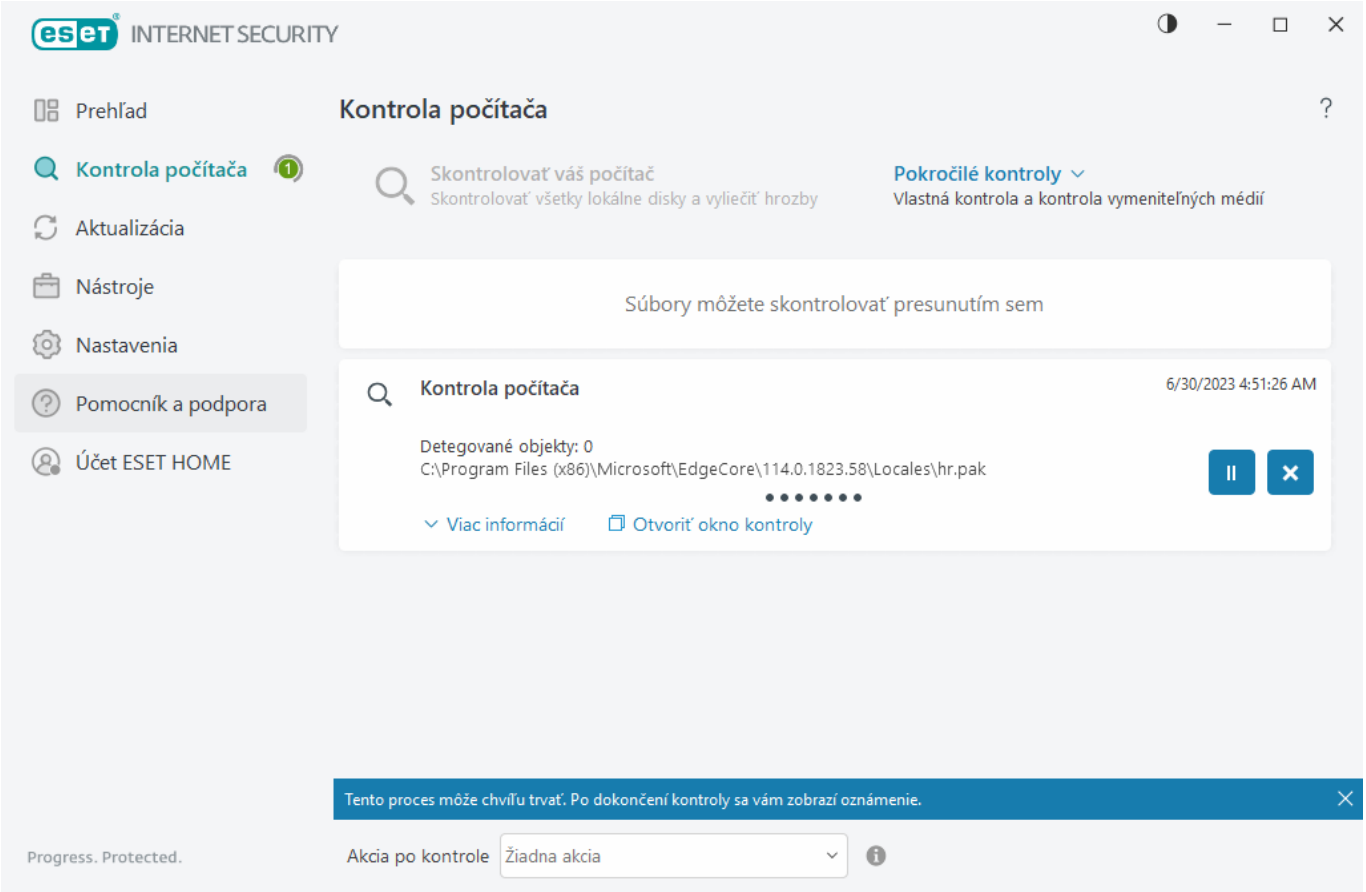
Ikona Pokračovať – táto možnosť sa zobrazí po pozastavení kontroly. Kliknutím na ikonu pokračujte v kontrole.

Ikona Zastaviť – ukončenie kontroly.

Kliknutím na možnosť **Otvoriť okno kontroly** otvoríte protokol o kontrole počítača s podrobnejšími informáciami o danej kontrole.

Rolovanie výpisu protokolu o kontrole – po zapnutí tejto možnosti uvidíte v okne kontroly vždy tie najnovšie záznamy o práve skontrolovaných objektoch.

Po kliknutí na možnosť Viac informácií alebo Otvoriť okno kontroly sa zobrazia podrobnosti o kontrole počítača, ktorá je práve spustená. Ďalšiu súbežnú kontrolu môžete spustiť kliknutím na možnosť **Skontrolovať váš počítač** alebo **Pokročilé kontroly** > **Vlastná kontrola**.



V roletovom menu **Akcia po kontrole** môžete nastaviť akciu, ktorá sa má vykonať automaticky po dokončení kontroly:

- **Žiadna akcia** – po ukončení kontroly nebude vykonaná žiadna akcia.
- **Vypnúť** – počítač sa po ukončení kontroly vypne.
- **Reštartovať v prípade potreby** – počítač sa reštartuje, ak bude potrebné dokončiť liečenie zachytených hrozieb.
- **Reštartovať** – počítač po ukončení kontroly zatvorí všetky spustené programy a reštartuje sa.
- **Vynútiť reštart v prípade potreby** – počítač sa nútene reštartuje, ak bude potrebné dokončiť liečenie zachytených hrozieb.
- **Vynútiť reštart** – po ukončení kontroly sa bez interakcie s používateľom nútene zatvoria všetky spustené programy a počítač sa reštartuje.
- **Uspať** – vaša relácia bude uložená a počítač sa prepne do úsporného režimu, tak aby sa dal rýchlo zapnúť.
- **Prepnúť do režimu dlhodobého spánku** – bude uložená snímka stavu počítača a počítač sa vypne. Pri opätovnom zapnutí počítača sa načíta uložený stav.

Možnosti **Uspať** a **Prepnúť do režimu dlhodobého spánku** sú dostupné v závislosti od nastavení napájania a režimu spánku v rámci operačného systému alebo od možností vášho počítača/laptopu. Berte na vedomie, že počítač v stave spánku je aj naďalej zapnutý. Takýto počítač má stále aktívne základné funkcie a naďalej spotrebúva elektrickú energiu, a to aj v prípade, že je napájaný z batérie. Pre šetrenie batérie, napríklad pri cestovaní mimo kancelárie, odporúčame použiť možnosť Prepnúť do režimu dlhodobého spánku.

Zvolená akcia sa spustí po dokončení všetkých prebiehajúcich kontrol. Ak ste zvolili akciu **Vypnúť** alebo **Reštartovať**, zobrazí sa dialógové okno s výzvou na potvrdenie akcie s 30‑sekundovým odpočítavaním, v rámci ktorého je možné plánované vypnutie/reštartovanie počítača zrušiť kliknutím na **Zrušiť**.

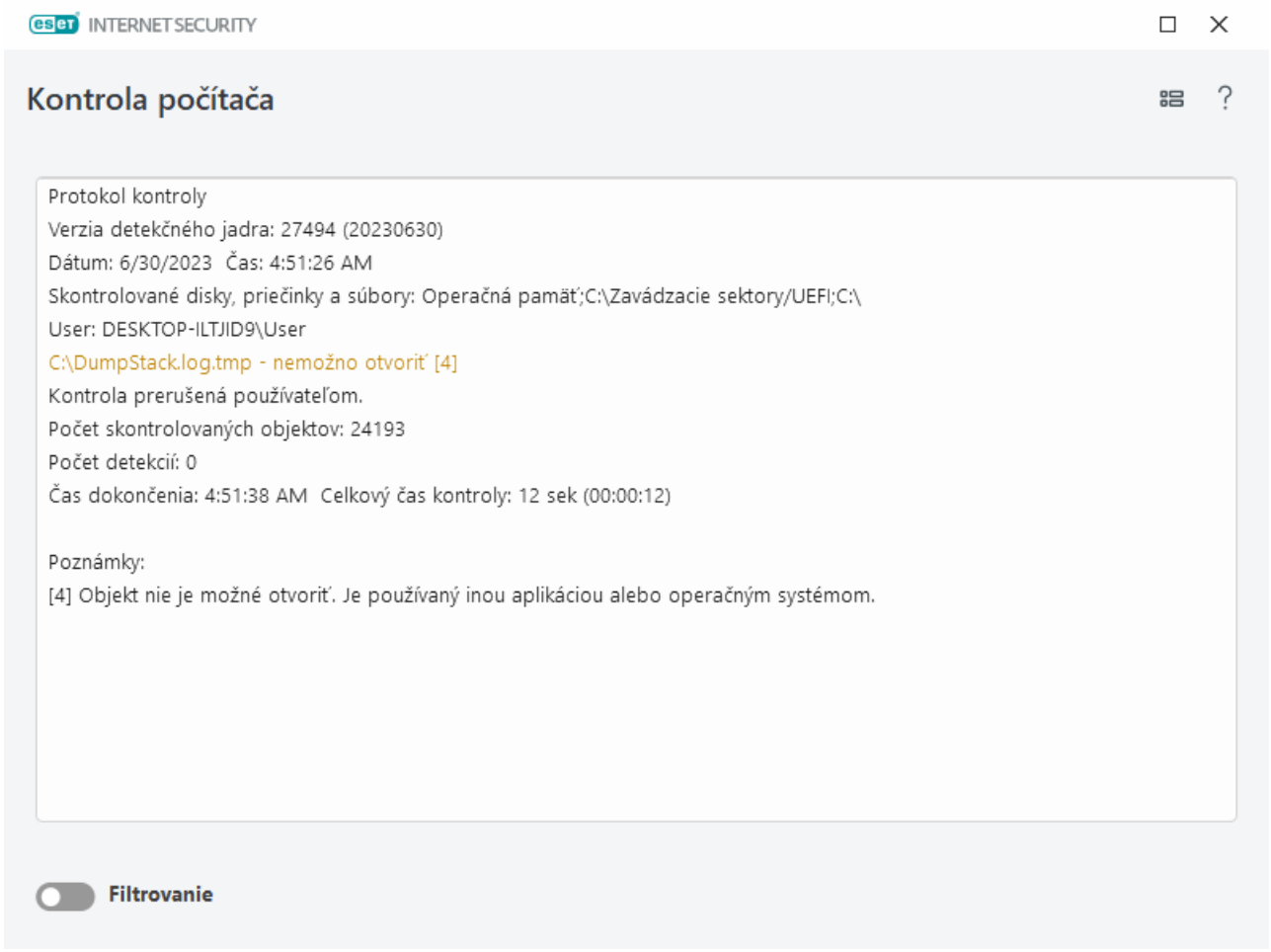
Protokol o kontrole počítača

Podrobné informácie týkajúce sa konkrétnej kontroly môžete zobraziť v Protokoloch. Protokol kontroly obsahuje nasledujúce informácie:

- Verzia detekčného jadra
- Dátum a čas spustenia kontroly
- Zoznam skontrolovaných diskov, priečinkov a súborov
- Názov plánovanej kontroly (iba pri plánovaných kontrolách)
- Používateľ, ktorý spustil kontrolu
- Stav kontroly
- Počet skontrolovaných objektov
- Počet detekcií
- Čas ukončenia kontroly
- Celkový čas kontroly

Nové spustenie plánovanej kontroly počítača sa preskočí, ak stále prebieha rovnaká plánovaná úloha, ktorá bola spustená už skôr. Vynechaná úloha plánovanej kontroly vytvorí protokol kontroly počítača s nulovým počtom skontrolovaných objektov a stavom **Kontrola sa nespustila, pretože stále prebiehala predchádzajúca kontrola**.

Ak si chcete pozrieť predchádzajúce protokoly kontroly, v hlavnom okne programu kliknite na **Nástroje** > **Protokoly**. V roletovom menu vyberte možnosť **Kontrola počítača** a dvakrát kliknite na požadovaný záznam.



Viac informácií o záznamoch „nemožno otvoriť“, „chyba pri otváraní“ alebo „poškodený archív“ nájdete v našom článku Databázy znalostí.

Kliknutím na ikonu prepínača **Filtrovanie** otvoríte okno Filtrovanie protokolov, kde môžete spresniť vyhľadávanie podľa vlastných kritérií. Ak chcete zobraziť kontextové menu, kliknite pravým tlačidlom myši na konkrétnu položku protokolu:

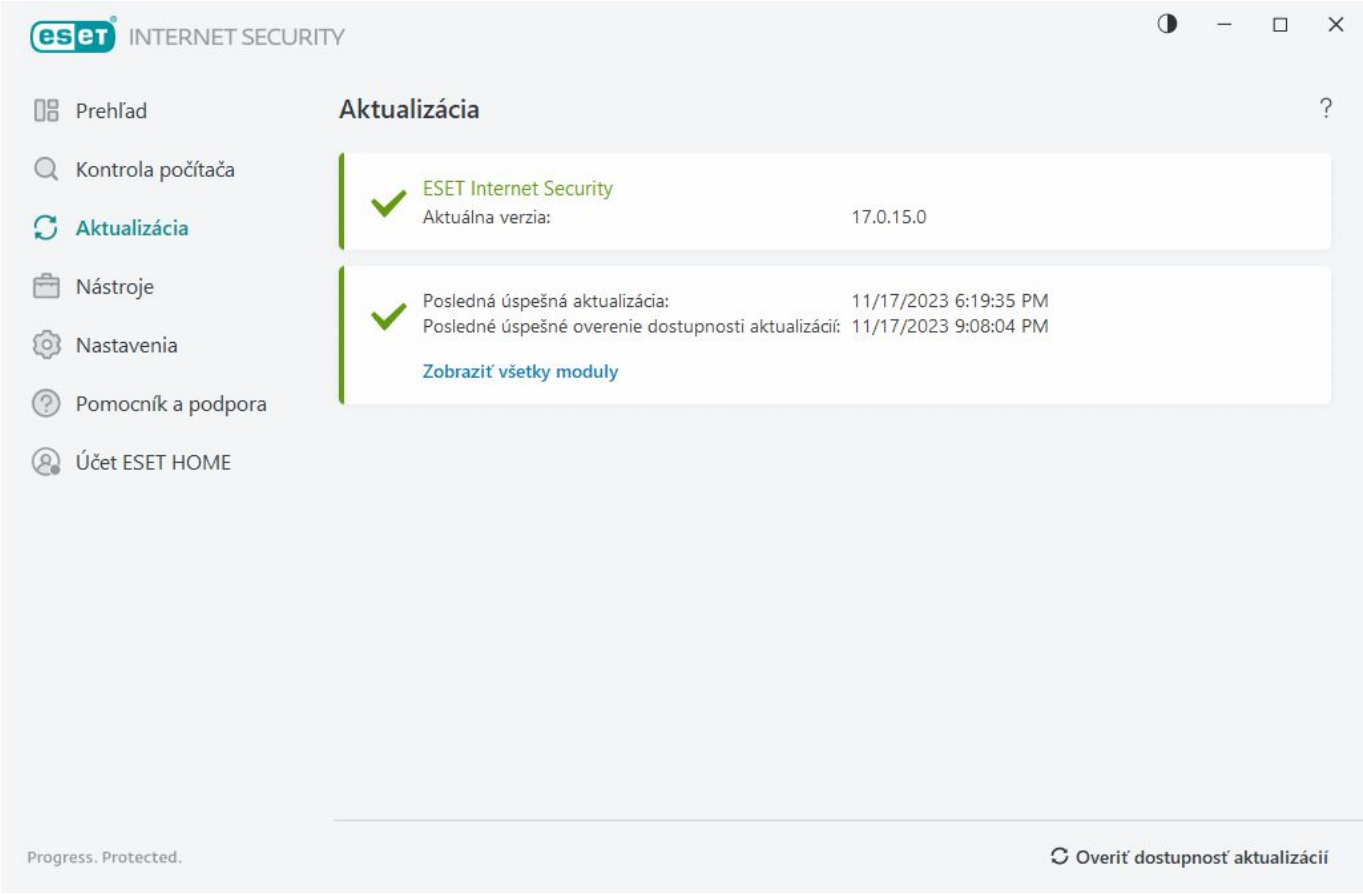
Akcia	Použitie
Filtrovať rovnaké záznamy	Aktivuje filtrovanie protokolov. V protokole budú zobrazené iba záznamy rovnakého typu, ako je zvolený protokol.
Filter	Po kliknutí na túto možnosť môžete v okne Filtrovanie protokolov definovať kritériá filtrovania pre konkrétne položky protokolu. Klávesová skratka `Ctrl+Shift+F`
Zapnúť filter	Aktivuje nastavenia filtra. Ak filter aktivujete prvýkrát, musíte definovať nastavenia v okne Filtrovanie protokolov.
Vypnúť filter	Vypne filter (rovnako ako prepínač naspodku).
Kopírovať	Skopíruje označený záznam do schránky. Klávesová skratka: `Ctrl+C`
Kopírovať všetko	Skopíruje všetky záznamy v okne.
Exportovať	Exportuje označený záznam do súboru XML.
Exportovať všetko	Exportuje všetky záznamy v okne do súboru XML.
Popis detekcie	Otvorí ESET Encyklopédiu hrozieb s podrobnými informáciami o označenej infiltrácii vrátane prejavov jej prítomnosti v systéme a bezpečnostných hrozieb, ktoré sa s ňou spájajú.

Aktualizácia

Pravidelná aktualizácia programu ESET Internet Security je základným predpokladom pre zaistenie maximálnej úrovne ochrany vášho počítača. Modul aktualizácie zabezpečuje, aby bol program vždy aktuálny, a to z hľadiska jednotlivých programových, ako aj systémových súčastí.

V sekcii **Aktualizácia** v hlavnom okne programu je zobrazený aktuálny stav aktualizácie vrátane informácie o dátume a čase poslednej úspešnej aktualizácie, prípadne aj o dostupnosti novej aktualizácie.

Popri automatických aktualizáciách môžete kedykoľvek použiť tlačidlo **Overiť dostupnosť aktualizácií** na manuálne spustenie aktualizácie. Pravidelné aktualizovanie programových modulov a súčastí je z pohľadu zaistenia komplexnej ochrany pred škodlivým kódom nevyhnutnosťou. Nastaveniu a funkčnosti aktualizácií preto treba venovať zvýšenú pozornosť. Bezpečnostný produkt ESET môže dostávať aktualizácie až po jeho aktivovaní pomocou aktivačného kľúča. Ak ste svoje licenčné údaje nezadali počas inštalácie, budete musieť ESET Internet Security aktivovať dodatočne, aby ste zabezpečili prístup k aktualizačným serverom spoločnosti ESET. Váš aktivačný kľúč vám bol zaslaný na vašu e-mailovú adresu po zakúpení produktu ESET Internet Security.



Aktuálna verzia – zobrazuje číslo verzie produktu, ktorú máte aktuálne nainštalovanú.

Posledná úspešná aktualizácia – zobrazuje dátum, keď sa program naposledy úspešne aktualizoval. Ak nie je zobrazený aktuálny dátum, programové moduly môžu byť zastarané.

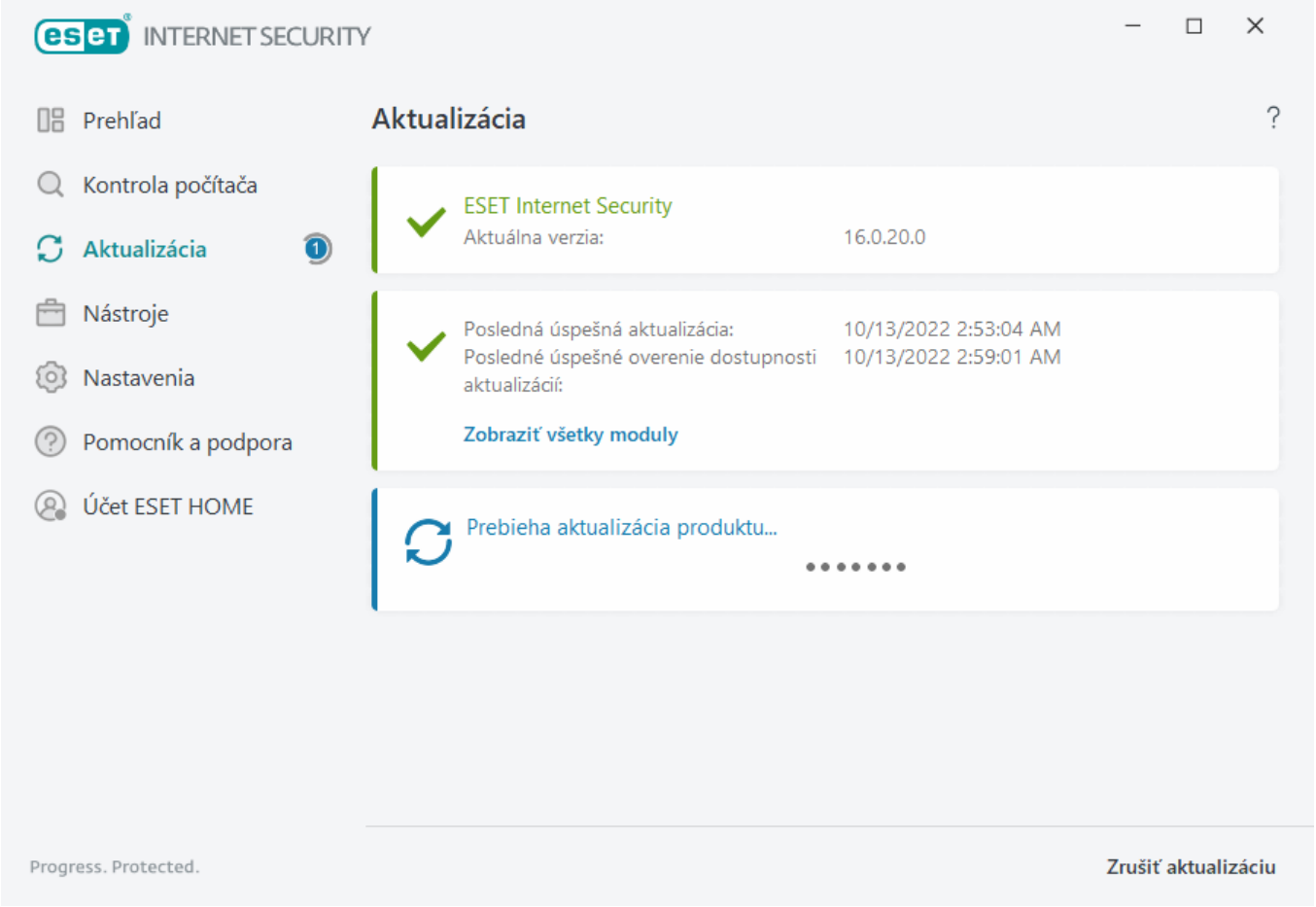
Posledné úspešné overenie dostupnosti aktualizácií – zobrazuje dátum, keď bola naposledy úspešne skontrolovaná dostupnosť aktualizácií.

Zobraziť všetky moduly – zobrazuje zoznam nainštalovaných programových modulov.

Po kliknutí na **Overiť dostupnosť aktualizácií** program skontroluje, či nie je k dispozícii novšia verzia ESET Internet Security.

Priebeh aktualizácie

Po kliknutí na **Overiť dostupnosť aktualizácií** sa spustí proces sťahovania aktualizácie. Zároveň sa zobrazí indikátor priebehu sťahovania a zostávajúci čas do konca procesu. Ak chcete aktualizáciu zastaviť, môžete kliknúť na tlačidlo **Zrušiť aktualizáciu**.



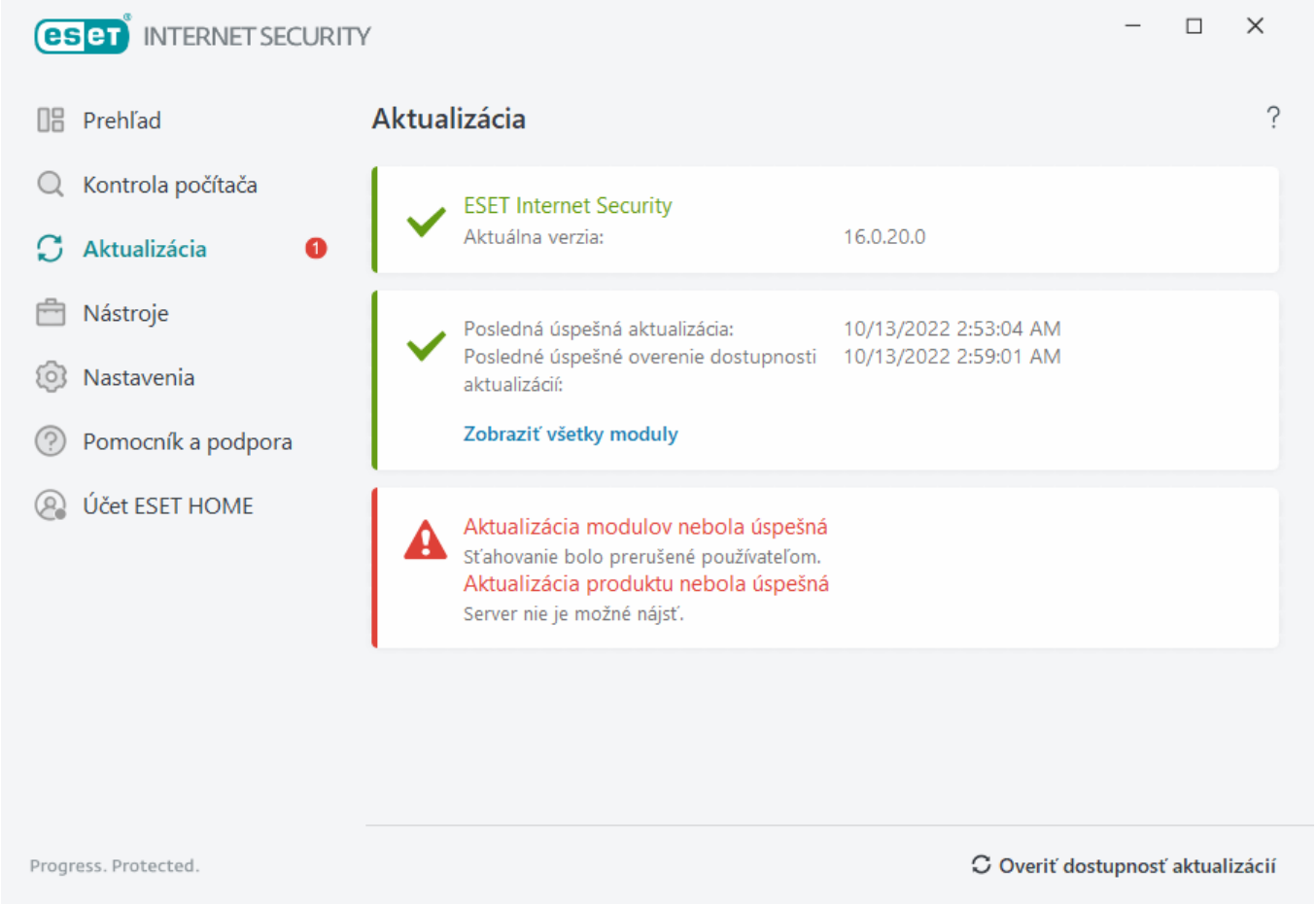
Za normálnych okolností v okne **Aktualizácia** uvidíte zelený symbol, ktorý označuje, že program je aktuálny. Ak tomu tak nie je, program nie je aktualizovaný a zvyšuje sa riziko napadnutia škodlivým kódom. Odporúčame vám v takomto prípade programové moduly čo najskôr aktualizovať.

Neúspešná aktualizácia

Ak sa vám zobrazí správa o neúspešnej aktualizácii modulov, zlyhanie aktualizácie môže byť zapríčinené nasledujúcimi problémami:

1. **Neplatné predplatné** – predplatné použité na aktiváciu je neplatné alebo mu platnosť uplynula. V hlavnom okne programu kliknite na **Pomocník a podpora** > **Zmeniť predplatné** a aktivujte svoj produkt iným predplatným.

2. **Pri sťahovaní aktualizačných súborov nastala chyba** – najčastejšou príčinou je nesprávne nastavenie internetového pripojenia. Odporúčame, aby ste skontrolovali pripojenie na internet (otvorením akejkoľvek webovej stránky v internetovom prehliadači). Ak sa webová stránka nenačíta, počítač pravdepodobne nie je pripojený na internet alebo má problémy s pripojením. Uistite sa tiež, že váš poskytovateľ internetových služieb nemá výpadok pripojenia.



Po úspešnej aktualizácii programu ESET Internet Security na novšiu verziu je nutné reštartovať počítač, aby ste zaistili, že všetky programové moduly sú správne aktualizované. Pri bežnej pravidelnej aktualizácii produktu nie je reštart počítača potrebný.

Viac informácií nájdete v nasledujúcom článku databázy znalostí spoločnosti ESET: Čo robiť, ak aktualizácia modulov nebola úspešná a skončila chybou.

Dialógové okno – Vyžaduje sa reštart

Po aktualizácii produktu ESET Internet Security na novú verziu je potrebný reštart počítača. Nové verzie ESET Internet Security sú vydávané s cieľom priniesť opravy chýb a vylepšenia produktu, ktoré nie je možné zahrnúť do automatickej aktualizácie programových modulov.

Novú verziu ESET Internet Security je možné nainštalovať automaticky na základe nastavenia aktualizácie programu alebo manuálne stiahnutím a nainštalovaním novšej verzie cez starú verziu.

Kliknutím na možnosť **Reštartovať teraz** reštartujte počítač. Ak plánujete počítač reštartovať neskôr, kliknite na možnosť **Pripomenúť neskôr**. Neskôr môžete počítač reštartovať manuálne z obrazovky **Prehľad** v hlavnom okne programu.

Vytvorenie aktualizačnej úlohy

Aktualizáciu môžete spustiť manuálne kliknutím na tlačidlo **Overiť dostupnosť aktualizácií** na záložke **Aktualizácia** v hlavnom okne programu.

Aktualizácie sa dajú spúšťať aj ako plánované úlohy. Tie možno nastaviť po kliknutí na **Nástroje** > **Plánovač**.
V programe ESET Internet Security sú predvolene aktivované nasledujúce aktualizačné úlohy:

- **Pravidelná automatická aktualizácia**
- **Automatická aktualizácia po prihlásení používateľa**

Každú z vyššie uvedených aktualizačných úloh môžete upravovať podľa vašich potrieb. Okrem predvolených aktualizačných úloh môžete vytvoriť nové plánované úlohy s vlastným nastavením. Podrobnejšie sa vytváraním a nastaveniami aktualizačných úloh zaoberá kapitola Plánovač.

Nástroje

Menu **Nástroje** obsahuje funkcie, ktoré ponúkajú dodatočné zabezpečenie a pomáhajú zjednodušiť správu programu ESET Internet Security. K dispozícii sú tieto nástroje:

 Protokoly

 Spustené procesy (ak je v ESET Internet Security povolený ESET LiveGrid®)

 Správa o bezpečnosti

 Sieťové pripojenia (ak je v ESET Internet Security povolený Firewall)

 ESET SysInspector

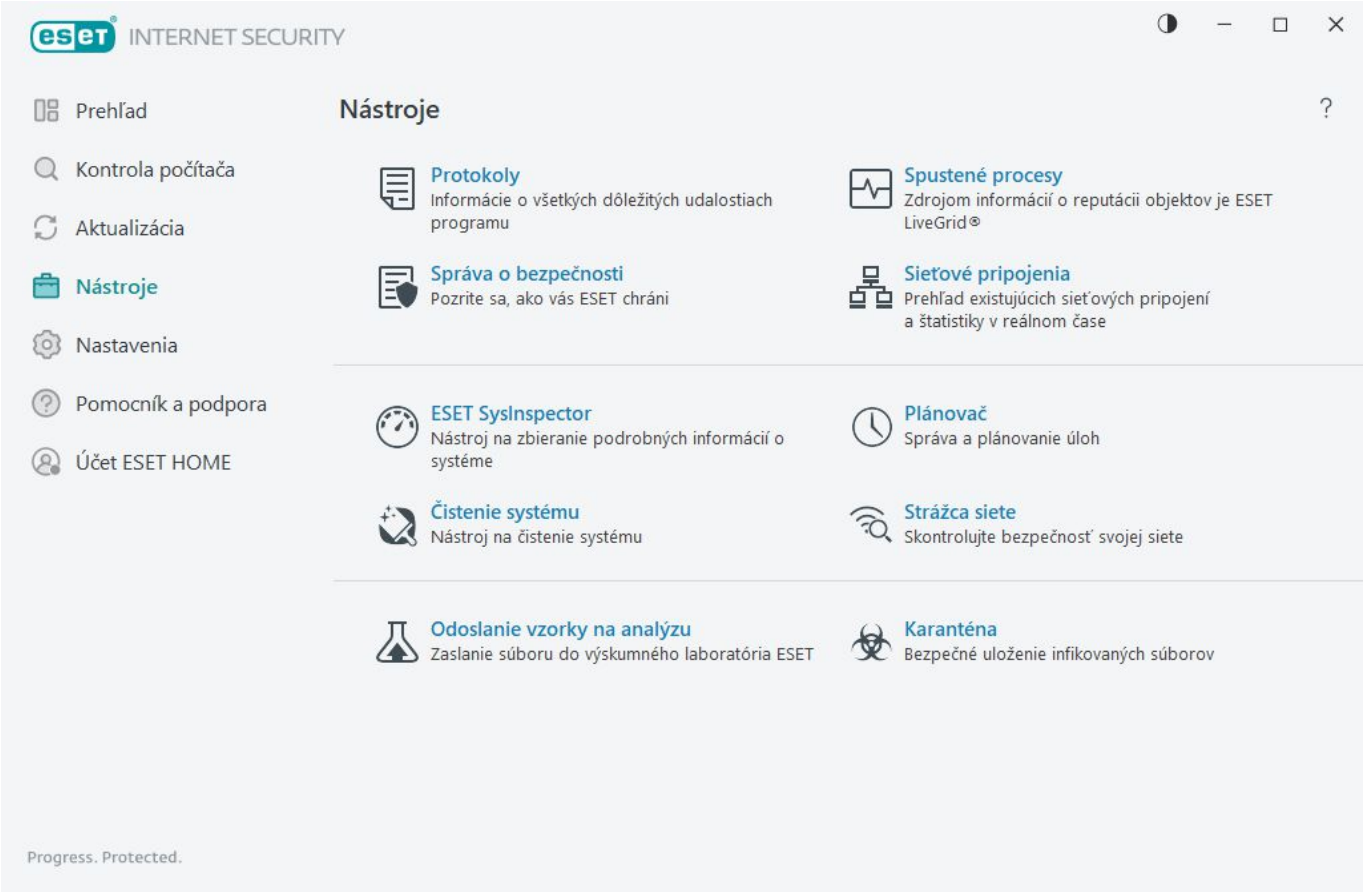
 Plánovač

 Čistenie systému

 Strážca siete

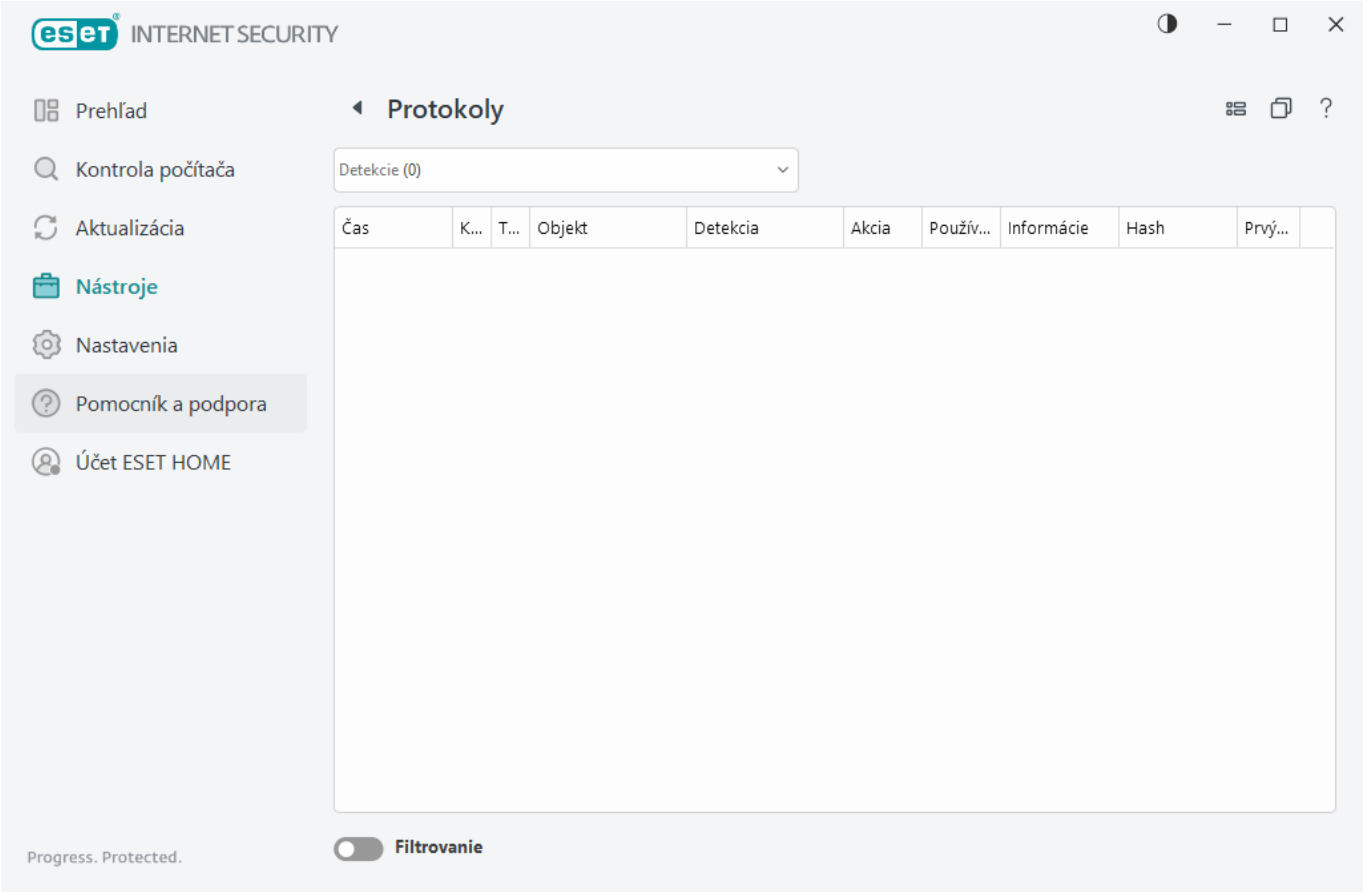
 Odoslanie vzorky na analýzu (dostupnosť závisí od vašej konfigurácie ESET LiveGrid®)

 Karanténa



Protokoly

Protokoly obsahujú informácie o dôležitých udalostiach v programe a poskytujú prehľad o odhalených hrozbách. Protokoly predstavujú silný nástroj systémovej analýzy, odhaľovania problémov a rizík a v neposlednom rade hľadania riešení. Vytváranie protokolov prebieha aktívne na pozadí bez akejkoľvek interakcie zo strany používateľa. Informácie sú zaznamenávané na základe nastavenej úrovne podrobnosti zápisu do protokolov. Textové správy a protokoly je možné prezerať či archivovať priamo z prostredia ESET Internet Security.



Protokoly sú dostupné z hlavného okna programu po kliknutí na **Nástroje** > **Protokoly**. Z roletového menu vyberte požadovaný typ protokolu:

- **Detekcie** – tento protokol ponúka podrobné informácie týkajúce sa detekcií a infiltrácií zachytených produktom ESET Internet Security. Informácie v protokoloch zahŕňajú čas detekcie, typ kontroly, typ objektu, umiestnenie objektu, názov detekcie, vykonanú akciu, meno používateľa prihláseného v čase detekcie, hash a prvý výskyt. Nevyliečené infiltrácie sú vždy označené červeným textom na svetločervenom pozadí. Vyliečené infiltrácie sú označené žltým textom na bielom pozadí. Nevyliečené potenciálne nebezpečné a nechcené aplikácie sú označené žltým textom na bielom pozadí.

- **Udalosti** – v tomto protokole sú zaznamenané všetky dôležité operácie vykonané programom ESET Internet Security. Protokol udalostí obsahuje informácie o udalostiach a chybách v programe. Je navrhnutý pre systémových správcov a používateľov na riešenie problémov. Informácie získané z tohto protokolu vám často pomôžu nájsť príčiny problémov, prípadne ich riešenie.

- **Kontrola počítača** – výsledky všetkých vykonaných kontrol sú zobrazené v tomto okne. Každý riadok prináleží samostatnej kontrole. Dvojitým kliknutím na akúkoľvek položku protokolu zobrazíte podrobnosti príslušnej kontroly.

- **HIPS** – tento protokol obsahuje záznamy konkrétnych pravidiel systému HIPS označených na zaznamenávanie. V protokole je zobrazená aplikácia, ktorá danú operáciu vyvolala, a následne výsledok (tzn. či bolo pravidlo povolené alebo zakázané) a názov pravidla.

- **Ochrana prehliadača** – obsahuje záznamy o neoverených/nedôveryhodných súboroch načítaných v prehliadači.

- **Ochrana siete** – v protokole ochrany siete sú zobrazené všetky vzdialené útoky zachytené Firewallom, Ochranou pred sieťovými útokmi (IDS) a Ochranou pred botnetmi. Tu nájdete informácie o všetkých útokoch

na váš počítač. V stĺpci Udalosť je typ zisteného útoku. V stĺpci Zdroj sú podrobnejšie informácie o útočníkovi. V stĺpci Protokol je uvedený komunikačný protokol použitý pri útoku. Analýzou tohto protokolu ochrany siete je možné včas odhaliť pokusy o prienik do systému. Viac informácií o sieťových útokoch nájdete v kapitole IDS a pokročilé možnosti.

- **Filtrované stránky** – tento zoznam je užitočný v prípade, ak si želáte zobraziť webové stránky, ktoré boli blokované modulom Ochrana prístupu na web alebo modulom Rodičovská kontrola. Každý protokol obsahuje čas, URL adresu, používateľa a aplikáciu, ktorá vytvorila spojenie s konkrétnou webovou stránkou.

- **Antispamová ochrana e-mailových klientov** – obsahuje záznamy súvisiace s e-mailovými správami, ktoré boli označené ako spam.

- **Rodičovská kontrola** – obsahuje webové stránky, ktoré boli blokované alebo povolené Rodičovskou kontrolou. Stĺpce Typ vyhodnotenia a Hodnota vyhodnotenia hovoria o tom, ako boli aplikované filtrovacie pravidlá.

- **Správa zariadení** – záznamy o vymeniteľných médiách alebo zariadeniach, ktoré boli pripojené k počítaču. V protokole sú zaznamenané len zariadenia s vytvoreným pravidlom v rámci Správy zariadení. Ak sa na pripojené zariadenie nevzťahuje žiadne pravidlo, záznam v protokole sa pre zariadenie nevytvorí. Môžete tu tiež vidieť podrobnosti o zariadeniach, ako napríklad typ zariadenia, sériové číslo, výrobcu, model a prípadne veľkosť pamäte média.

- **Ochrana webovej kamery** – obsahuje záznamy o aplikáciách blokovaných Ochranou webovej kamery.

Označte obsah akéhokoľvek protokolu a stlačením klávesovej kombinácie **CTRL + C** ho skopírujte do schránky. Viacero položiek môžete označiť podržaním klávesu **CTRL** alebo **SHIFT**.

Kliknite na **Filtrovanie**. Otvorí sa okno Filtrovanie protokolov, kde môžete nastaviť podmienky filtrovania zoznamu protokolov.

Kliknite pravým tlačidlom na konkrétny záznam pre otvorenie kontextového menu. V kontextovom menu sú dostupné nasledujúce možnosti:

- **Zobraziť** – zobrazia sa podrobnejšie informácie o označenom protokole v novom okne.

- **Filtrovať rovnaké záznamy** – po aktivácii tohto filtra sa zobrazia protokoly rovnakého typu (diagnostické, varovania atď.).

- **Filtrovať** – po kliknutí na túto možnosť môžete v okne Filtrovanie protokolov definovať kritériá filtrovania pre konkrétne položky protokolu.

- **Zapnúť filter** – zapne filter, ktorý ste nastavili v okne Filtrovanie protokolov.

- **Zrušiť filter** – vypne aktivovaný filter.

- **Kopírovať/Kopírovať všetko** – skopíruje informácie o vybraných protokoloch.

- **Kopírovať bunku** – skopíruje obsah bunky, na ktorú ste klikli pravým tlačidlom myši.

- **Odstrániť/Odstrániť všetko** – odstráni označené alebo všetky zobrazené protokoly. Na vykonanie tejto akcie sú potrebné práva správcu.

- **Exportovať/Exportovať všetko** – exportuje informácie o označených alebo všetkých protokoloch vo

formáte XML.

• **Hľadať/Hľadať ďalší/Hľadať predošlý** – po kliknutí na túto možnosť môžete v okne Filtrovanie protokolov definovať kritériá filtrovania pre konkrétne položky protokolu.

• **Popis detekcie** – otvorí ESET Encyklopédiu hrozieb s podrobnými informáciami o zachytenej infiltrácii vrátane prejavov jej prítomnosti v systéme a bezpečnostných hrozieb, ktoré sa s ňou spájajú.

• **Vytvoriť vylúčenie** – umožňuje vytvoriť nové vylúčenie detekcie pomocou sprievodcu (táto možnosť nie je dostupná pre detekcie malvéru).

• **Pridať na zoznam povolených položiek ochrany prehliadača** – otvorí okno Zoznam povolených položiek ochrany prehliadača a pridá novú položku do zoznamu.

Filtrovanie protokolov

Na definovanie kritérií filtrovania kliknite na **Filtrovanie** v sekcii **Nástroje** > **Protokoly**.

Funkcia filtrovania protokolov vám pomôže nájsť informácie, ktoré hľadáte, a to najmä v prípade, ak sa v protokoloch nachádza veľký počet záznamov. Umožňuje vám zúžiť záznamy protokolov napríklad vtedy, keď hľadáte konkrétny typ udalosti, stav alebo časové obdobie. Záznamy protokolov môžete filtrovať použitím konkrétnych možností vyhľadávania. V okne Protokoly sa následne zobrazia len tie záznamy, ktoré zodpovedajú zadaným kritériám vyhľadávania.

Do poľa **Hľadať text** zadajte kľúčové slovo, ktoré chcete vyhľadať. Pre upresnenie vyhľadávania použite roletové menu **Hľadať v stĺpcoch**. V roletovom menu **Typy záznamov** vyberte jeden alebo viacero záznamov. Upresnite **Časové obdobie**, pre ktoré chcete zobraziť výsledky. Môžete použiť aj ďalšie možnosti vyhľadávania, ako napr. **Hľadať iba celé slová** alebo **Rozlišovať veľké a malé písmená**.

Hľadať text

Zadajte reťazec (slovo alebo časť slova). Zobrazia sa iba záznamy, ktoré obsahujú tento reťazec. Ostatné záznamy budú vynechané.

Hľadať v stĺpcoch

Vyberte stĺpce, ktoré budú pri vyhľadávaní brané do úvahy. Môžete označiť jeden alebo viacero stĺpcov.

Typy záznamov

Z roletového menu vyberte jeden alebo viacero typov záznamov:

• **Diagnostické** – zaznamenávané budú informácie dôležité pre ladenie programu, ako aj všetky udalosti s vyššou závažnosťou.

• **Informatívne** – zaznamenávané budú informatívne správy, napríklad o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.

• **Varovania** – zaznamenávané budú varovné správy a kritické chyby.

- **Chyby** – zaznamenávané budú chyby typu „Chyba pri preberaní súboru“ a kritické chyby.
- **Kritické** – zaznamenávané budú len kritické chyby (nespustenie antivírusovej ochrany).

Časové obdobie

Zadajte časové obdobie, pre ktoré chcete zobraziť výsledky:

- **Nešpecifikované** (predvolené) – vyhľadávanie nebude vykonané pre konkrétne časové obdobie, ale bude prehľadaný celý protokol.
- **Posledný deň**
- **Posledný týždeň**
- **Posledný mesiac**
- **Vlastné** – môžete nastaviť konkrétne časové obdobie (od – do), v ktorom chcete filtrovať záznamy.

Hľadať iba celé slová

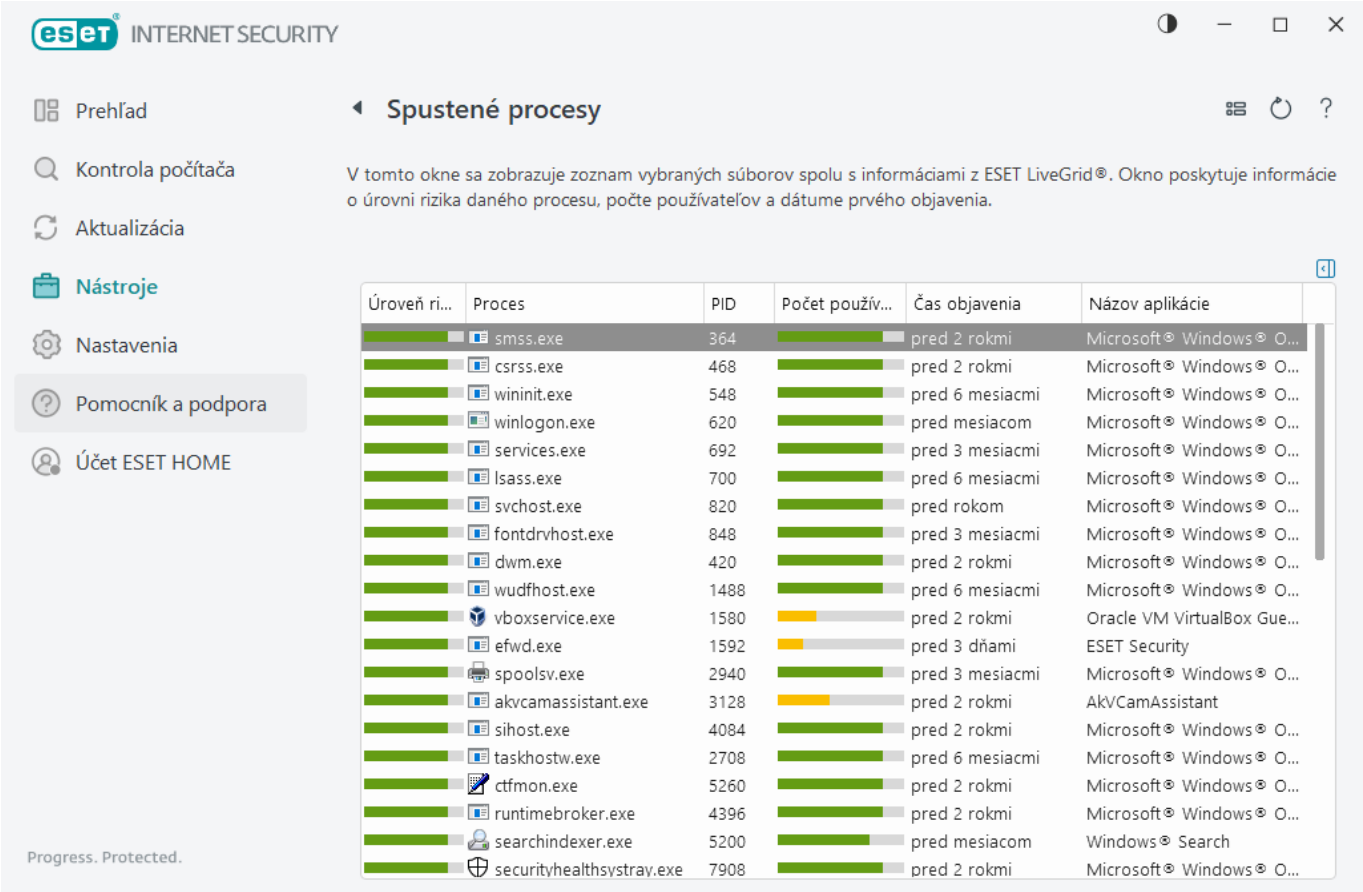
Túto možnosť použite v prípade, ak si želáte vyhľadávať celé slová a zobraziť tak presnejšie výsledky.

Rozlišovať veľké a malé písmená

Túto možnosť použite v prípade, ak je pri filtrovaní dôležité rozlišovať veľké a malé písmená. Po nastavení filtrovania/vyhľadávania kliknite na **OK** pre zobrazenie filtrovaných záznamov protokolu, prípadne kliknite na **Hľadať** pre spustenie vyhľadávania. Protokoly sú prehľadávané zhora nadol, počnúc vašou aktuálnou pozíciou (záznam, ktorý je zvýraznený). Vyhľadávanie sa zastaví pri nájdení prvého zodpovedajúceho záznamu. Stlačením **F3** vyhľadáte ďalší záznam, prípadne kliknite pravým tlačidlom myši a vyberte možnosť **Hľadať** pre upresnenie vyhľadávania.

Spustené procesy

Okno Spustené procesy zobrazuje programy a procesy, ktoré sú spustené vo vašom počítači. Umožňuje tiež, aby bola spoločnosť ESET pohotovo a neustále informovaná o nových infiltráciách. Pri povolenej technológii ESET LiveGrid® ESET Internet Security poskytuje podrobné informácie o spustených procesoch s cieľom chrániť používateľov.



Úroveň rizika – vo väčšine prípadov ESET Internet Security pomocou technológie ESET LiveGrid® priradí objektom (súborom, procesom, kľúčom registra atď.) určitý stupeň rizika na základe heuristických pravidiel, ktoré preskúmajú každý objekt a vyhodnotia pravdepodobnosť nebezpečnej aktivity. Podľa výsledkov heuristiky sa objektom pridelí úroveň rizika od 1 – v poriadku (zelenou farbou) až po 9 – riziko (červenou farbou).

Proces – názov aplikácie alebo procesu, ktorý je momentálne spustený na počítači. Pre lepší prehľad o všetkých procesoch použite Správcu úloh (MS Windows). Správcu úloh môžete otvoriť kliknutím pravým tlačidlom myši kdekoľvek na systémovom paneli úloh a vybratím možnosti **Spustiť správcu úloh**, prípadne pomocou klávesovej skratky **Ctrl** + **Shift** + **Esc**.

Známe aplikácie označené zelenou farbou nepredstavujú riziko a sú bezpečné. Budú preto vyňaté z kontroly, čím sa zvyšuje výkon a rýchlosť kontroly.

PID – číslo identifikátora procesu môže byť použité ako parameter napr. pri upravovaní priority daného procesu.

Počet používateľov – počet používateľov, ktorí používajú danú aplikáciu. Tieto informácie sú zhromažďované pomocou technológie ESET LiveGrid®.

Čas objavenia – čas, ktorý uplynul od prvého zachytenia aplikácie technológiou ESET LiveGrid®.

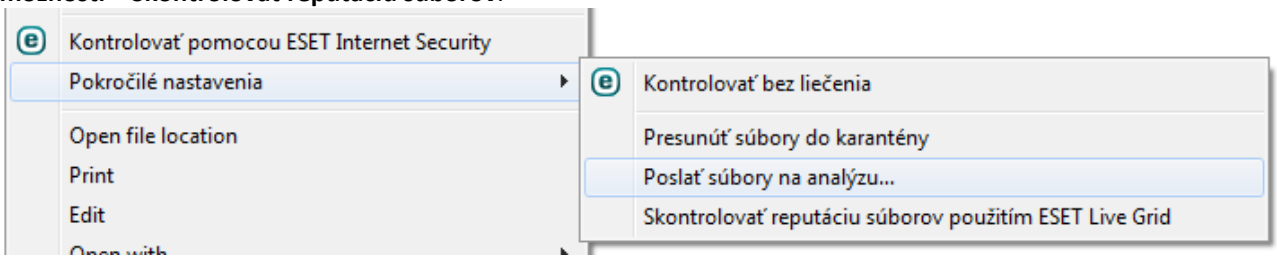
Aj v prípade, že je aplikácia označená ako Neznáma (oranžová), nemusí to znamenať, že obsahuje škodlivý kód. Obvykle je to nová aplikácia. Ak si nie je používateľ istý, či je tomu skutočne tak, má možnosť poslať vzorku na analýzu do výskumného laboratória spoločnosti ESET. Ak sa ukáže, že ide o nebezpečnú aplikáciu, jej detekcia bude pridaná v niektorej najbližšej aktualizácii.

Názov aplikácie – názov aplikácie alebo procesu.

Po kliknutí na jednotlivé aplikácie sa v dolnej časti okna zobrazia nasledovné informácie:

- **Cesta** – umiestnenie aplikácie vo vašom počítači.
- **Veľkosť** – veľkosť v kB (kilobajtoch) alebo MB (megabajtoch).
- **Popis** – charakteristika súboru vychádzajúca z popisu daného súboru operačným systémom.
- **Spoločnosť** – názov vydavateľa aplikácie alebo procesu.
- **Verzia** – táto informácia pochádza od vydavateľa aplikácie alebo procesu.
- **Produkt** – názov aplikácie, zvyčajne obchodné meno.
- **Vytvorené/upravené** – dátum a čas vytvorenia (úpravy).

Reputáciu môžete skontrolovať aj pri súboroch, ktoré sa nesprávajú ako spustené programy/procesy. V rámci bežného prieskumníka súborov kliknite pravým tlačidlom myši na vybraný súbor a zvoľte možnosť **Pokročilé možnosti** > **Skontrolovať reputáciu súborov**.



Správa o bezpečnosti

Táto funkcia vám poskytuje štatistické údaje o činnosti programu rozdelené do nasledujúcich kategórií:

- **Zablokované webové stránky** – zobrazuje počet zablokovaných webových stránok (URL adresa na blackliste z dôvodu PUA, phishingu, hacknutého routera, IP alebo certifikátu).
- **Zachytené infikované e□mailové objekty** – zobrazuje počet infikovaných e□mailových objektov, ktoré boli programom detegované.
- **Zablokované webové stránky v rodičovskej kontrole** – zobrazuje počet stránok zablokovaných rodičovskou kontrolou.
- **Zachytené potenciálne nechcené aplikácie** – zobrazuje počet potenciálne nechcených aplikácií (PUA), ktoré boli programom detegované.
- **Zachytené spamové e□maily** – zobrazuje počet spamových e□mailov, ktoré boli programom detegované.
- **Zablokované prístupy k webovej kamere** – zobrazuje počet zablokovaných prístupov k webovej kamere.
- **Skontrolované dokumenty** – zobrazuje počet skontrolovaných dokumentov.
- **Skontrolované aplikácie** – zobrazuje počet skontrolovaných spustiteľných objektov.
- **Skontrolovaných iných objektov** – zobrazuje počet iných skontrolovaných objektov.
- **Skontrolované objekty webových stránok** – zobrazuje počet skontrolovaných objektov webových stránok.

- **Skontrolované e-mailové objekty** – zobrazuje počet skontrolovaných e-mailových objektov.

Poradie uvedených kategórií sa dynamicky mení, pričom na začiatku je vždy zobrazená kategória s najvyššou číselnou hodnotou a na konci s najnižšou. Kategórie s nulovými hodnotami sa nezobrazujú. Pre zobrazenie skrytých kategórií kliknite na možnosť **Zobraziť viac**.

Priamo zo Správy o bezpečnosti tiež máte možnosť aktivovať nasledujúce funkcie:

- Rodičovská kontrola
- Anti-Theft

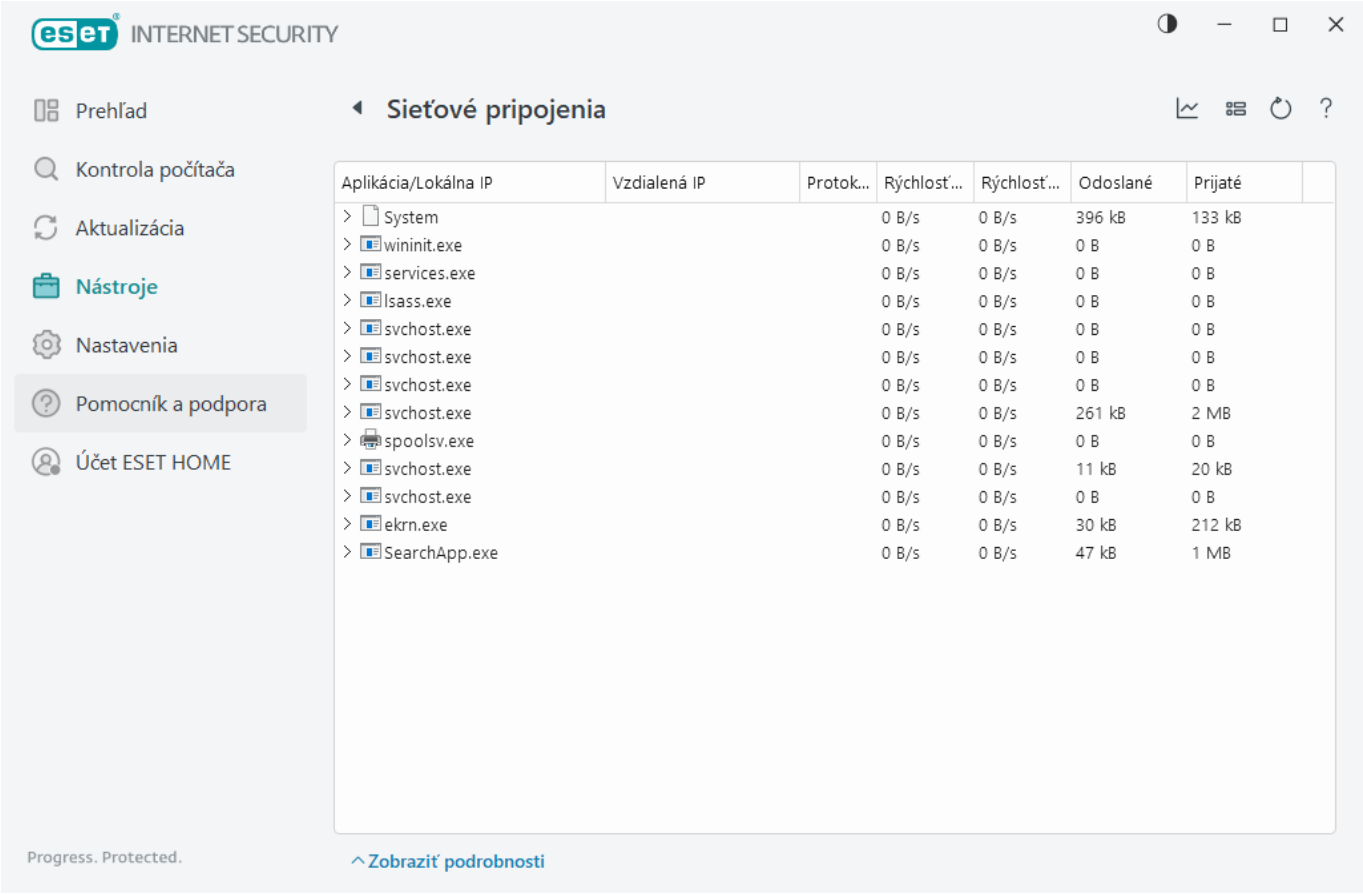
Ak niektorú z týchto funkcií aktivujete, nebude sa viac zobrazovať v rámci správy o bezpečnosti ako nefunkčná.

Kliknutím na ikonu ozubeného kolesa v pravom hornom rohu môžete **Zapnúť/Vypnúť oznámenia správy o bezpečnosti** a taktiež si zvoliť, či sa majú zobrazovať dáta za posledných 30 dní alebo od aktivácie produktu. Ak ste program ESET Internet Security nainštalovali pred menej ako 30 dňami, zvoliť bude možné len počet dní, ktoré uplynuli od inštalácie. Predvolenou nastavenou hodnotou je 30 dní.

Pomocou možnosti **Vynulovať dáta** odstránite všetky štatistiky a existujúce dáta zo Správy o bezpečnosti. Táto akcia si bude vyžadovať vaše potvrdenie v prípade, že ste predtým nezrušili označenie možnosti **Potvrdzovanie pred vynulovaním štatistiky** v Rozšírených nastaveniach v sekcii **Oznámenia** > **Interaktívne upozornenia** > **Potvrdzovacie správy** > **Upraviť**.

Sieťové pripojenia

V sekcii Sieťové pripojenia môžete vidieť zoznam aktívnych alebo čakajúcich spojení. Získate tak prehľad o aplikáciách, ktoré komunikujú so vzdialenou stranou.



Kliknutím na ikonu grafu si zobrazíte sieťovú aktivitu.

Prvý riadok zobrazuje meno aplikácie a rýchlosť dátového prenosu. Zoznam sieťových pripojení pre danú aplikáciu (a viac podrobnejších informácií) si môžete zobraziť kliknutím na **>**.

Stĺpce

Aplikácia/Lokálna IP – názov aplikácie, lokálna IP adresa a komunikačný port.

Vzdialená IP – IP adresa a komunikačný port vzdialenej strany.

Protokol – komunikačný protokol.

Rýchlosť nahrávania/Rýchlosť sťahovania – zobrazuje rýchlosť prichádzajúcej/odchádzajúcej komunikácie.

Odoslané/Prijaté – objem dát, ktorý je prenesený v rámci spojenia.

Zobraziť podrobnosti – zobrazí podrobnosti o vybranom spojení.

Pravým tlačidlom myši kliknite na pripojenie a zobrazia sa vám doplňujúce možnosti:

Prekladať IP adresy na mená – pokiaľ je to možné, sieťové adresy sú uvádzané v DNS forme a nie v číselnej

podobe IP adresy.

Zobrazovať iba pripojenia TCP – v zozname sa zobrazia iba tie spojenia, ktoré patria pod protokol TCP.

Zobrazovať počúvajúce pripojenia – zobrazia sa iba spojenia, pri ktorých neprebieha komunikácia, systém však má otvorený port a čaká na spojenie.

Zobrazovať pripojenia v rámci počítača – zobrazia sa iba pripojenia, ktoré majú ako vzdialenú stranu použitý lokálny systém. Týka sa to tzv. localhost pripojení.

Rýchlosť obnovovania – frekvencia, s akou sa budú obnovovať informácie o aktívnych pripojeniach.

Obnoviť teraz – obnovia sa informácie v okne **Sieťové pripojenia**.

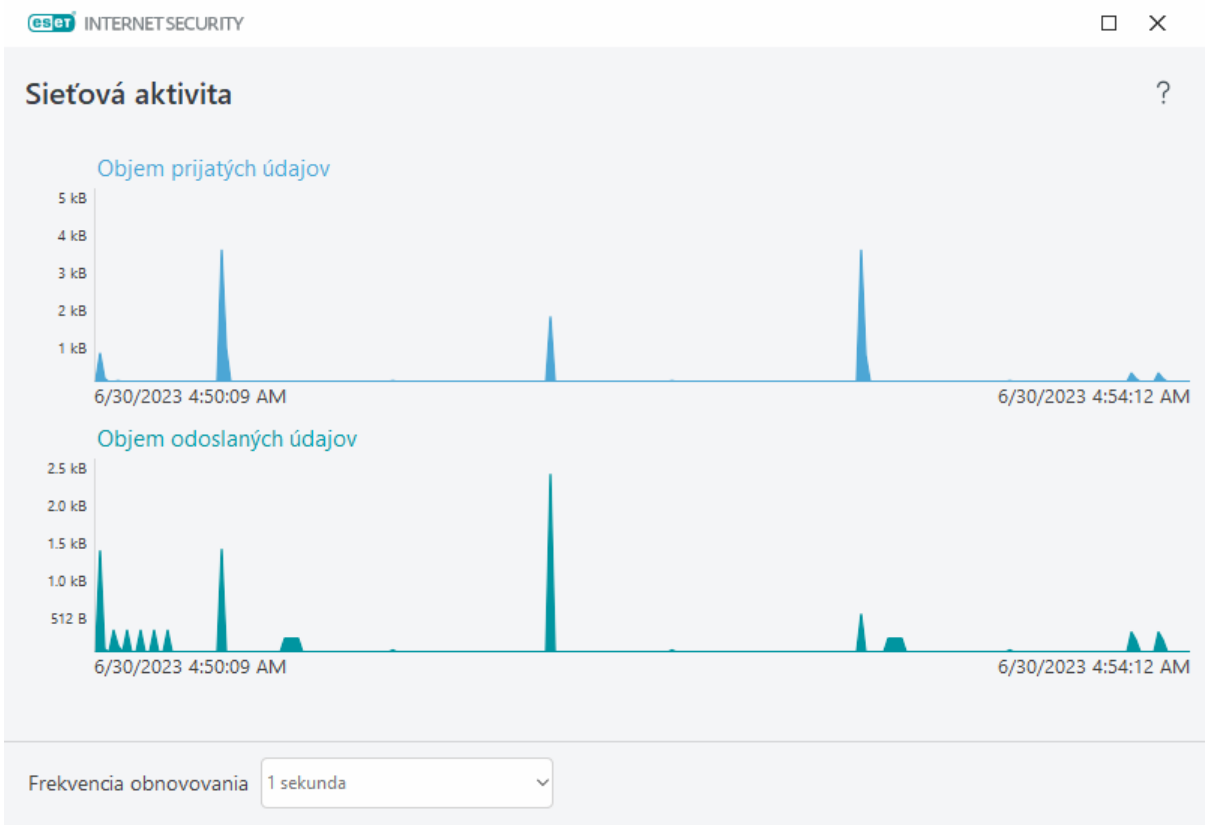
Nasledujúce možnosti sú dostupné len po kliknutí na aplikáciu alebo proces, nie na aktívne spojenie:

Dočasne zablokovať komunikáciu pre daný proces – zablokuje nadviazané spojenie pre danú aplikáciu. V prípade vytvorenia nového spojenia firewall použije vopred definované pravidlo. Viac informácií o nastaveniach nájdete v kapitole Pravidlá firewallu.

Dočasne povoliť komunikáciu pre daný proces – povolí nadviazané spojenie pre danú aplikáciu. V prípade vytvorenia nového spojenia firewall použije vopred definované pravidlo. Viac informácií o nastaveniach nájdete v kapitole Pravidlá firewallu.

Sieťová aktivita

Ak chcete zobraziť aktuálnu **sieťovú aktivitu** na grafe, kliknite na **Nástroje** > **Sieťové pripojenia** a kliknite na ikonu grafu . V spodnej časti grafu je časová os, ktorá zaznamenáva sieťovú aktivitu v reálnom čase a obnovuje sa v nastavených intervaloch. Ak chcete zmeniť interval obnovenia, vyberte želanú hodnotu z roletového menu **Frekvencia obnovovania**.



K dispozícii sú nasledujúce možnosti:

- **1 sekunda** – graf sa obnovuje každú sekundu, časová os zobrazuje posledné 4 minúty.
- **1 minúta (posledných 24 hodín)** – graf sa obnovuje každú minútu, časová os zobrazuje posledných 24 hodín.
- **1 hodina (posledný mesiac)** – graf sa obnovuje každú hodinu, časová os zobrazuje posledný mesiac.

Zvislá os grafu zobrazuje objem prijatých alebo odoslaných údajov. Po prejdení kurzorom do vybranej časti grafu sa zobrazí presné množstvo prijatých/odoslaných údajov v konkrétnom časovom úseku.

ESET SysInspector

ESET SysInspector je aplikácia slúžiaca na dôkladné preskúmanie stavu vášho počítača, ktorá je schopná zhromažďovať údaje o nainštalovaných ovládačoch a programoch, sieťových pripojeniach či dôležitých položkách databázy Registry a zobraziť úroveň rizika jednotlivých komponentov systému v jednoduchej čitateľnej forme. Tieto informácie vám môžu pomôcť zistiť príčiny podozrivého správania systému, či už vplyvom nekompatibility alebo infekcie škodlivým kódom. Ak sa chcete dozvedieť, ako používať ESET SysInspector, pozrite si Online pomocníka pre ESET SysInspector.

V okne ESET SysInspector sa nachádzajú nasledujúce informácie o protokoloch:

- **Čas** – čas vytvorenia.
- **Komentár** – stručný komentár.
- **Používateľ** – meno používateľa, ktorý vytvoril protokol.

- **Stav** – stav vytvorenia.

Sú dostupné tieto akcie:

- **Zobraziť** – otvorí zvolený protokol v nástroji ESET SysInspector. Môžete tiež kliknúť pravým tlačidlom na konkrétny protokol a z kontextového menu vybrať možnosť **Zobraziť**.

- **Vytvoriť** – vytvorí nový protokol. Počkajte, kým sa vygeneruje protokol nástroja ESET SysInspector (stav protokolu bude označený ako **Vytvorený**). Protokol sa uloží do umiestnenia C:\ProgramData\ESET\ESET Security\SysInspector.

- **Odstrániť** – odstráni označený protokol zo zoznamu.

Nasledujúce položky budú dostupné z kontextového menu, ak je označený jeden alebo viacero protokolov:

- **Zobraziť** – otvorí zvolený protokol v nástroji ESET SysInspector (rovnako ako pri dvojitom kliknutí na protokol).

- **Vytvoriť** – vytvorí nový protokol. Počkajte, kým sa vygeneruje protokol nástroja ESET SysInspector (stav protokolu bude označený ako **Vytvorený**).

- **Odstrániť** – odstráni označený protokol zo zoznamu.

- **Odstrániť všetko** – vymaže všetky protokoly.

- **Exportovať** – uloží protokol do súboru .xml alebo do skomprimovaného súboru .zip.

Plánovač

Plánovač umožňuje správu a spúšťanie naplánovaných úloh s prednastavenými parametrami a vlastnosťami.

Je prístupný z menu hlavného okna programu ESET Internet Security v sekcii **Nástroje** > **Plánovač**. **Plánovač** obsahuje zoznam všetkých naplánovaných úloh, ich nastavení a vlastností, ktoré sa vykonávajú v stanovený čas s použitím zadefinovaných profilov.

Plánovač slúži na plánovanie úloh, ako je napr. aktualizácia modulov, kontrola počítača, kontrola súborov spúšťaných pri štarte či pravidelné čistenie protokolov. Priamo z hlavného okna Plánovača môžete pridať alebo vymazať úlohu kliknutím na príslušné tlačidlo v dolnej časti okna (tlačidlá **Pridať plánovanú úlohu** a **Odstrániť**). Zmazať všetky zmeny a vrátiť zoznam plánovaných úloh späť do predvolených nastavení môžete kliknutím na tlačidlo **Predvolené**. Kontextové menu, ktoré sa otvorí po kliknutí pravým tlačidlom myši v okne plánovača, umožňuje tieto akcie: zobrazenie detailných informácií o úlohe, okamžité vykonanie úlohy, pridanie novej úlohy, úpravu, resp. odstránenie už existujúcej úlohy. Zaškrtávacím políčkom pri úlohe je úlohu možné vypnúť/zapnúť.

V predvolenom nastavení **Plánovača** sú dostupné nasledujúce úlohy:

- **Údržba protokolov**

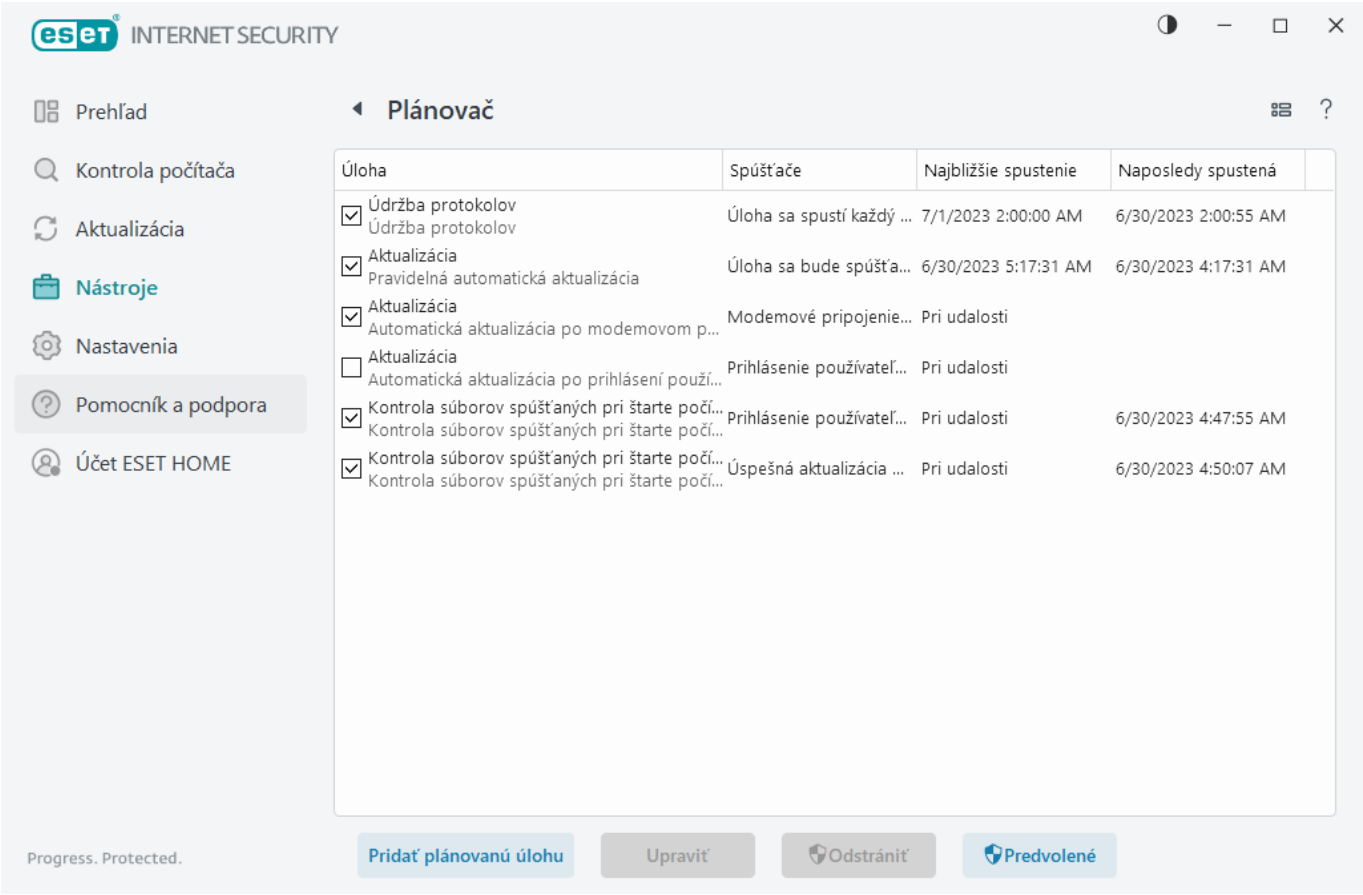
- **Pravidelná automatická aktualizácia**

- **Automatická aktualizácia po prihlásení používateľa**

- **Kontrola súborov spúšťaných pri štarte počítača** (po prihlásení používateľa)

- **Kontrola súborov spúšťaných pri štarte počítača** (po úspešnej aktualizácii detekčného jadra)

Nastavenia existujúcich plánovaných úloh (a to tak predvolených, ako aj vlastných) je možné meniť cez kontextové menu potvrdením voľby **Upraviť** alebo výberom príslušného riadku v zozname úloh a kliknutím na tlačidlo **Upraviť**.



Pridanie plánovanej úlohy

1. Kliknite na **Pridať plánovanú úlohu** v spodnej časti okna.

2. Zadajte názov úlohy.

3. Zvoľte typ úlohy z roletového menu:

   - **Spustenie externej aplikácie** – výber aplikácie, ktorá má byť spustená plánovačom.

   - **Údržba protokolov** – v protokoloch môžu zostávať stopy po vymazaných záznamoch. Táto úloha pravidelne optimalizuje záznamy v protokoloch, čím sa zefektívni a zrýchli práca s nimi.

   - **Kontrola súborov spúšťaných pri štarte počítača** – kontroluje súbory, ktoré sa spúšťajú pri štarte alebo prihlásení do systému.

   - **Vytvorenie záznamu o stave počítača** – vytvára záznam o stave počítača cez nástroj ESET SysInspector, ktorý slúži na zhromažďovanie podrobných informácií o systémových súčastiach (napr. ovládače, aplikácie) a posudzuje úroveň rizika každej súčasti.

   - **Manuálna kontrola počítača** – vykoná kontrolu diskov, jednotlivých priečinkov a súborov na počítači.

- **Aktualizácia** – zabezpečuje aktualizáciu programových modulov.

4. Pomocou prepínacieho tlačidla vedľa možnosti **Zapnuté** aktivujte úlohu (môžete tak urobiť aj neskôr začiarknutím políčka v zozname naplánovaných úloh) a po kliknutí na **Ďalej** nastavte načasovanie úlohy:

- **Raz** – úloha sa vykoná iba raz v presne určený deň a čas.
- **Opakovane** – úloha bude vykonávaná opakovane v určenom časovom intervale.
- **Denne** – úloha bude vykonávaná opakovane každý deň v určenom čase.
- **Týždenne** – úloha sa bude vykonávať týždenne vo zvolené dni a v určený čas.
- **Pri udalosti** – úloha sa bude vykonávať pri určitej udalosti.

5. Možnosť **Nespúšťať úlohu, ak je počítač napájaný z batérie** je dobré použiť, ak prenosný počítač nie je zapojený do elektrickej siete a chcete v tomto čase minimalizovať jeho systémové prostriedky. Zadajte čas/dátum alebo interval, v ktorom bude úloha vykonaná, do poľa **Vykonanie úlohy**. V prípade, že sa naplánovanú úlohu nepodarí vykonať v určenom čase, môžete nastaviť, kedy sa má opätovne spustiť:

- **V najbližšom naplánovanom čase**
- **Hneď ako to bude možné**
- **Okamžite, ak od posledného naplánovaného spustenia uplynul stanovený časový interval v hodinách** – ide o čas, ktorý uplynul od momentu, keď mala byť úloha prvýkrát spustená. Ak sa stanovený čas prekročí, úloha sa spustí okamžite. Čas nastavte pomocou číselníka nižšie.

Informácie o naplánovanej úlohe zobrazíte kliknutím pravým tlačidlom myši na danú úlohu a potom na možnosť **Zobraziť podrobnosti**.

Možnosti plánovanej kontroly

V tomto okne môžete meniť rozšírené nastavenia pre plánované úlohy kontroly počítača.

Na vykonanie kontroly bez liečenia kliknite na **Rozšírené nastavenia** a vyberte možnosť **Kontrolovať bez liečenia**. História kontrol sa zaznamenáva do protokolu kontroly.

Ak je vybraná možnosť **Ignorovať vylúčenia**, súbory s príponami, ktoré boli predtým vylúčené z kontroly, budú kontrolované bez výnimky.

V roletovom menu **Akcia po kontrole** môžete nastaviť akciu, ktorá sa má vykonať automaticky po dokončení kontroly:

- **Žiadna akcia** – po ukončení kontroly nebude vykonaná žiadna akcia.
- **Vypnúť** – počítač sa po ukončení kontroly vypne.
- **Reštartovať v prípade potreby** – počítač sa reštartuje, ak bude potrebné dokončiť liečenie zachytených hrozieb.
- **Reštartovať** – počítač po ukončení kontroly zatvorí všetky spustené programy a reštartuje sa.

• **Vynútiť reštart v prípade potreby** – počítač sa nútene reštartuje, ak bude potrebné dokončiť liečenie zachytených hrozieb.

• **Vynútiť reštart** – po ukončení kontroly sa bez interakcie s používateľom nútene zatvoria všetky spustené programy a počítač sa reštartuje.

• **Uspať** – vaša relácia bude uložená a počítač sa prepne do úsporného režimu, tak aby sa dal rýchlo zapnúť.

• **Prepnúť do režimu dlhodobého spánku** – bude uložená snímka stavu počítača a počítač sa vypne. Pri opätovnom zapnutí počítača sa načíta uložený stav.

i Možnosti **Uspať** a **Prepnúť do režimu dlhodobého spánku** sú dostupné v závislosti od nastavení napájania a režimu spánku v rámci operačného systému alebo od možností vášho počítača/laptopu. Berte na vedomie, že počítač v stave spánku je aj naďalej zapnutý. Takýto počítač má stále aktívne základné funkcie a naďalej spotrebúva elektrickú energiu, a to aj v prípade, že je napájaný z batérie. Pre šetrenie batérie, napríklad pri cestovaní mimo kancelárie, odporúčame použiť možnosť Prepnúť do režimu dlhodobého spánku.

Zvolená akcia sa spustí po dokončení všetkých prebiehajúcich kontrol. Ak ste zvolili akciu **Vypnúť** alebo **Reštartovať**, zobrazí sa dialógové okno s výzvou na potvrdenie akcie s 30□sekundovým odpočítavaním, v rámci ktorého je možné plánované vypnutie/reštartovanie počítača zrušiť kliknutím na **Zrušiť**.

Kliknite na možnosť **Kontrolu nemožno prerušiť**, ak si prajete, aby neoprávnený používateľ nemohol prerušiť akciu po ukončení kontroly.

Nastavte hodnotu pre možnosť **Pozastaviť plánované kontroly o (min.)**, ak chcete umožniť používateľovi s obmedzenými oprávneniami pozastaviť kontrolu počítača na stanovený čas.

Prečítajte si tiež kapitolu Priebeh kontroly.

Informácie o naplánovanej úlohe

Toto dialógové okno zobrazuje informácie o označenej naplánovanej úlohe. Zobrazuje sa po dvojitom kliknutí na úlohu plánovača alebo po kliknutí pravým tlačidlom na myši a vybratí možnosti **Zobraziť informácie** z kontextového menu.

Podrobnosti úlohy

Zadajte názov do textového poľa **Názov úlohy**, vyberte typ úlohy z roletového menu **Typ úlohy** a kliknite na **Ďalej**:

• **Spustenie externej aplikácie** – výber aplikácie, ktorá má byť spustená plánovačom.

• **Údržba protokolov** – v protokoloch môžu zostávať stopy po vymazaných záznamoch. Táto úloha pravidelne optimalizuje záznamy v protokoloch, čím sa zefektívni a zrýchli práca s nimi.

• **Kontrola súborov spúšťaných pri štarte počítača** – kontroluje súbory, ktoré sa spúšťajú pri štarte alebo prihlásení do systému.

• **Vytvorenie záznamu o stave počítača** – vytvára záznam o stave počítača cez nástroj ESET SysInspector, ktorý slúži na zhromažďovanie podrobných informácií o systémových súčastiach (napr. ovládače, aplikácie) a

posudzuje úroveň rizika každej súčasti.

- **Manuálna kontrola počítača** – vykoná kontrolu diskov, jednotlivých priečinkov a súborov na počítači.
- **Aktualizácia** – zabezpečuje aktualizáciu programových modulov.

Načasovanie úlohy

Úloha bude vykonávaná opakovane v určenom časovom intervale. Vyberte interval vykonania úlohy:

- **Raz** – úloha sa vykoná iba raz v presne určenom dátume a čase.
- **Opakovane** – úloha bude vykonávaná opakovane v stanovených intervaloch (hodinách).
- **Denne** – úloha bude vykonávaná opakovane každý deň v určenom čase.
- **Týždenne** – úloha bude vykonaná raz alebo viackrát za týždeň, vo zvolených dňoch a časoch.
- **Pri udalosti** – úloha bude vykonaná v prípade, že nastane zvolená udalosť.

Nespúšťať úlohu, ak je počítač napájaný z batérie – úloha sa nevykoná v čase plánovaného spustenia, ak je počítač napájaný z batérie. To sa vzťahuje aj na počítače napájané neprerušiteľným zdrojom napájania (UPS).

Načasovanie úlohy – raz

Vykonanie úlohy – úloha sa spustí iba raz v zadanom dátume a čase.

Načasovanie úlohy – denne

Úloha sa bude spúšťať opakovane každý deň v určenom čase.

Načasovanie úlohy – týždenne

Úloha sa bude spúšťať opakovane každý týždeň vo zvolených dňoch a časoch.

Načasovanie úlohy – pri udalosti

Úloha bude vykonávaná pri jednej z nasledujúcich udalostí:

- **Každé spustenie počítača**
- **Prvé spustenie počítača počas dňa**
- **Modemové pripojenie k internetu/VPN**
- **Úspešná aktualizácia modulov**

- **Úspešná aktualizácia produktu**
- **Prihlásenie používateľa**
- **Detekcia hrozieb**

Pri vytváraní plánovanej úlohy spúšťanej pri určitej udalosti vám Plánovač umožňuje nastaviť minimálny časový interval medzi dvoma po sebe nasledujúcimi spusteniami danej úlohy. Napríklad, ak sa prihlasujete na počítač viackrát za deň, nastavením intervalu na 24 hodín sa táto úloha vykoná len pri prvom prihlásení a následne až v nasledujúci deň.

Vynechaná úloha

Môže dôjsť k vynechaniu plánovanej úlohy v prípade, že je počítač napájaný z batérie alebo vypnutý.
Z dostupných možností vyberte, kedy sa má úloha opätovne spustiť, ak v naplánovanom čase nebola vykonaná, a kliknite na **Ďalej**:

- **Vykonať úlohu v najbližšom naplánovanom čase** – úloha sa spustí v najbližšom naplánovanom čase, ak bude počítač práve vtedy zapnutý.
- **Hneď ako to bude možné** – úloha sa spustí, keď je počítač zapnutý.
- **Okamžite, ak od posledného naplánovaného spustenia uplynul stanovený časový interval v hodinách** – ide o čas, ktorý uplynul od prvého vynechania úlohy. Ak sa stanovený čas prekročí, úloha sa spustí okamžite.

Okamžite, ak od posledného naplánovaného spustenia uplynul stanovený časový interval v hodinách – príklady

Príkladová úloha je nastavená tak, aby sa spúšťala opakovane každú hodinu. Je vybraná možnosť **Okamžite, ak od posledného naplánovaného spustenia uplynul stanovený časový interval v hodinách**, pričom časový interval je nastavený na dve hodiny. Úloha sa spustí o 13:00 a po jej dokončení počítač prejde do režimu spánku:

- Počítač sa prebudí o 15:30. V čase 14:00 bolo vykonanie úlohy prvýkrát vynechané. Od 14:00 uplynulo iba 1,5 hodiny (čo je menej ako 2 hodiny), takže úloha sa spustí opäť o 16:00.
- Počítač sa prebudí o 16:30. V čase 14:00 bolo vykonanie úlohy prvýkrát vynechané. Od 14:00 uplynulo už dva a pol hodiny, takže úloha sa spustí okamžite.

Podrobnosti úlohy – aktualizácia

Nastavenie hlavného a alternatívneho profilu pre aktualizáciu umožňuje vykonávať aktualizáciu z dvoch miest. Alternatívny profil bude použitý v prípade, že z prvého sa aktualizáciu nepodarí vykonať. Túto možnosť je možné využiť napríklad pre notebooky, ktoré sú používané v lokálnej LAN sieti a zároveň aj v iných sieťach s pripojením na internet. V prípade neúspešnej aktualizácie z hlavného profilu s nastavením na lokálnu LAN, bude aktualizácia vykonaná z alternatívneho profilu, ktorý bude nastavený pre aktualizáciu priamo zo serverov spoločnosti ESET.

Podrobnosti úlohy – spustenie aplikácie

Táto úloha slúži na plánované spustenie externej aplikácie.

Spustiteľný súbor – vyberte spustiteľný súbor kliknutím na **...** alebo cestu k súboru aplikácie zadajte manuálne.

Pracovný priečinok – zadajte pracovný adresár aplikácie. Všetky dočasné súbory tohto **spustiteľného súboru** budú vytvorené v tomto adresári.

Parametre – parametre, s ktorými bude aplikácia spustená (voliteľné).

Kliknite na **Dokončiť** pre pridanie úlohy.

Čistenie systému

Nástroj na čistenie systému vám po odstránení infiltrácie z napadnutého počítača pomôže obnoviť váš systém do plne funkčného stavu. Niektoré druhy malvéru sú schopné vypnúť systémové nástroje, akými sú Editor databázy Registry, Správca úloh alebo Aktualizácie systému Windows. Nástroj na čistenie systému obnoví predvolené hodnoty a nastavenia pre daný operačný systém na jedno kliknutie.

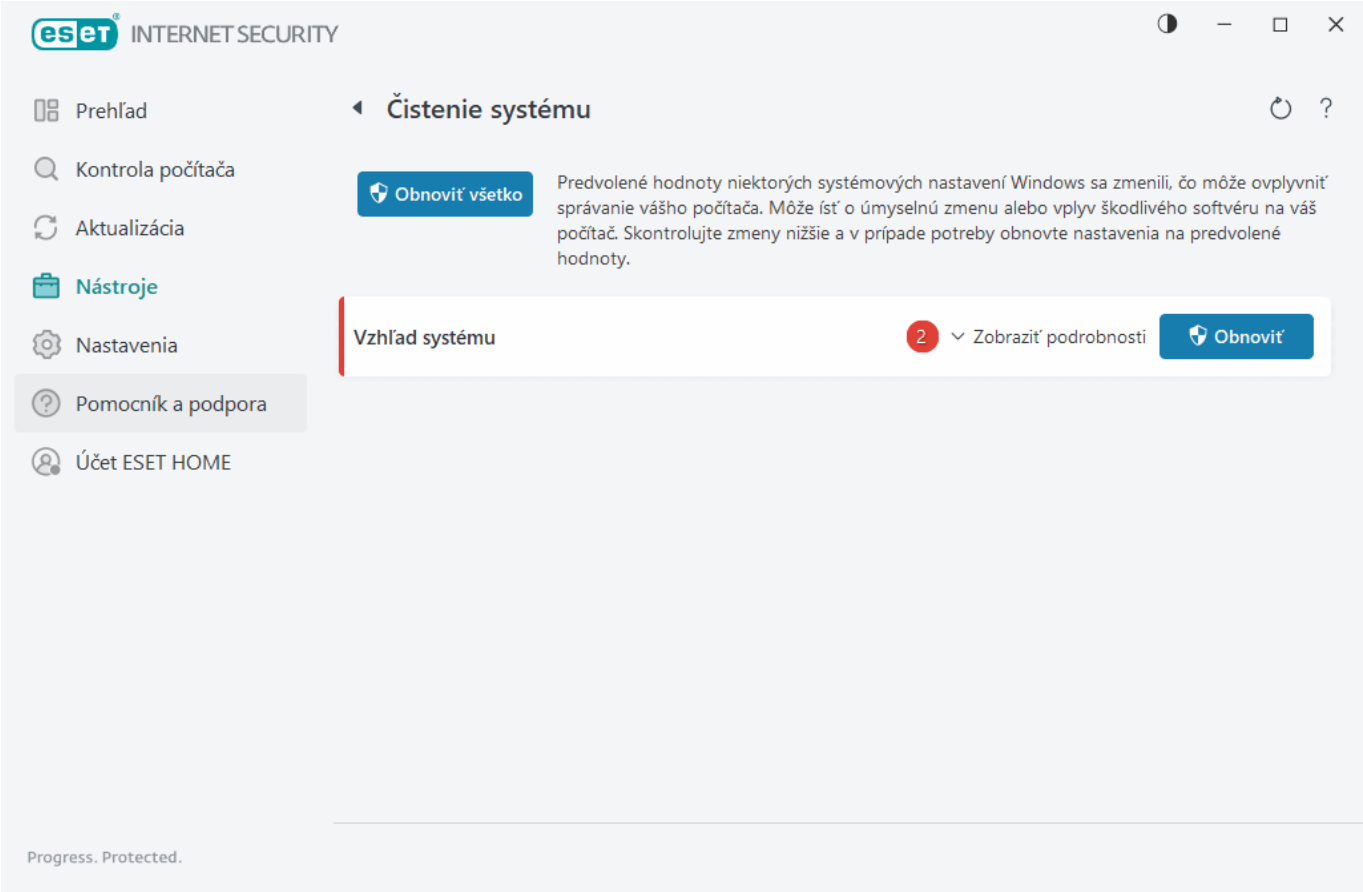
Nástroj na čistenie systému zaznamenáva problémy v rámci piatich kategórií nastavení:

- **Nastavenia zabezpečenia**: zmeny v nastaveniach, ktoré môžu viesť k vyššej zraniteľnosti vášho počítača (napríklad zmeny v nastaveniach Windows Update).
- **Nastavenia systému**: zmeny v nastaveniach systému, ktoré majú vplyv na správanie vášho počítača (napríklad priradenia súborov).
- **Vzhľad systému**: zmeny v nastaveniach, ktoré ovplyvňujú vzhľad vášho systému (napríklad pozadie pracovnej plochy).
- **Vypnuté funkcie**: vypnutie dôležitých funkcií a aplikácií.
- **Obnovovanie systému Windows**: nastavenia pre funkciu obnovovania systému Windows, ktorá vám umožňuje vrátiť systém do predošlého stavu.

Čistenie systému je možné vyžiadať:

- keď sa na počítači nájde hrozba,
- keď používateľ klikne na možnosť **Obnoviť**.

Môžete si prezrieť jednotlivé zmeny v systéme a podľa potrieb obnoviť predvolené nastavenia.



Vykonávať akcie v nástroji na čistenie systému môže len používateľ s právami správcu.

Strážca siete

Strážca siete pomáha odhaliť bezpečnostné zraniteľnosti v rámci vašej dôveryhodnej (domácej alebo pracovnej) siete, ako napr. slabé heslo routera či otvorené porty. Poskytuje tiež zoznam pripojených zariadení, pričom zariadenia sú rozdelené do kategórií podľa typu (napr. tlačiarne, routery, mobilné zariadenia atď.). Vďaka tomu budete mať prehľad o tom, aké zariadenia sú pripojené k vašej sieti (napr. herná konzola, zariadenia IoT alebo iné domáce smart zariadenia).

Funkcia Strážca siete vám pomáha identifikovať bezpečnostné zraniteľnosti routera a zvyšuje úroveň vašej ochrany pri pripojení sa do siete.

Strážca siete však nemôže ovplyvniť konfiguráciu vášho routera. Všetky zmeny v nastaveniach musíte vykonať sami prostredníctvom špecializovaného rozhrania vášho routera. Domáce routery sú veľmi zraniteľné a ľahko napadnuteľné malvérom, prostredníctvom ktorého sa iniciujú tzv. DDoS útoky (distributed denial-of-service attacks, vo voľnom preklade „distribuované útoky zamedzenia služby“). Ak používateľ nezmení heslo prednastavené výrobcom routera, pre útočníka je veľmi jednoduché toto heslo uhádnuť. Útočník následne môže získať prístup k routeru a zmeniť jeho nastavenia alebo ohroziť bezpečnosť celej vašej siete.

Dôrazne vám odporúčame vytvoriť si pre router silné a dostatočne dlhé heslo, ktoré okrem bežných znakov obsahuje aj čísla, špeciálne znaky alebo veľké písmená. Použitím kombinácie rôznych takýchto znakov zabezpečíte, že vaše heslo nebude jednoduché prelomiť.

Ak je sieť, ku ktorej ste pripojený, nakonfigurovaná ako dôveryhodná, môžete sieť označiť ako „Moja sieť“. Kliknutím na možnosť **Označiť ako „Moja sieť“** priradíte sieti označenie Moja sieť. Toto označenie sa bude

zobrazovať vedľa siete naprieč celým produktom ESET Internet Security v záujme lepšej identifikácie a dohľadu nad zabezpečením. Ak chcete označenie siete odobrať, kliknite na možnosť **Zrušiť označenie „Moja sieť“**.

Každé zariadenie, ktoré je pripojené k vašej sieti, sa zobrazí v zozname spolu so základnými informáciami. Kliknutím na konkrétne zariadenie môžete zariadenie upraviť alebo si zobraziť podrobné informácie.

Pomocou roletového menu **Siete** môžete zariadenia v zozname filtrovať podľa nasledujúcich kritérií:

- zariadenia pripojené ku konkrétnej sieti,
- zariadenia pripojené ku **Všetkým sieťam**,
- nekategorizované zariadenia.

Kliknutím na ikonu zariadenia si môžete zobraziť podrobné informácie o danom zariadení alebo zariadenie upraviť. Nedávno pripojené zariadenia sú zobrazené bližšie pri routeri, aby ste ich mohli jednoducho nájsť.

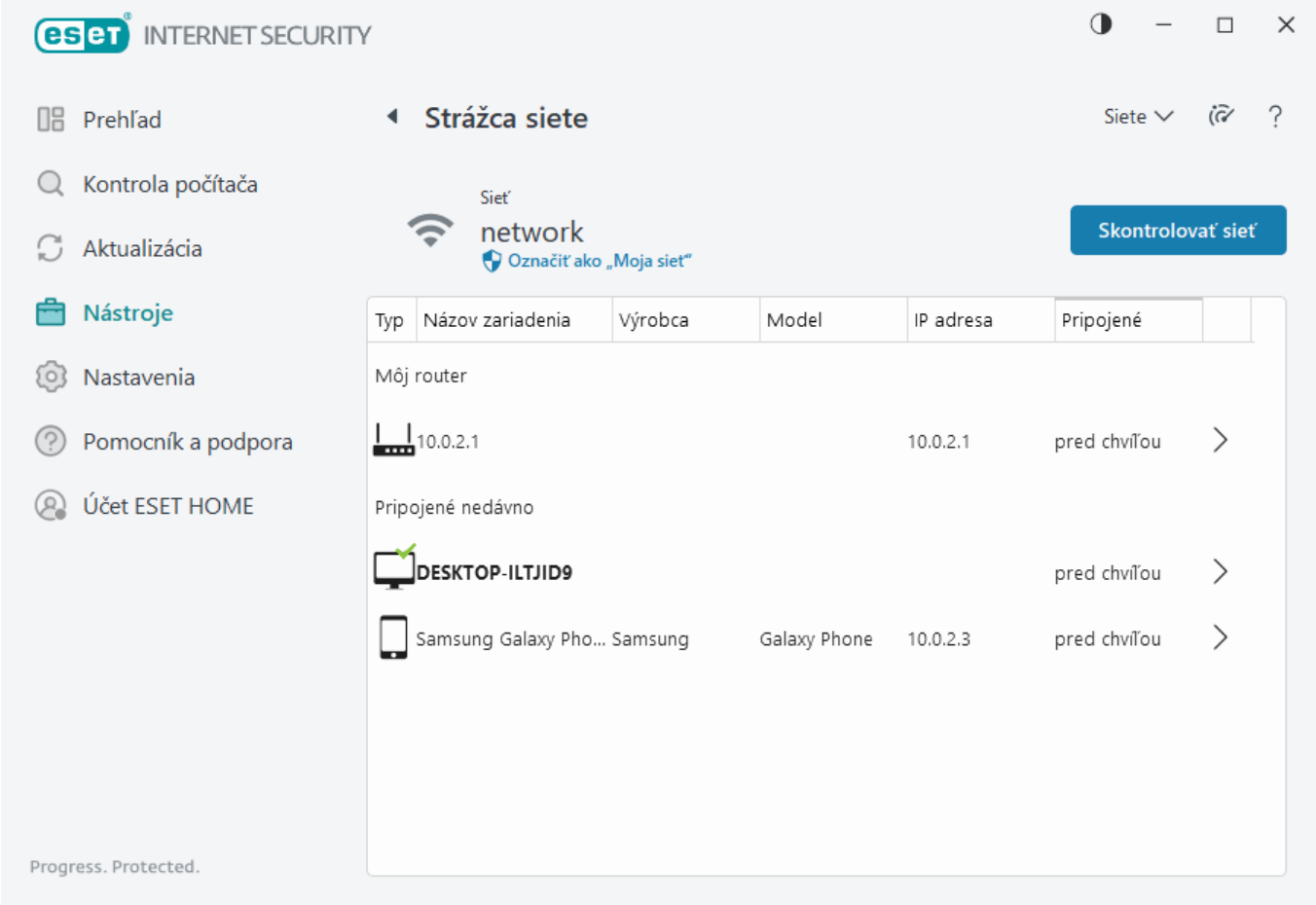
Kliknutím na ozubené koliesko v pravom hornom rohu vyberte, či sa má zobraziť oznámenie v prípade, že sa v sieti objaví nové zariadenie.

Kontrolu siete, ku ktorej ste momentálne pripojený, môžete manuálne spustiť kliknutím na možnosť **Skontrolovať sieť**. Možnosť **Skontrolovať sieť** je dostupná len pre dôveryhodné siete. Ak chcete skontrolovať alebo upraviť nastavenia siete, pozrite si časť Profily sieťového pripojenia.

Môžete sa rozhodnúť, čo chcete skontrolovať. K dispozícii sú nasledujúce možnosti:

- Skontrolovať všetko,
- Skontrolovať iba router,
- Skontrolovať iba zariadenia.

Túto kontrolu vykonávajte len na dôveryhodnej sieti! Ak kontrolu vykonáte na nedôveryhodných sieťach, hrozí potenciálne riziko.



Po dokončení kontroly sa zobrazí oznámenie obsahujúce odkaz na základné informácie o podozrivom zariadení. Podrobnosti zobrazíte aj tak, že dvakrát kliknete na podozrivé zariadenie v zozname alebo sonarovom zobrazení. Na zobrazenie nedávno blokovanej komunikácie kliknite na **Riešiť problémy**. Viac informácií o riešení problémov s firewallom

Modul Strážca siete vás prostredníctvom oznámenia môže upozorniť na nasledujúce udalosti:

- **K sieti sa pripojilo nové zariadenie** – toto oznámenie sa zobrazí v prípade, že je používateľ pripojený k sieti a do tejto siete sa pripojí nové zariadenie.

- **Nájdené nové sieťové zariadenia** – toto oznámenie sa zobrazí v prípade, že sa znova pripojíte k dôveryhodnej sieti a od vášho posledného pripojenia sa v nej objavilo nové zariadenie.

V oboch prípadoch vás program upozorňuje na to, že k vašej sieti sa pokúša pripojiť neautorizované zariadenie. Ak chcete zobraziť podrobnosti, kliknite na možnosť **Pozrite si podrobnosti zariadenia**.

Čo znamenajú jednotlivé ikony zobrazené pri zariadeniach v rámci funkcie Strážca siete?

	Žltá hviezdička označuje zariadenia, ktoré sú v sieti nové alebo ktoré program ESET zachytil prvýkrát.
	Žltý výkričník označuje, že router môže obsahovať bezpečnostné zraniteľnosti. Kliknutím na túto ikonu vo vašom produkte získate podrobnejšie informácie o probléme.
	Červený výkričník označuje, že router obsahuje bezpečnostné zraniteľnosti a môže byť infikovaný. Kliknutím na túto ikonu vo vašom produkte získate podrobnejšie informácie o probléme.

Modrá ikona sa môže objaviť, keď váš produkt ESET získa dodatočné informácie o routeri, ktoré však nevyžadujú okamžitú pozornosť, pretože neexistujú žiadne bezpečnostné riziká. Kliknutím na ikonu získate podrobnejšie informácie.

Sieťové zariadenie v rámci Strážcu siete

V tejto sekcii môžete nájsť podrobné informácie o sieťovom zariadení vrátane nasledujúcich údajov:

- názov zariadenia,
- typ zariadenia,
- posledné pripojenie,
- názov siete,
- IP adresa,
- MAC adresa,
- operačný systém.

Ikona ceruzky vám umožňuje upraviť názov alebo typ zariadenia.

Odstrániť z histórie – umožňuje vymazať zariadenie zo zoznamu zariadení. Táto možnosť je dostupná len pre zariadenia, ktoré práve nie sú pripojené k vašej sieti.

Pre každý typ zariadenia sú dostupné tieto možnosti:

Router

Nastavenia routera – k nastaveniam routera môžete pristúpiť z webového rozhrania, mobilnej aplikácie alebo kliknutím na **Otvoriť rozhranie routera**. Ak máte router od svojho poskytovateľa internetového pripojenia, na vyriešenie zachytených bezpečnostných problémov bude možno potrebné kontaktovať technickú podporu vášho poskytovateľa internetového pripojenia alebo výrobcu routera. Vždy dodržiavajte správne bezpečnostné opatrenia tak, ako sú uvedené v používateľskej príručke k vášmu routeru.
Ochrana – na ochranu svojho routera a siete pred kybernetickými útokmi sa riaďte týmito základnými odporúčaniami.

Sieťové zariadenie

Identifikácia zariadenia – ak máte pochybnosti o zariadení pripojenom k vašej sieti, skontrolujte názov dodávateľa alebo výrobcu uvedený pod názvom zariadenia. Môže vám to pomôcť identifikovať, o aký druh zariadenia ide. Zmeňte názov zariadenia, aby ste ho nabudúce ľahko spoznali.
Odpojenie zariadenia – ak si nie ste istý, že pripojené zariadenie je pre vašu sieť alebo zariadenia bezpečné, upravte sieťový prístup pre dané zariadenie v nastaveniach routera alebo zmeňte sieťové heslo.
Ochrana – na ochranu svojho zariadenia pred útokmi a škodlivým softvérom nainštalujte na zariadenie kybernetickú ochranu a pravidelne aktualizujte operačný systém a nainštalovaný softvér. Ak chcete zostať chránený, nepripájajte sa k nezabezpečeným sieťam Wi-Fi.

Toto zariadenie

Toto zariadenie predstavuje váš počítač na sieti.
Sieťové adaptéry – zobrazia sa informácie o vašich sieťových adaptéroch.

Oznámenia zo Strážcu siete

V tejto kapitole uvádzame zoznam oznámení, ktoré sa môžu používateľovi zobraziť, ak program ESET Internet Security nájde nejaký bezpečnostný problém súvisiaci s routerom. Každé oznámenie zahŕňa krátky popis problému, ako aj odporúčané riešenie, ktoré vám pomôže minimalizovať bezpečnostné riziko zistené na routeri. Ak sami neviete alebo si netrúfate robiť zmeny v routeri, odporúčame vám kontaktovať výrobcu routera alebo poskytovateľa internetového pripojenia.

Nájdená potenciálna zraniteľnosť
Váš router môže obsahovať známe zraniteľnosti, vinou ktorých môže byť ľahko zraniteľný voči útokom alebo zneužitiu. Aktualizujte firmvér svojho routera.

Nájdená zraniteľnosť
Váš router obsahuje známe zraniteľnosti, vinou ktorých môže byť ľahko zraniteľný voči útokom a zneužitiu. Aktualizujte firmvér svojho routera.

Našla sa hrozba
Váš router je napadnutý malvérom. Reštartujte router a opakujte kontrolu.

Slabé heslo routera
Heslo vášho routera je slabé a je možné ho ľahko uhádnuť. Zmeňte heslo svojho routera.

Škodlivé sieťové presmerovanie
Váš prenos dát do siete internet sa zdá byť presmerovaný na škodlivé webové stránky. Toto môže znamenať, že zabezpečenie vášho routera bolo prelomené. Zmeňte nastavenia DNS servera na vašom routeri.

Služby otvorenej siete
Na vašom routeri sú spustené sieťové služby, ktoré môžu byť zneužité. Môže to byť v dôsledku slabej konfigurácie alebo prelomenej ochrany routera. Skontrolujte konfiguráciu svojho routera.

Citlivé služby otvorenej siete
Na vašom routeri sú spustené citlivé sieťové služby, ktoré môžu byť zneužité. Môže ísť o dôsledok slabej konfigurácie alebo prelomenej ochrany routera. Skontrolujte konfiguráciu svojho routera.

Firmvér je neaktuálny
Firmvér na vašom routeri je neaktuálny a môže obsahovať zraniteľnosti. Aktualizujte firmvér svojho routera.

Škodlivé nastavenie routera
DNS server, ktorý používa váš router, je škodlivý a môže vás smerovať na nebezpečné webové stránky. Toto môže znamenať, že zabezpečenie vášho routera bolo prelomené. Zmeňte nastavenia DNS servera na vašom routeri.

Sieťové služby
Na vašom routeri sú spustené bežné sieťové služby. Tieto služby sú potrebné pre sieť a pravdepodobne sú bezpečné. Skontrolujte konfiguráciu routera.

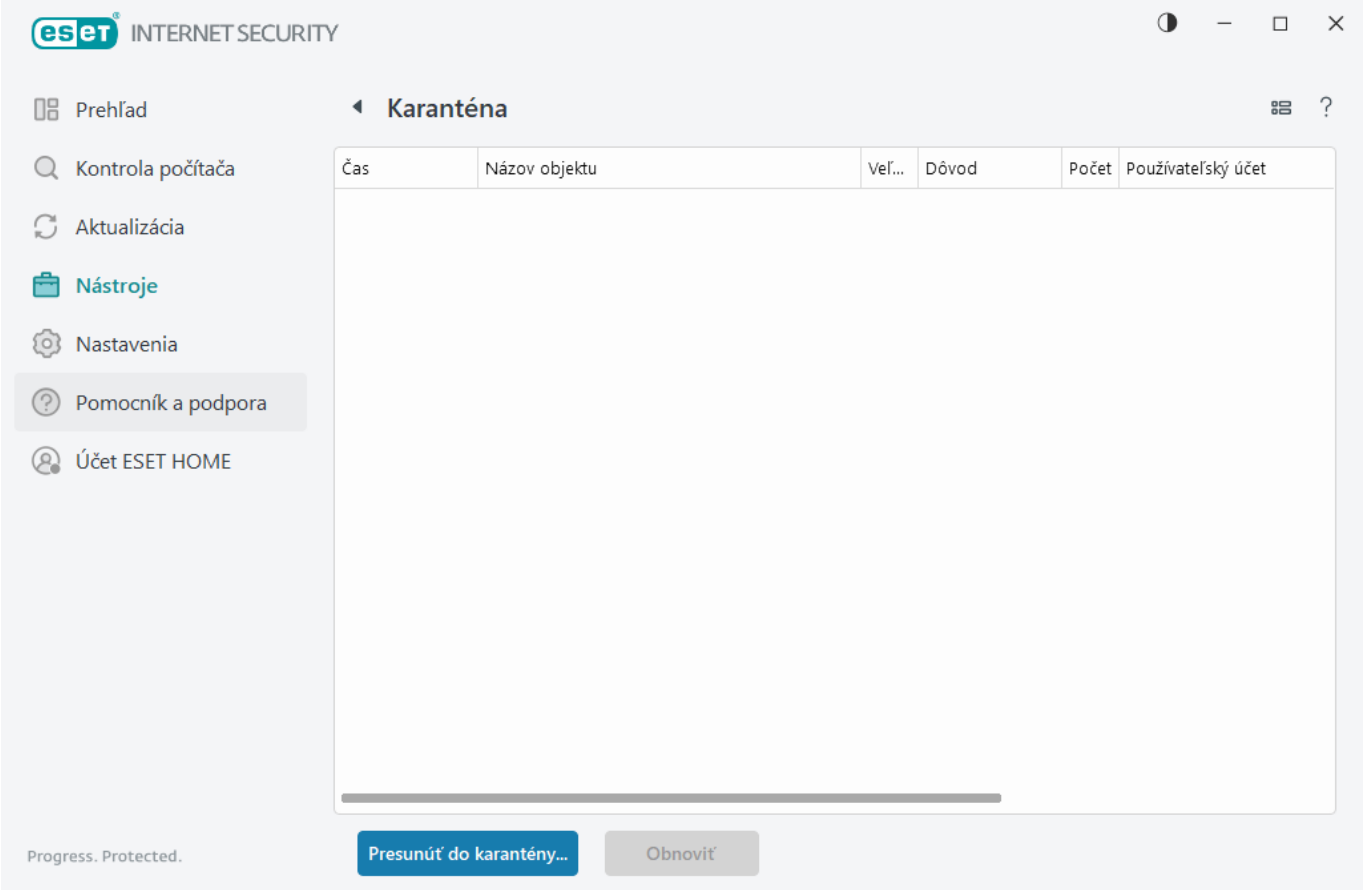
Karanténa

Hlavnou funkciou karantény je bezpečné uloženie detegovaných objektov (napríklad malvéru, infikovaných súborov alebo potenciálne nechcených aplikácií).

Karanténa je prístupná z hlavného okna programu ESET Internet Security po kliknutí na **Nástroje** > **Karanténa**.

Súbory uložené v karanténe si môžete prezrieť v prehľadnej tabuľke, ktorá obsahuje tieto informácie:

- dátum a čas presunutia súboru do karantény,
- cesta k pôvodnému umiestneniu súboru,
- veľkosť súboru v bytoch,
- dôvod (napr. objekt pridaný používateľom),
- počet detekcií (napr. opakovaná detekcia toho istého súboru alebo archív obsahujúci viacero infiltrácií).



Presunutie súborov do karantény

ESET Internet Security automaticky presunie odstránené súbory do karantény (ak ste túto možnosť nedeaktivovali v okne s upozornením).

Ďalšie súbory by mali byť presunuté do karantény, ak:

a.ich nie je možné vyliečiť,

b.nie je bezpečné alebo vhodné ich odstrániť,

c.sú nesprávne detegované programom ESET Internet Security,

d.sa správajú podozrivo, ale nie sú detegované ochranou.

Súbory môžete presunúť do karantény viacerými spôsobmi:

a.Manuálne presuniete súbor do karantény tak, že naň kliknete a podržíte tlačidlo myši stlačené, potom presuniete kurzor myši do vyznačeného priestoru a uvoľníte prst. Aplikácia sa následne presunie do popredia.

b.Pravým tlačidlom myši kliknite na súbor a vyberte **Pokročilé možnosti** > **Presunúť súbor do karantény**.

c.V okne **Karanténa** kliknite na tlačidlo **Presunúť do karantény**.

d.Na tento účel môžete použiť aj kontextové menu. V okne **Karanténa** kliknite pravým tlačidlom myši a z kontextového menu vyberte **Presunúť do karantény**.

Obnovenie súborov z karantény

Súbory presunuté do karantény možno obnoviť do ich pôvodného umiestnenia:

- Na tento účel použite funkciu **Obnoviť**, ktorá je k dispozícii v kontextovom menu po kliknutí pravým tlačidlom myši na daný súbor v karanténe.
- Ak je súbor označený ako potenciálne nechcená aplikácia, možnosť **Obnoviť a vylúčiť z kontroly** bude zapnutá. Prečítajte si tiež kapitolu Vylúčenia.
- Kontextové menu ponúka aj možnosť **Obnoviť do**, ktorá vám umožňuje obnoviť súbor do iného umiestnenia, než bolo to pôvodné, z ktorého bol súbor vymazaný.
- Funkcia obnovenia súborov nie je v niektorých prípadoch k dispozícii, napr. pri súboroch na zdieľanom mieste v sieti určených len na čítanie.

Odstránenie súborov z karantény

Kliknite pravým tlačidlom na danú položku a vyberte možnosť **Odstrániť z karantény** alebo vyberte položku, ktorú chcete odstrániť, a stlačte kláves **Delete**. Ak chcete vybrať a odstrániť všetky položky v karanténe, môžete na klávesnici stlačiť **Ctrl + A** a potom **Delete**. Odstránené položky budú natrvalo vymazané z vášho zariadenia a z karantény.

Posielanie súboru z karantény na analýzu

Ak máte v karanténe uložený podozrivý súbor, ktorý program nedetegoval alebo ho detegoval nesprávne (napr. prostredníctvom heuristickej analýzy kódu) a následne presunul do karantény, pošlite jeho vzorku na analýzu do výskumného laboratória ESET. Súbor odošlete tak, že naň kliknete pravým tlačidlom a z kontextového menu vyberiete **Poslať na analýzu**.

Popis detekcie

Ak na položku kliknete pravým tlačidlom a zvolíte možnosť **Popis detekcie**, otvorí sa ESET Encyklopédia hrozieb s podrobnými informáciami o zachytenej infiltrácii vrátane prejavov jej prítomnosti v systéme a bezpečnostných hrozieb, ktoré sa s ňou spájajú.

Ilustrované inštrukcie

Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:

- Obnovenie súboru z karantény v programe ESET Internet Security
- Odstránenie súboru z karantény v programe ESET Internet Security
- Môj produkt ESET ma upozornil na detekciu. Čo mám robiť?

Uloženie do karantény nebolo úspešné

Ak určité súbory nie je možné presunúť do karantény, dôvody sú nasledujúce:

- **Nemáte povolenia na čítanie** – to znamená, že nemôžete zobraziť obsah súboru.
- **Nemáte povolenia na zápis** – to znamená, že nemôžete meniť obsah súboru, t. j. pridať nový obsah alebo odstrániť existujúci obsah.
- **Súbor, ktorý sa pokúšate presunúť do karantény, je príliš veľký** – je potrebné zmenšiť veľkosť súboru.

Keď sa vám zobrazí chybové hlásenie „Uloženie do karantény nebolo úspešné“, kliknite na tlačidlo **Viac informácií**. Zobrazí sa okno karantény, kde uvidíte názov súboru a dôvod, prečo sa súbor nepodarilo presunúť do karantény.

Vybrať vzorku na analýzu

Ak vo svojom počítači nájdete podozrivý súbor alebo na internete narazíte na podozrivú stránku, môžete takéto vzorky poslať na analýzu do výskumného laboratória ESET Research Lab (nemusí byť k dispozícii vzhľadom na konfiguráciu ESET LiveGrid®).

Pred zaslaním vzorky do spoločnosti ESET

Vzorku pošlite do spoločnosti ESET na analýzu len v tom prípade, že spĺňa aspoň jednu z nasledujúcich podmienok:

- Vzorka nie je vaším produktom ESET vôbec detegovaná.
- Vzorka je nesprávne detegovaná ako hrozba.
- Súkromné súbory (ktoré by ste chceli nechať spoločnosťou ESET skontrolovať na prítomnosť malvéru) neprijímame ako vzorky (výskumné laboratórium spoločnosti ESET nevykonáva kontroly používateľských súborov na vyžiadanie).
- Pri zasielaní vzorky na analýzu uveďte výstižný predmet správy a poskytnite čo najviac informácií o vzorke (napr. snímka obrazovky alebo webová stránka, z ktorej ste podozrivý súbor stiahli).

Vzorku (súbor alebo webovú stránku) môžete na analýzu do spoločnosti ESET poslať jedným z nasledujúcich spôsobov:

1. Použite formulár na zaslanie vzorky, ktorý je dostupný priamo z vášho produktu ESET. Prejdite do sekcie **Nástroje** > **Odoslanie vzorky na analýzu**. Maximálna veľkosť odoslanej vzorky je 256 MB.

2. Vzorku na analýzu môžete odoslať aj prostredníctvom e-mailu. Súbor zabaľte do archívu pomocou WinRAR/WinZIP a ochráňte heslom „infected“. Následne ho odošlite na adresu samples@eset.com.

3. Ak chcete nahlásiť spam alebo, naopak, e-mail nesprávne zaradený medzi spam, prípadne nesprávne kategorizované webové stránky v Rodičovskej kontrole, prečítajte si náš článok Databázy znalostí spoločnosti ESET.

Vo formulári s názvom **Vybrať vzorku na analýzu** v roletovom menu **Dôvod odoslania vzorky** vyberte popis, ktorý

najviac zodpovedá predmetu vašej správy:

- Podozrivý súbor
- Podozrivá stránka (stránka infikovaná malvérom)
- Nesprávne detegovaná stránka
- Nesprávne detegovaný súbor (súbor, ktorý je detegovaný ako hrozba, no v skutočnosti infikovaný nie je)
- Iné

Súbor/Stránka – cesta k súboru alebo webovej stránke, ktorú chcete odoslať na analýzu.

Kontaktný e-mail – kontaktný e-mail bude odoslaný spolu s podozrivým súborom do spoločnosti ESET, aby v prípade potreby mohol byť použitý na vyžiadanie dodatočných informácií nevyhnutných k analýze. Zadanie kontaktného e-mailu nie je povinné. Ak svoju adresu zadať nechcete, označte možnosť **Odoslať anonymne**.

> **Kontaktovať vás budeme len v prípade potreby**
> Odpoveď na vami zaslanú vzorku vám zo spoločnosti ESET príde len v tom prípade, že budú pracovníci výskumného laboratória pri analýze potrebovať viac informácií. Každý deň používatelia na naše servery odošlú tisícky súborov, preto nie je možné každému odpovedať.
> Ak sa analýzou vzorky preukáže, že ide o nebezpečnú aplikáciu alebo webovú stránku, jej detekcia bude zahrnutá do najbližšej aktualizácie.

Vybrať vzorku na analýzu – Podozrivý súbor

Pozorované príznaky a symptómy infikovania malvérom – opíšte správanie podozrivého súboru v systéme, čo umožní jeho presnejšiu analýzu.

Pôvod súboru (URL adresa alebo výrobca aplikácie) – uveďte pôvod súboru (zdroj) a popíšte, ako ste sa k súboru dostali.

Poznámky a dodatočné informácie – všetky ďalšie informácie, ktoré by mohli pomôcť pri identifikácii a spracovaní podozrivého súboru.

> Povinné je len prvé pole **Pozorované náznaky a symptómy infikovania malvérom**. Poskytnutie doplňujúcich informácií však našim laboratóriám dokáže výrazne zjednodušiť prácu pri identifikácii a spracovaní vzoriek.

Vybrať vzorku na analýzu – Podozrivá stránka

Z roletového menu **Aký je problém so stránkou?** vyberte jednu z nasledujúcich možností:

- **Infikovaná** – webová stránka, ktorá obsahuje alebo rôznymi spôsobmi rozširuje vírusy a iný malvér.
- **Phishingová** – snaží sa získať citlivé údaje, ako napríklad čísla bankových účtov, PIN kódy a iné. Viac o tomto type útoku sa môžete dočítať v slovníku pojmov.
- **Podvodná** – falošná alebo podvodná webová stránka, ktorej cieľom je rýchly zisk pomocou zavádzania jej

návštevníkov.

- Ak stránka nespĺňa žiadnu z uvedených vlastností, vyberte možnosť **Iné**.

Poznámky a dodatočné informácie – uveďte všetky ďalšie informácie alebo popis, ktoré by mohli pomôcť pri analýze podozrivej webovej stránky.

Vybrať vzorku na analýzu – Nesprávne detegovaný súbor

Prosíme vás, aby ste nám posielali súbory, ktoré boli vyhodnotené ako infikované, ale v skutočnosti infikované nie sú. Pomôžete nám tým vylepšiť naše antivírusové a antispyvérové jadro a zvýšiť tak účinnosť ochrany pre ostatných používateľov. Falošný poplach (False positive – FP) môže nastať vtedy, keď sa štruktúra alebo charakteristika konkrétneho súboru zhoduje so vzorom obsiahnutým v detekčnom jadre.

Názov a verzia aplikácie – názov programu a jeho verzia (napr. číslo, alias alebo krycí názov).

Pôvod súboru (URL adresa alebo výrobca aplikácie) – uveďte pôvod súboru (zdroj) a popíšte, ako ste sa k danému súboru dostali.

Účel aplikácie – uveďte účel a typ aplikácie (napr. prehliadač, prehrávač médií atď.) pre rýchlejšie zaradenie a identifikáciu.

Poznámky a dodatočné informácie – všetky ďalšie informácie, ktoré by mohli pomôcť pri identifikácii a spracovaní podozrivého súboru.

> Prvé tri parametre sú povinné z dôvodu lepšej identifikácie legitímnej aplikácie a jej odlíšenia od škodlivého kódu. Poskytnutím doplňujúcich informácií pomôžete významnou mierou našim laboratóriám pri identifikácii a spracovaní vzoriek.

Vybrať vzorku na analýzu – Nesprávne detegovaná stránka

Prosíme vás, aby ste nám posielali webové stránky, ktoré boli vyhodnotené ako infikované, podvodné či phishingové, avšak v skutočnosti neobsahujú žiaden škodlivý obsah. Falošný poplach (False positive – FP) môže nastať vtedy, keď sa štruktúra alebo charakteristika konkrétneho súboru zhoduje so vzorom obsiahnutým v detekčnom jadre. Zaslaním nesprávne detegovanej stránky nám umožníte vylepšiť naše antivírusové a antiphishingové jadro a zvýšiť tak účinnosť ochrany pre ostatných používateľov.

Poznámky a dodatočné informácie – všetky ďalšie informácie, ktoré by mohli pomôcť pri identifikácii a spracovaní podozrivej webovej stránky.

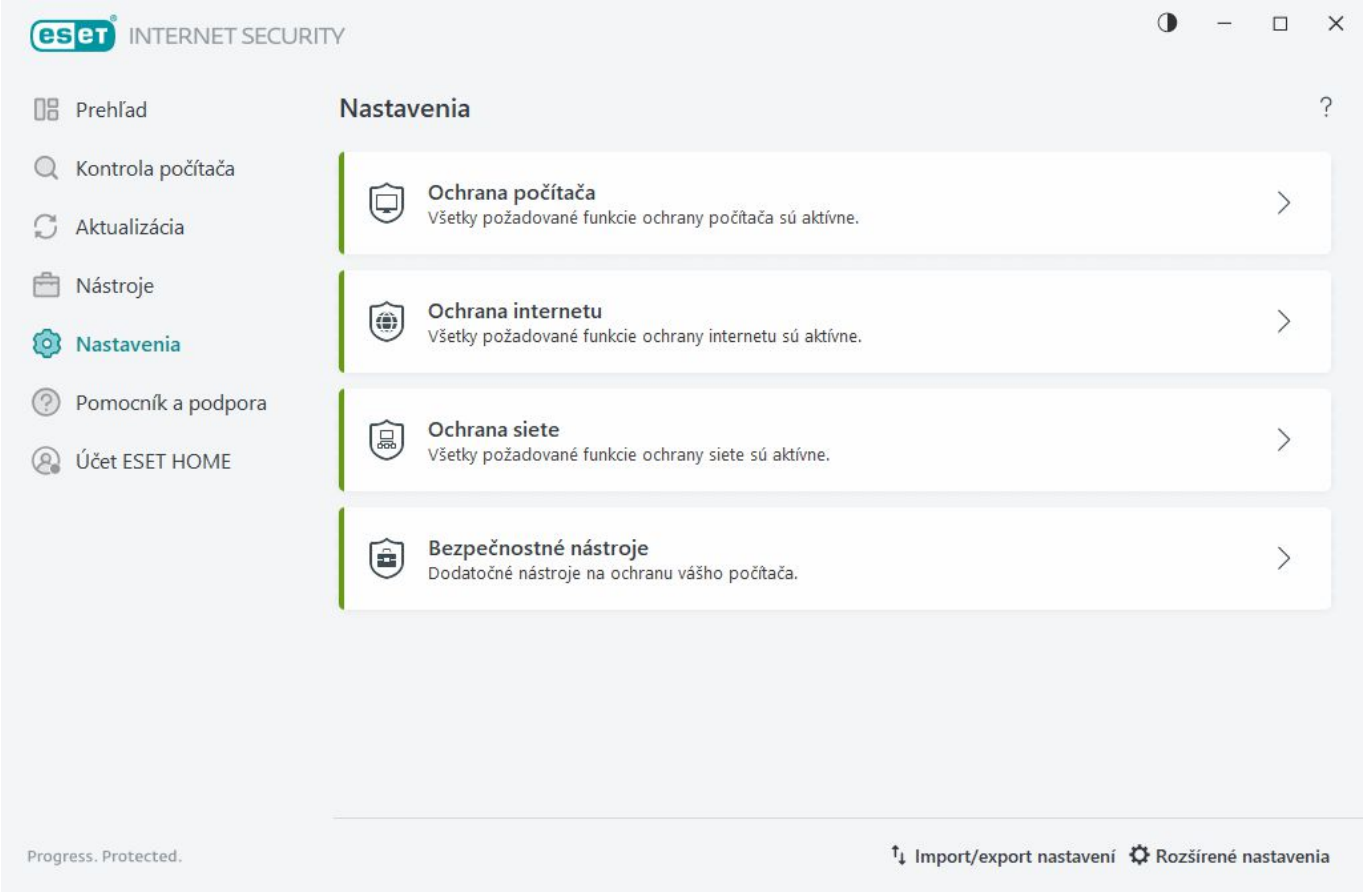
Vybrať vzorku na analýzu – Iné

Tento formulár sa používa v prípade, že súbor nie je možné kategorizovať ako **Podozrivý súbor** ani ako **Nesprávne detegovaný súbor**.

Dôvod odoslania súboru – uveďte dôvod odoslania súboru a čo najpresnejší popis súboru.

Nastavenia

Skupiny dostupných funkcií ochrany nájdete v hlavnom okne programu > **Nastavenia**.



Sekcia **Nastavenia** je rozdelená na nasledujúce časti:

Ochrana počítača

Ochrana internetu

Ochrana siete

Bezpečnostné nástroje

Ďalšie možnosti nastavení sú dostupné v dolnej časti okna. Kliknutím na Rozšírené nastavenia sa dostanete k podrobným parametrom každého modulu. Funkciu Import/export nastavení môžete použiť na načítanie nastavení uložených v súbore .xml do produktu alebo na uloženie aktuálnych nastavení produktu do konfiguračného súboru.

Ochrana počítača

Kliknutím na položku **Ochrana počítača** cez hlavné okno programu > **Nastavenia** zobrazíte prehľad všetkých modulov ochrany:

- Rezidentná ochrana súborového systému – všetky súbory, ktoré sa v počítači otvárajú, vytvárajú a spúšťajú, sú kontrolované na prítomnosť škodlivého kódu.
- Správa zariadení – tento modul umožňuje kontrolovať, blokovať a nastaviť rozšírené prístupové práva a pravidlá na filtrovanie prístupu používateľa k médiám (CD/DVD/USB...).
- Host Intrusion Prevention System (HIPS) – HIPS monitoruje udalosti vo vnútri operačného systému a reaguje na ne na základe stanovených pravidiel.
- Herný režim – zapnutie alebo vypnutie Herného režimu. Po zapnutí Herného režimu sa zobrazí upozornenie (potenciálne bezpečnostné riziko) a hlavné okno programu zmení farbu na oranžovú.
- Ochrana webovej kamery – kontroluje procesy a aplikácie, ktoré využívajú alebo majú prístup k webovej kamere vášho počítača.

Ak chcete pozastaviť alebo vypnúť jednotlivé moduly ochrany, kliknite na prepínacie tlačidlo .

Vypnutie modulov ochrany môže znížiť úroveň zabezpečenia vášho počítača.

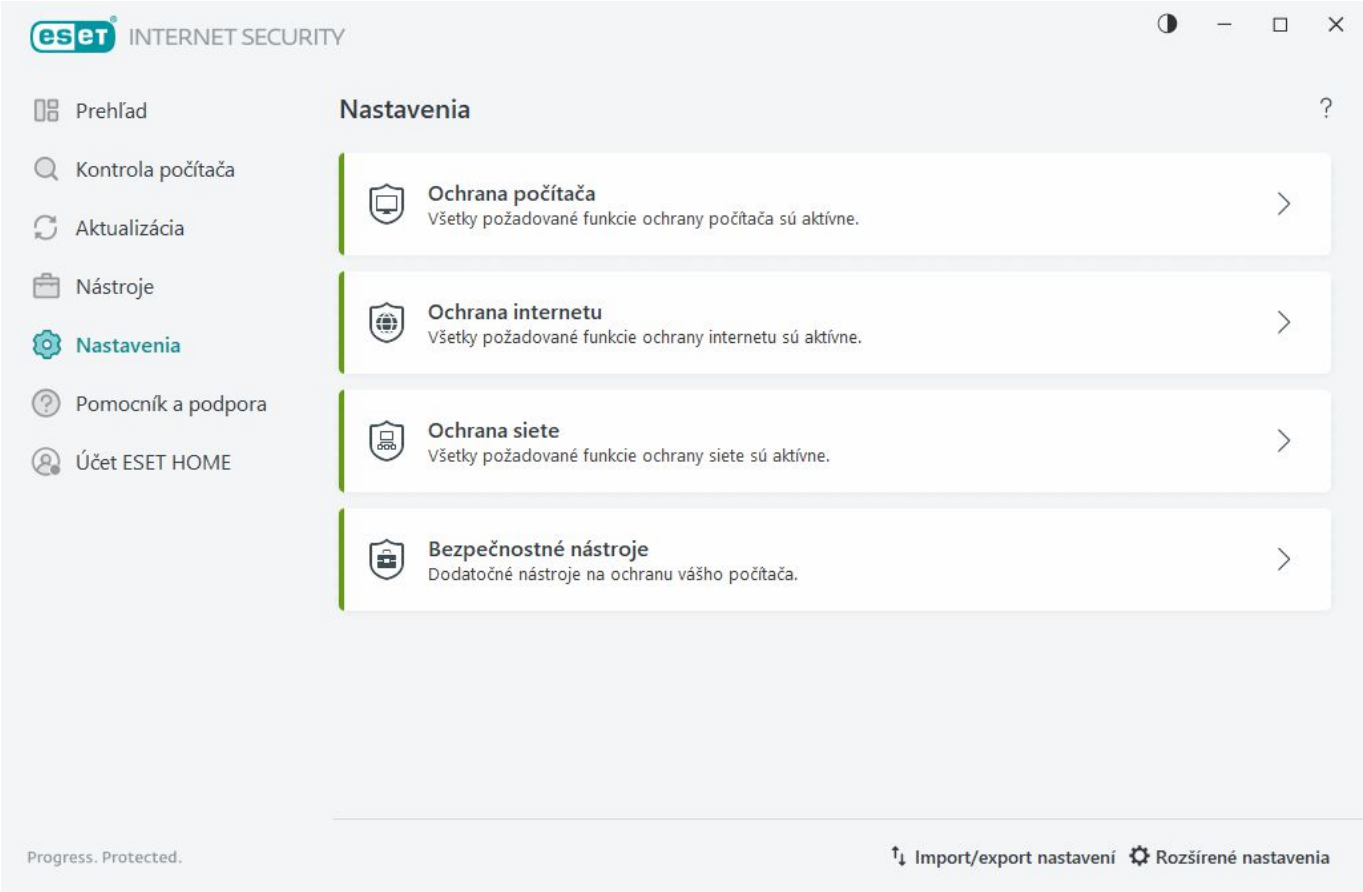
Kliknutím na ikonu ozubeného kolesa vedľa modulu ochrany prejdete do rozšírených nastavení daného modulu.

Po kliknutí na ikonu ozubeného kolesa vedľa **Rezidentnej ochrany súborového systému** máte na výber nasledujúce možnosti:

- **Konfigurovať** – otvoria sa rozšírené nastavenia Rezidentnej ochrany súborového systému.
- **Nastaviť vylúčenia** – otvorí sa okno na nastavenie vylúčení, v ktorom môžete nastaviť súbory a adresáre, ktoré nemajú byť kontrolované.

Po kliknutí na ikonu ozubeného kolesa vedľa **Ochrany webovej kamery** máte na výber nasledujúce možnosti:

- **Konfigurovať** – otvoria sa rozšírené nastavenia Ochrany webovej kamery.
- **Blokovať prístup až do reštartu** – zablokuje všetky pokusy o prístup k webovej kamere až do reštartu počítača.
- **Blokovať prístup natrvalo** – zablokuje všetky pokusy o prístup k webovej kamere, až pokým toto nastavenie nevypnete.
- **Zastaviť blokovanie prístupu** – zastaví blokovanie prístupu k webovej kamere. Táto možnosť je dostupná len v prípade, že bol prístup k webovej kamere predtým zablokovaný.



Pozastaviť antivírusovú a antispyvérovú ochranu – vypne všetky moduly antivírusovej a antispyvérovej ochrany. Ak vypnete ochranu, zobrazí sa okno, kde vyberiete **časový interval**, počas ktorého bude ochrana vypnutá. Túto možnosť používajte len v prípade, že ste skúsený používateľ, alebo na základe pokynov od technickej podpory spoločnosti ESET.

Našla sa infiltrácia

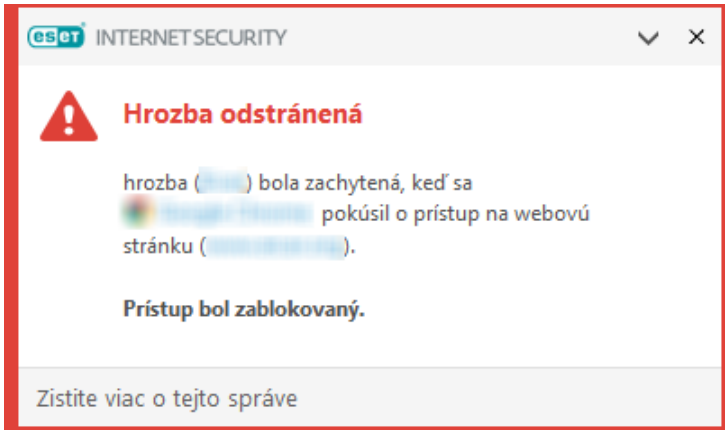
Infiltrácie sa môžu do systému dostať z rôznych zdrojov: z webových stránok, zo zdieľaných priečinkov, prostredníctvom e□mailu alebo z vymeniteľných médií (USB kľúče, externé disky, CD, DVD a pod.).

Štandardné správanie

V programe ESET Internet Security môžu byť infiltrácie zachytené pomocou nasledujúcich modulov:

- Rezidentná ochrana súborového systému
- Ochrana prístupu na web
- Ochrana e□mailových klientov
- Manuálna kontrola počítača

Každý z týchto modulov používa prednastavenú úroveň liečenia a pokúsi sa súbor buď vyliečiť a presunúť do Karantény, alebo preruší spojenie. Notifikácie sa zobrazujú v paneli oznámení v pravej dolnej časti obrazovky. Podrobné informácie o zachytených/vyliečených objektoch nájdete v kapitole Protokoly. Viac informácií o jednotlivých úrovniach liečenia a správaní nájdete v kapitole Úrovne liečenia.



Kontrola počítača na prítomnosť infikovaných súborov

Ak má váš počítač príznaky infekcie škodlivým kódom, napr. je pomalší alebo zamŕza, odporúčame vám postupovať nasledovne:

1.V hlavnom okne programu ESET Internet Security kliknite na **Kontrola počítača**.

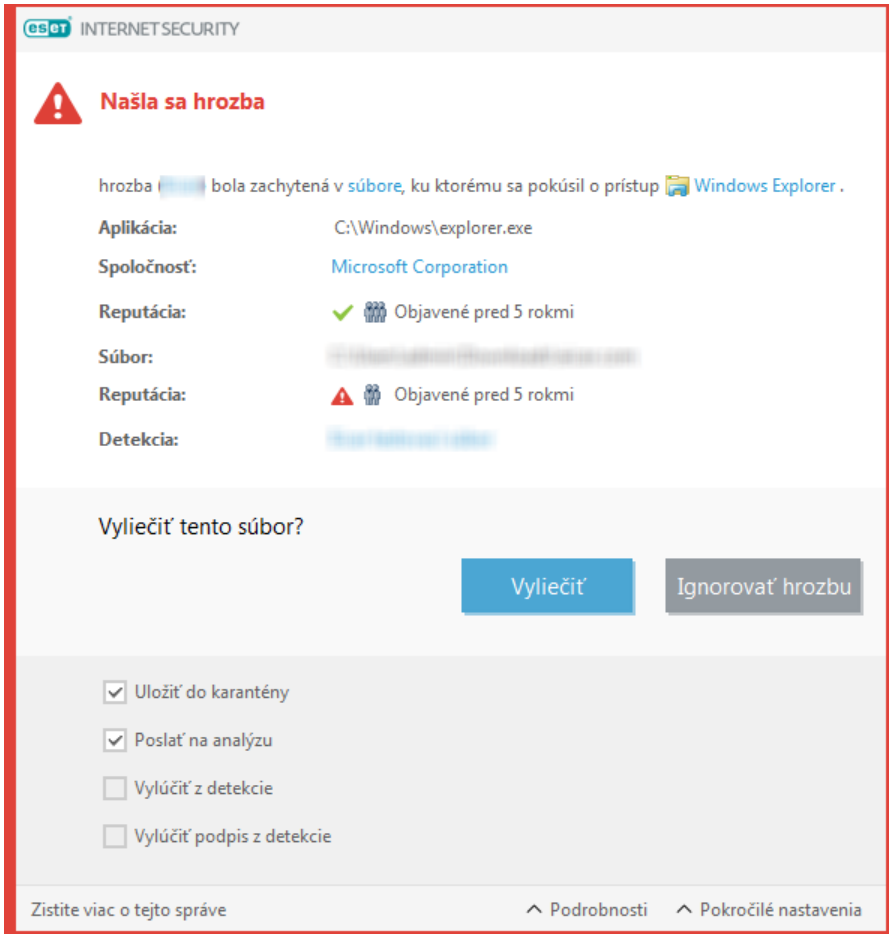
2.Kliknite na možnosť **Skontrolovať váš počítač** pre začatie kontroly vášho počítača (pre viac informácií si prečítajte kapitolu Kontrola počítača).

3.Po ukončení kontroly skontrolujte počet kontrolovaných, infikovaných a vyliečených súborov v protokole.

Ak chcete skontrolovať len určité časti svojho počítača, vyberte možnosť **Vlastná kontrola** a označte ciele kontroly.

Liečenie a mazanie

Ak rezidentná ochrana súborového systému nevie vybrať akciu, vyzve vás pomocou výstražného okna, aby ste akciu vybrali sami. Na výber sú spravidla akcie **Liečiť**, **Odstrániť** a **Žiadna akcia**. Možnosť **Žiadna akcia** sa neodporúča, nakoľko infiltrácia zostáva na svojom pôvodnom mieste, a tak stále predstavuje potenciálnu hrozbu. Výnimkou je, ak máte úplnú istotu, že daný súbor bol ako infiltrácia detegovaný omylom.



Liečenie sa dá aplikovať v prípade, že do súboru bola zavedená časť, ktorá obsahuje škodlivý kód. V tomto prípade má zmysel pokúsiť sa infikovaný súbor liečiť a dostať ho tak do pôvodného stavu. Ak súbor pozostáva výlučne zo škodlivého kódu, bude celý súbor odstránený.

V prípade, že súbor s infiltráciou je „držaný“, napr. systémovým procesom, môže nastať situácia, že nebude vymazaný okamžite, ale až po jeho uvoľnení po reštarte počítača.

Obnovenie súborov z karantény

Karanténa je prístupná z hlavného okna programu ESET Internet Security po kliknutí na **Nástroje** > **Karanténa**.

Súbory presunuté do karantény možno obnoviť do ich pôvodného umiestnenia:

- Na tento účel použite funkciu **Obnoviť**, ktorá je k dispozícii v kontextovom menu po kliknutí pravým tlačidlom myši na daný súbor v karanténe.
- Ak je súbor označený ako potenciálne nechcená aplikácia, možnosť **Obnoviť a vylúčiť z kontroly** bude zapnutá. Prečítajte si tiež kapitolu Vylúčenia.
- Kontextové menu ponúka aj možnosť **Obnoviť do**, ktorá vám umožňuje obnoviť súbor do iného umiestnenia, než bolo to pôvodné, z ktorého bol súbor vymazaný.
- Funkcia obnovenia súborov nie je v niektorých prípadoch k dispozícii, napr. pri súboroch na zdieľanom mieste v sieti určených len na čítanie.

Viaceré hrozby

Ak pri kontrole počítača neboli niektoré infikované súbory vyliečené (prípadne úroveň liečenia bola nastavená na hodnotu **Neliečiť**), zobrazí sa okno s možnosťou výberu akcie pre jednotlivé súbory. Akcia sa nastavuje pre každý infikovaný súbor zvlášť a vykoná sa naraz pre všetky súbory po stlačení tlačidla **Vykonať**.

Mazanie súborov v archívoch

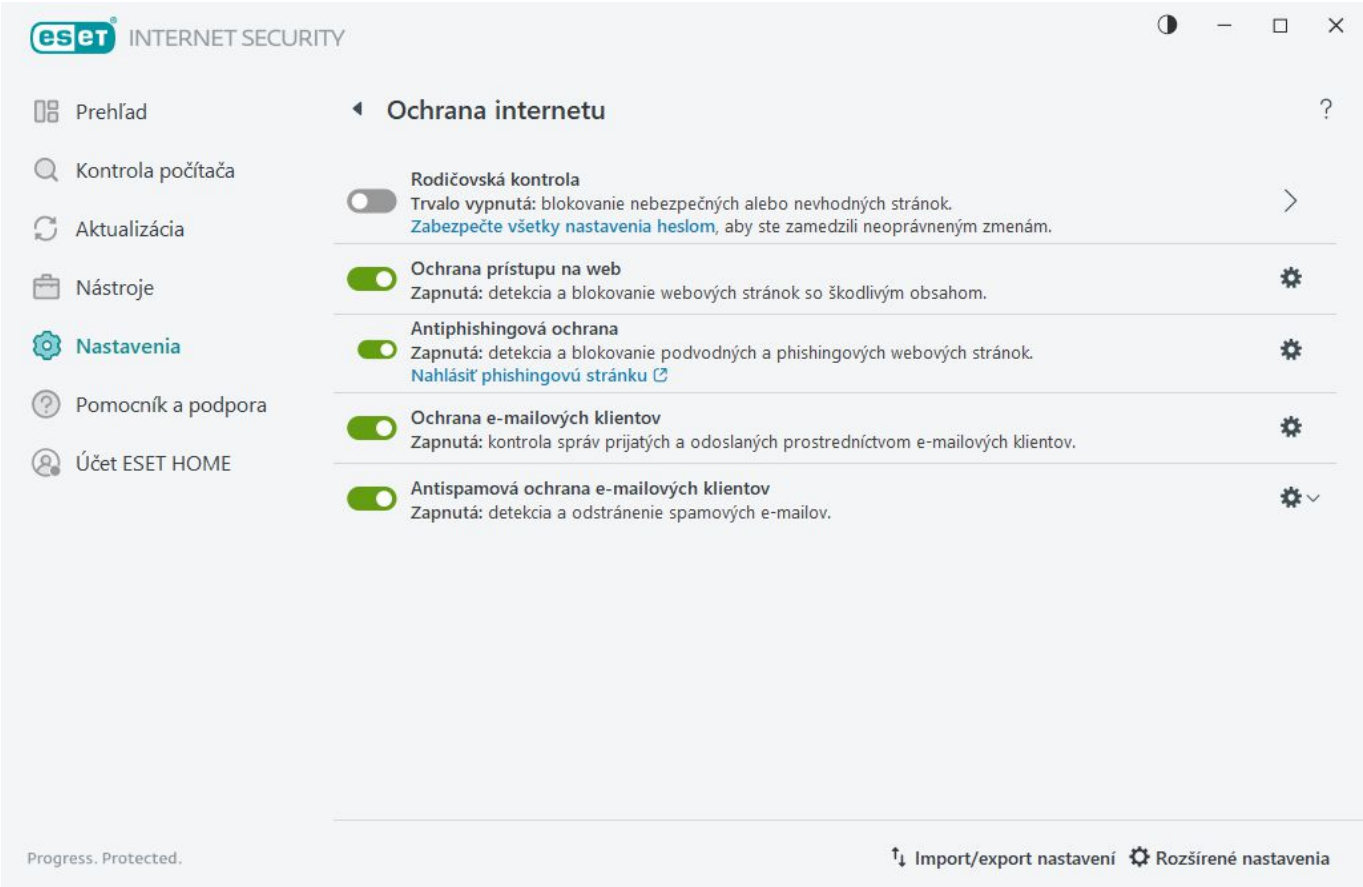
Pri štandardnej úrovni liečenia je archív vymazaný len v prípade, že obsahuje iba infikované súbory a žiadne iné bezpečné súbory. Archív teda nebude zmazaný, ak okrem infiltrácie obsahuje aj neškodné súbory. Obozretne postupujte pri nastavení prísnej úrovne liečenia, pretože v tomto prípade bude archív s infikovanými súbormi odstránený vždy bez ohľadu na to, či jeho obsah tvoria aj nejaké neškodné súbory.

Ochrana internetu

Internetové pripojenie patrí do štandardnej výbavy osobných počítačov. Zároveň sa stalo aj hlavným médiom prenosu škodlivého softvéru. Otvorte hlavné okno programu > **Nastavenia** > **Ochrana internetu** a nakonfigurujte funkcie v programe ESET Internet Security, ktoré zvyšujú ochranu internetu.

Ak chcete pozastaviť alebo vypnúť jednotlivé moduly ochrany, kliknite na prepínacie tlačidlo .

Vypnutie modulov ochrany môže znížiť úroveň zabezpečenia vášho počítača.



Kliknutím na ikonu ozubeného kolesa vedľa modulu ochrany prejdete do rozšírených nastavení daného modulu.

Modul Rodičovskej kontroly chráni vaše deti na internete blokovaním nevhodného a škodlivého obsahu.

Ochrana prístupu na web kontroluje HTTP/HTTPS komunikáciu na prítomnosť malvéru a phishingu. Ochranu prístupu na web by ste mali vypnúť len v prípade riešenia problémov.

Antiphishingová ochrana umožňuje blokovať webové stránky podozrivé z phishingu. Odporúčame ponechať túto funkciu zapnutú.

Nahlásiť phishingovú stránku – nahláste phishingovú/škodlivú webovú stránku na analýzu spoločnosťou ESET.

> Skôr ako pošlete stránku do spoločnosti ESET na analýzu, uistite sa, že spĺňa aspoň jedno z nasledujúcich kritérií:
> • Webová stránka ešte nie je v programe detegovaná.
> • Webová stránka sa nesprávne deteguje ako hrozba. V takom prípade kliknite na odkaz Nahlásiť nesprávne blokovanú stránku.

Ochrana e-mailových klientov zabezpečuje kontrolu e-mailovej komunikácie prijímanej prostredníctvom protokolov POP3(S) a IMAP(S). Pomocou doplnku (pluginu) do e-mailových klientov zabezpečuje ESET Internet Security kontrolu všetkej komunikácie týchto klientov.

Antispamová ochrana e-mailových klientov filtruje nevyžiadané e-mailové správy.

Po kliknutí na ikonu ozubeného kolesa vedľa **Antispamovej ochrany e-mailových klientov** máte na výber nasledujúce možnosti:

- **Konfigurovať** – otvoria sa rozšírené nastavenia pre antispamovú ochranu e-mailových klientov.

- **Používateľský zoznam adries** (ak je povolený) – otvorí sa dialógové okno, kde môžete pridávať, upravovať alebo mazať adresy a definovať pravidlá antispamu. Pravidlá v tomto zozname sa budú vzťahovať na aktuálneho používateľa.

- **Globálny zoznam adries** (ak je povolený) – otvorí sa dialógové okno, kde môžete pridávať, upravovať alebo mazať adresy a definovať pravidlá antispamu. Pravidlá v tomto zozname sa budú vzťahovať na všetkých používateľov.

Antiphishingová ochrana

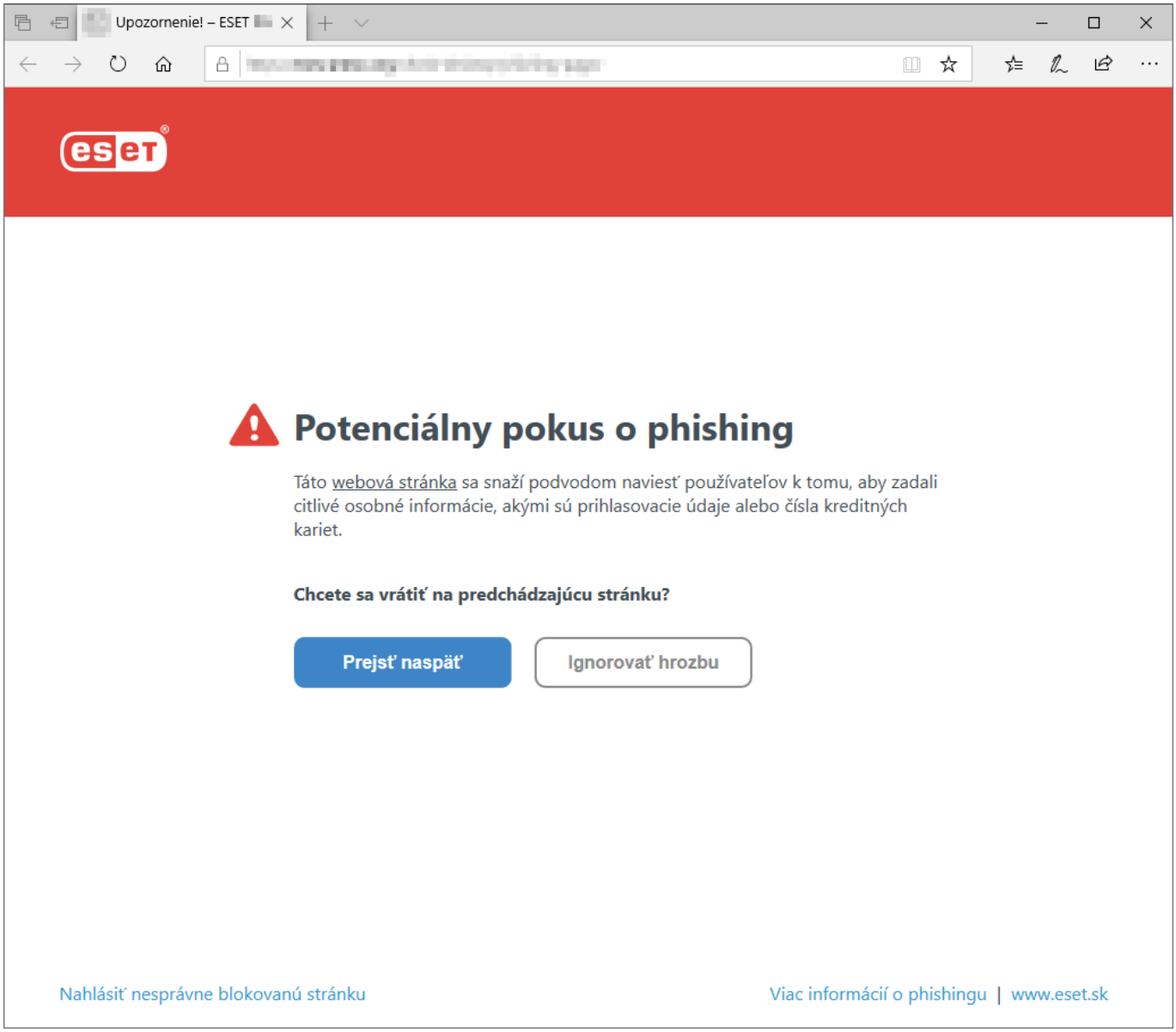
Termín phishing označuje kriminálnu aktivitu, ktorá používa techniky sociálneho inžinierstva (manipulovanie používateľov na získanie dôverných informácií). Jej cieľom je získať prístup k citlivým dátam, ako sú heslá k bankovým účtom, PIN kódy a iné detaily. Viac o tomto type aktivity sa môžete dočítať v slovníku pojmov. ESET Internet Security má zabudovanú ochranu pred phishingom, vďaka ktorej sú známe webové stránky s týmto typom obsahu blokované.

Antiphishingová ochrana je na základe predvolených nastavení zapnutá. Toto nastavenie je možné konfigurovať v sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana prístupu na web.**

Viac informácií o Antiphishingovej ochrane v programe ESET Internet Security nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Prístup na phishingovú stránku

Ak navštívite phishingovú stránku, otvorí sa vám v prehliadači nasledujúce upozornenie. Ak aj napriek tomu chcete prejsť na stránku, kliknite na **Ignorovať hrozby** (neodporúča sa).



Povolenie potenciálnej phishingovej stránky horeuvedeným spôsobom vyprší v produkte po niekoľkých hodinách. Ak chcete konkrétnu webovú stránku povoliť natrvalo, použite nástroj Manažment URL adries. V sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana prístupu na web** > **Manažment URL adries** > **Zoznam adries** > **Upraviť** pridajte požadovanú webovú stránku do zoznamu.

Nahlásenie phishingovej stránky

Odkaz **Nahlásiť nesprávne blokovanú stránku** vám umožňuje nahlásiť webovú stránku, ktorá je nesprávne detegovaná ako hrozba.

Webovú stránku môžete odoslať na analýzu aj prostredníctvom e-mailu. V takom prípade ju pošlite na adresu samples@eset.com. Nezabudnite uviesť výstižný predmet správy a čo najviac informácií o webovej stránke (napr. URL adresa, z ktorej ste sa na túto stránku dostali, ako ste sa o nej dozvedeli a pod.).

Rodičovská kontrola

Modul Rodičovská kontrola umožňuje konfigurovať nastavenia rodičovskej kontroly, ktoré rodičom pomáhajú chrániť deti pri používaní internetu a nastavovať obmedzenia pre používanie zariadení a služieb. Hlavnou úlohou rodičovskej kontroly je zamedziť deťom a dospievajúcej mládeži prístup na webové stránky s nebezpečným alebo nevhodným obsahom.

Rodičovská kontrola vám umožňuje blokovať webové stránky, ktoré môžu obsahovať nevhodný obsah. Okrem toho môžete zakázať prístup na 40 predvolených kategórií a 140 podkategórií webových stránok.

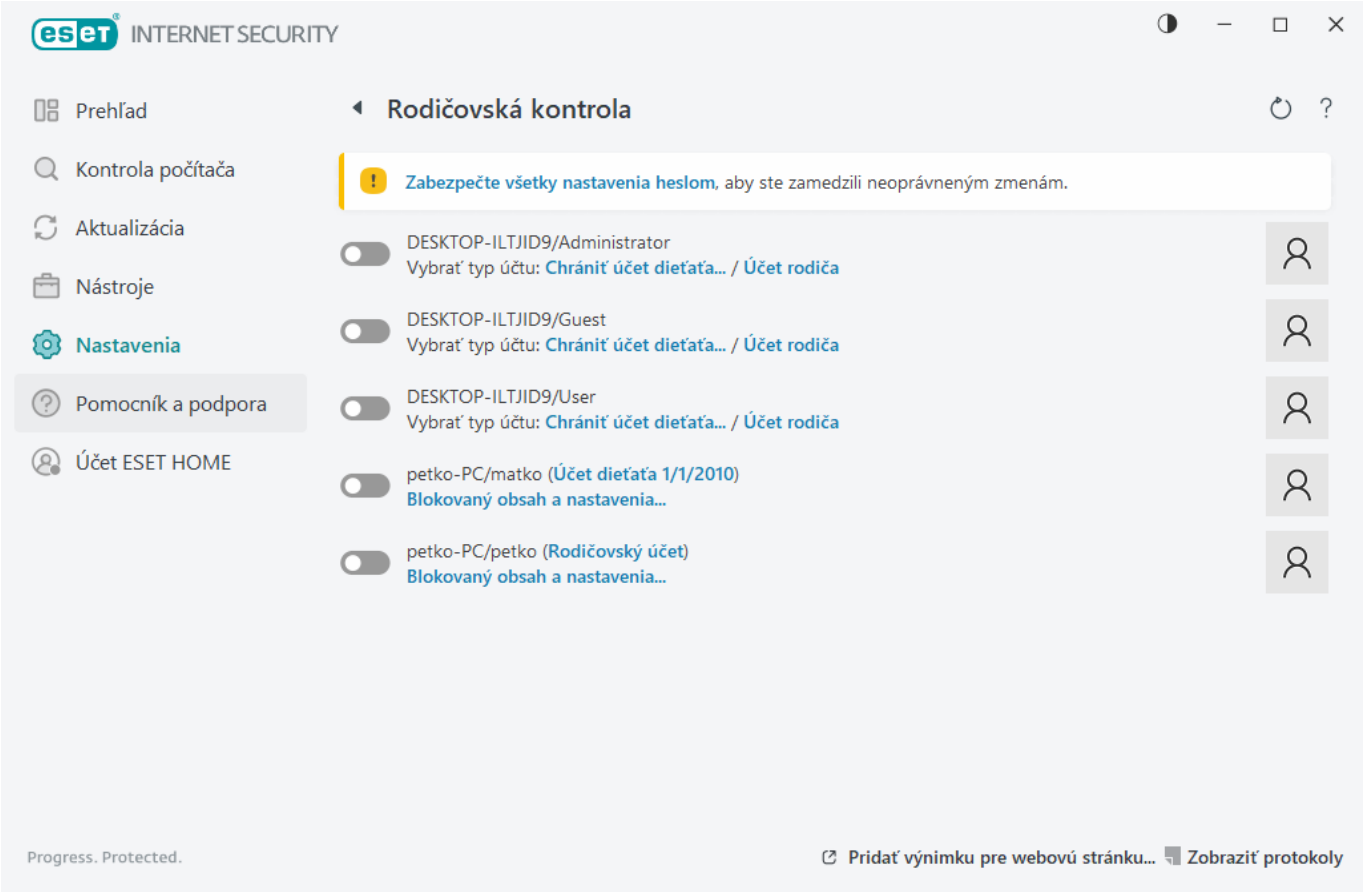
Pre aktiváciu Rodičovskej kontroly pre konkrétny používateľský účet postupujte podľa nasledujúcich inštrukcií:

1. V predvolenom nastavení je Rodičovská kontrola v produkte ESET Internet Security vypnutá. Rodičovskú kontrolu môžete aktivovať dvoma spôsobmi:

   • V hlavnom okne programu v sekcii **Nastavenia** > **Ochrana internetu** > **Rodičovská kontrola** kliknite na prepínacie tlačidlo  a zmeňte stav modulu rodičovskej kontroly na zapnutý.

   • Prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana prístupu na web** > **Rodičovská kontrola** a kliknite na prepínacie tlačidlo vedľa možnosti **Zapnúť rodičovskú kontrolu**.

2. V hlavnom okne programu kliknite na **Nastavenia** > **Ochrana internetu** > **Rodičovská kontrola**. Napriek tomu, že je **Rodičovská kontrola Zapnutá**, musíte ešte nastaviť požadovaný používateľský účet. Kliknite na šípku a v nasledujúcom okne vyberte **Chrániť účet dieťaťa** alebo **Účet rodiča**. V zobrazenom okne zadajte dátum narodenia na určenie úrovne prístupu a webových stránok vhodných pre príslušný vek. Rodičovská kontrola bude teraz pre daný používateľský účet plne funkčná. Kliknite na **Blokovaný obsah a nastavenia** pod konkrétnym používateľským účtom, ak si želáte zmeniť kategórie webových stránok, ktoré budú povolené alebo blokované, na karte Kategórie. Pre povolenie či blokovanie vlastných webových stránok (ktoré nepatria ani do jednej predvolenej kategórie) kliknite na kartu Výnimky.



V hlavnom okne programu ESET Internet Security kliknite na **Nastavenia** > **Ochrana internetu** > **Rodičovská kontrola**. Zobrazené okno bude obsahovať nasledujúce prvky:

Používateľské účty systému Windows

V prípade, že máte vytvorenú rolu pre existujúci účet, zobrazí sa práve tu. Kliknite na prepínač vedľa účtu rodičovskej kontroly a uistite sa, že je zobrazený zelenou farbou. Pod aktívnym účtom kliknite na Blokovaný obsah a nastavenia a následne sa zobrazí zoznam kategórií webových stránok, ktoré môžete pre tento účet zablokovať alebo povoliť.

Dolná časť okna obsahuje:

Pridať výnimku pre webovú stránku – môžete zablokovať alebo povoliť webovú stránku samostatne pre každý používateľský účet podľa vášho rozhodnutia.

Zobraziť protokoly – zobrazí sa podrobný protokol o činnosti modulu Rodičovská kontrola (blokované stránky, účet, pre ktorý bola stránka zablokovaná, dôvod zablokovania atď.). Tento protokol tiež môžete filtrovať podľa vami zvolených kritérií, kliknutím na tlačidlo **Filtrovať**.

Rodičovská kontrola

Po vypnutí rodičovskej kontroly sa objaví okno **Vypnúť rodičovskú kontrolu**. Umožní vám zvoliť časové obdobie, počas ktorého bude modul vypnutý. Táto možnosť potom zmení svoj stav na **Pozastavená** alebo **Trvalo vypnutá**.

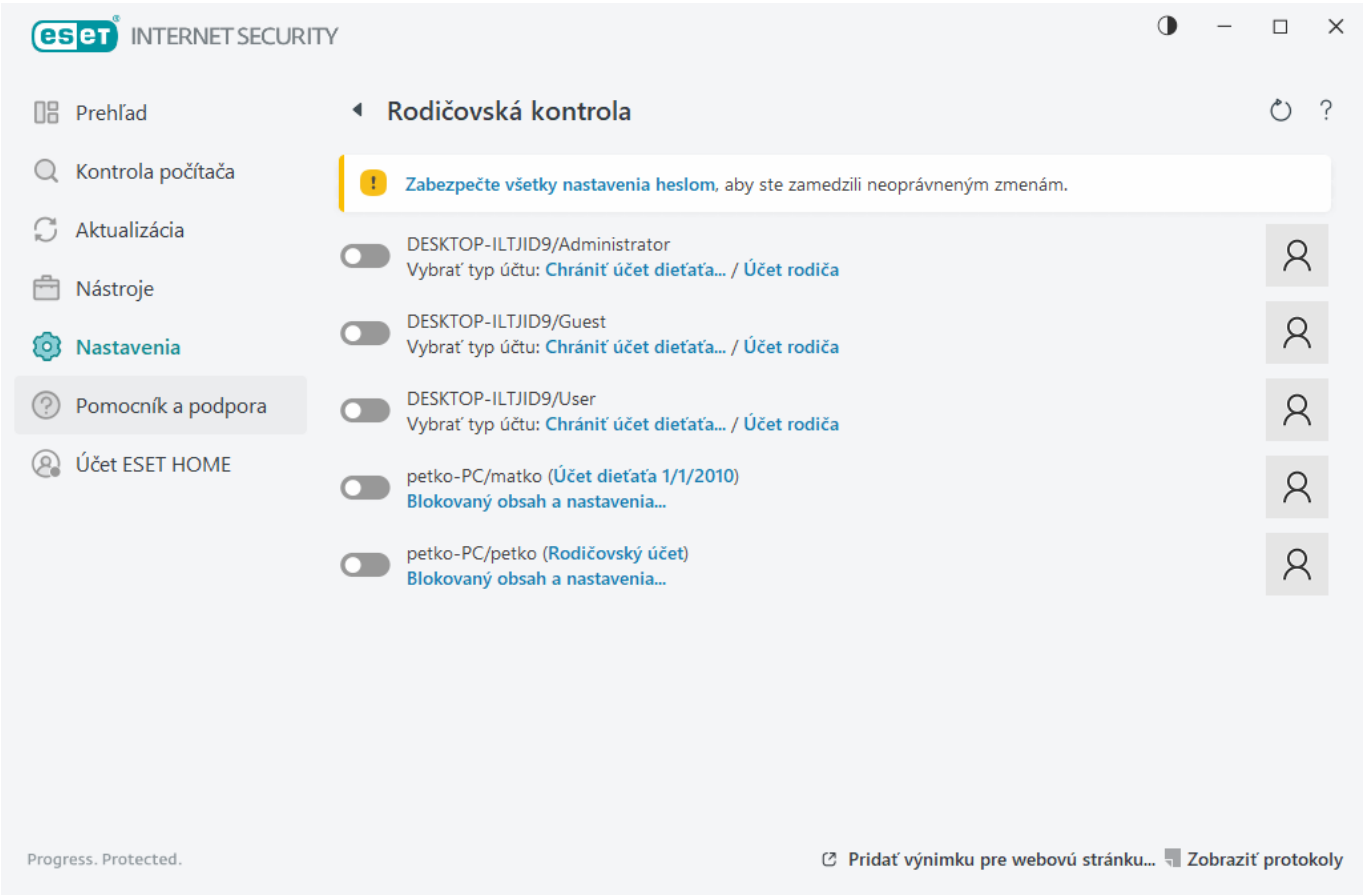
Je dôležité chrániť nastavenia v produkte ESET Internet Security heslom. Heslo môžete nastaviť v sekcii Nastavenia prístupu. Ak nie je nastavené heslo, zobrazí sa upozornenie **Zabezpečte všetky nastavenia heslom**, aby ste

zamedzili neautorizovaným zmenám. Obmedzenia nastavené v rodičovskej kontrole ovplyvnia iba štandardné používateľské účty. Pretože administrátor vie prekonať všetky obmedzenia, tieto nebudú mať želaný účinok.

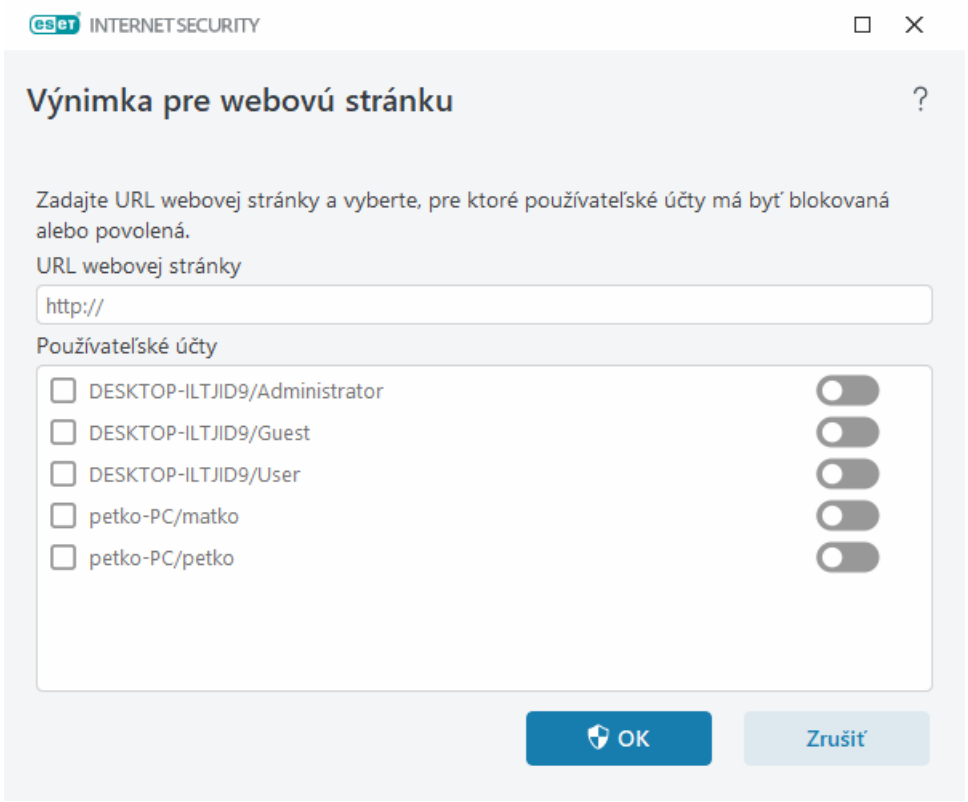
Na to, aby rodičovská kontrola fungovala správne, je potrebné zapnúť kontrolu sieťovej komunikácie, kontrolu komunikácie HTTP(S) a Firewall. Tieto funkcie sú v predvolených nastaveniach povolené.

Výnimky pre webové stránky

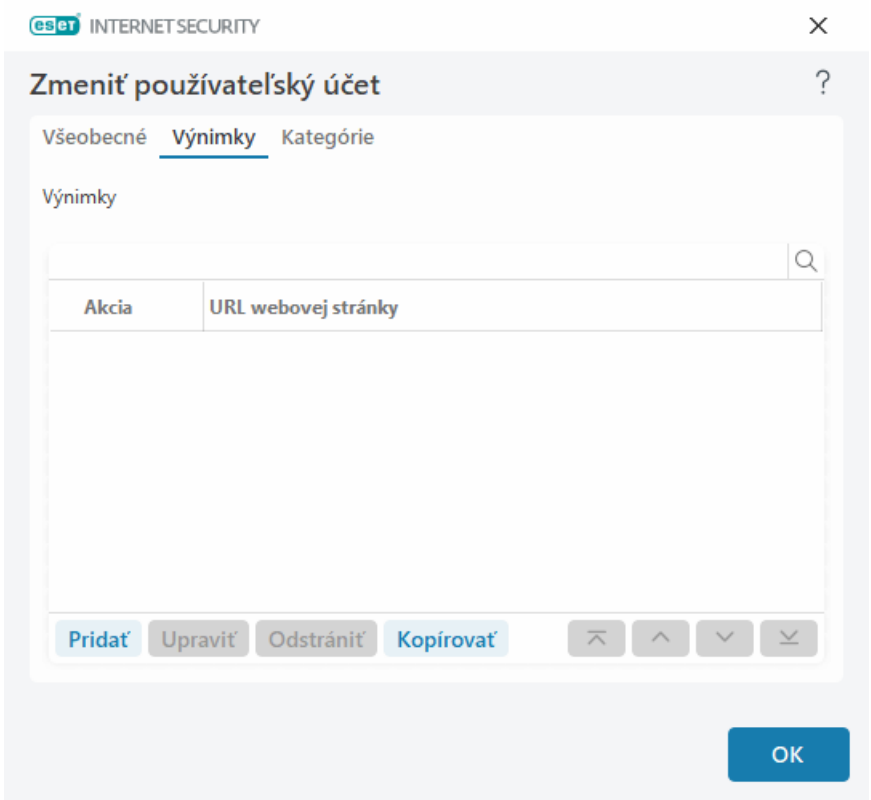
Ak chcete pridať výnimku pre webovú stránku, kliknite na **Nastavenia** > **Ochrana internetu** > **Rodičovská kontrola** a potom kliknite na **Pridať výnimku pre webovú stránku**.



Zadajte URL adresu do poľa **URL webovej stránky**, pre každý používateľský účet vyberte ✔ (povolené) alebo ⊘ (blokované) a kliknutím na **OK** pridajte stránku do zoznamu.



Ak chcete odstrániť URL adresu zo zoznamu, kliknite na **Nastavenia** > **Ochrana internetu** > **Rodičovská kontrola**, pod príslušným používateľským účtom kliknite na **Blokovaný obsah a nastavenia**, kliknite na kartu **Výnimky**, vyberte výnimku a kliknite na **Odstrániť**.



V zoznamoch URL adries nie je možné používať špeciálne znaky * (hviezdička) a ? (otáznik). Napríklad adresy webových stránok s viacerými TLD musíte zadať ručne (napríklad *examplepage.com*, *examplepage.sk*). Keď pridáte adresu do zoznamu, celý obsah nachádzajúci sa na danej doméne a všetkých jej subdoménach (napríklad *sub.examplepage.com*) bude blokovaný alebo povolený na základe toho, akú akciu ste pre URL vybrali.

Blokovanie alebo povolenie určitej webovej stránky môže byť presnejšie ako blokovanie kategórie stránok. Pri zmene nastavení a pri pridaní kategórie do zoznamu buďte opatrný.

Kopírovať výnimky od používateľa

Pomocou roletového menu vyberte používateľa, od ktorého chcete skopírovať výnimku.

Kopírovať kategórie z účtu

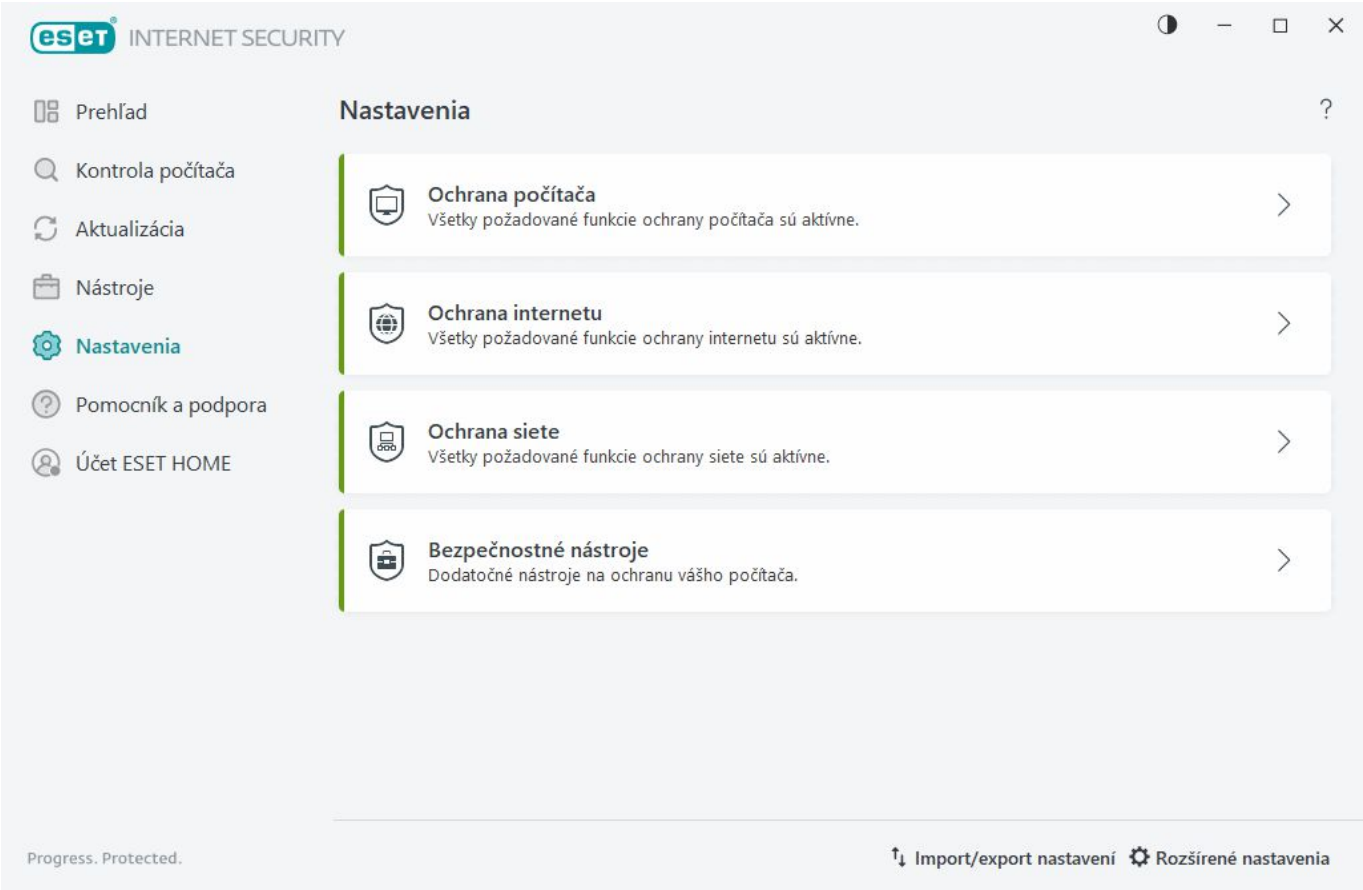
Umožňuje kopírovať zoznam povolených alebo blokovaných kategórií od existujúceho používateľského účtu.

Ochrana siete

Otvorte hlavné okno programu > **Nastavenia** > **Ochrana siete** a nakonfigurujte základné nastavenia ochrany siete alebo odstráňte problémy so sieťovou komunikáciou.

Ak chcete pozastaviť alebo vypnúť jednotlivé moduly ochrany, kliknite na prepínacie tlačidlo .

Vypnutie modulov ochrany môže znížiť úroveň zabezpečenia vášho počítača.



Kliknutím na ikonu ozubeného kolesa vedľa modulu ochrany prejdete do rozšírených nastavení daného modulu.

Firewall – filtruje všetku sieťovú komunikáciu na základe konfigurácie programu ESET Internet Security.

Konfigurovať – otvoria sa rozšírené nastavenia firewallu, kde môžete určiť, akým spôsobom bude firewall spravovať sieťovú komunikáciu.

Pozastaviť firewall (povoliť všetku komunikáciu) – pri použití tejto možnosti je filtrovanie komunikácie firewallom úplne vypnuté a všetky prichádzajúce aj odchádzajúce spojenia sú povolené. Ak chcete opätovne zapnúť firewall, keď je filtrovanie sieťovej komunikácie v tomto režime, kliknite na možnosť **Zapnúť firewall**.

Zablokovať všetku komunikáciu – každá prichádzajúca a odchádzajúca komunikácia bude firewallom bez upozornenia používateľa zablokovaná. Použiť tento spôsob blokovania je vhodné napríklad pri podozrení na možné kritické bezpečnostné riziká, kedy je nutné odpojiť systém od siete. Ak je v rámci filtrovania sieťovej komunikácie nastavená možnosť **Zablokovať všetku komunikáciu**, kliknutím na možnosť **Zastaviť blokovanie všetkej komunikácie** prepnete firewall do štandardného režimu.

Automatický režim – (ak je povolený iný režim filtrovania) – kliknutím na túto možnosť sa režim filtrovania zmení na automatický (s pravidlami nastavenými používateľom).

Interaktívny režim (ak je povolený iný režim filtrovania) – kliknutím na túto možnosť sa režim filtrovania zmení na interaktívny.

Ochrana pred sieťovými útokmi (IDS) – analyzuje obsah sieťovej komunikácie a chráni pred sieťovými útokmi. Zablokovaná bude každá škodlivá sieťová komunikácia. ESET Internet Security vás upozorní, ak sa pripojíte k nezabezpečenej bezdrôtovej sieti alebo k sieti so slabou ochranou.

Ochrana pred botnetmi – rýchlo a presne odhaľuje malvér v systéme.

Sieťové pripojenia – zobrazuje siete, na ktoré sú pripojené sieťové adaptéry, s podrobnými informáciami.

Vyriešiť blokovanú komunikáciu – pomáha pri riešení problémov so sieťovým spojením, ktoré môžu byť zapríčinené ESET Firewallom. Viac informácií nájdete v kapitole Sprievodca riešením problémov.

Vyriešiť dočasne blokované IP adresy – zobraziť zoznam IP adries, ktoré boli detegované ako zdroj útokov a pridané na blacklist s cieľom na istý čas zablokovať spojenie.

Zobraziť protokoly – otvorí sa súbor protokolu ochrany siete.

Sieťové pripojenia

Zobrazuje siete, na ktoré sú pripojené sieťové adaptéry. Ak chcete zobraziť sieťové pripojenia, otvorte hlavné okno programu > **Nastavenia** > **Ochrana siete** > **Sieťové pripojenia**.

Dvojitým kliknutím na pripojenie uvedené v zozname zobrazíte jeho podrobnosti a podrobnosti o sieťovom adaptéri.

Prejdite kurzorom myši nad konkrétne sieťové pripojenie, kliknite na ikonu menu ⋮ v stĺpci **Dôveryhodné** a vyberte jednu z nasledujúcich možností:

- **Upraviť** – otvorí sa okno Nastavenie ochrany siete, v ktorom môžete priradiť profil Ochrany siete konkrétnej sieti
- **Zabudnúť** – obnoví sa predvolená konfigurácia sieťového pripojenia

- **Skontrolovať sieť pomocou Strážcu siete** – otvorí sa Strážca siete, ktorý vykoná kontrolu siete
- **Označiť ako „Moja sieť“** – sieti sa priradí označenie „Moja sieť“; toto označenie sa bude zobrazovať vedľa siete naprieč celým produktom ESET Internet Security v záujme lepšej identifikácie a dohľadu nad zabezpečením
- **Zrušiť označenie „Moja sieť“** – odstráni sa označenie Moja sieť; táto možnosť je k dispozícii iba v prípade, že sieti už bolo predtým priradené dané označenie

Podrobnosti sieťového pripojenia

Dvojitým kliknutím na pripojenie v zozname Sieťové pripojenia zobrazíte jeho podrobnosti spolu s podrobnosťami o sieťovom adaptéri. Podrobnosti o sieťovom pripojení a adaptéri vám pomôžu identifikovať sieť, ktorú sa snažíte nakonfigurovať v rámci Ochrany sieťového pripojenia.

Podrobnosti sieťového pripojenia:

- Stav sieťového pripojenia
- Dátum a čas prvej detekcie siete
- Posledná aktivita siete
- Celkový čas strávený pripojením k tejto sieti
- Profil sieťového pripojenia
- Profil sieťového pripojenia definovaný v systéme Windows
- Konfigurácia ochrany siete (či je sieť dôveryhodná)

Podrobnosti o sieťovom adaptéri:

- Typ pripojenia (drôtové, virtuálne atď.)
- Názov sieťového adaptéra
- Popis adaptéra
- IP a MAC adresa
- IPv4 a IPv6 adresa siete s podsieťou
- Prípona DNS
- IP adresa DNS servera
- IP adresa DHCP servera
- IP a MAC adresa predvolenej brány
- MAC adresa adaptéra

Riešenie problémov s prístupom na sieť

Sprievodca riešením problémov vám umožňuje riešiť problémy s pripojením, ktoré môžu vznikať pri používaní Firewallu. **Riešenie problémov s prístupom na sieť** nájdete v hlavnom okne programu v časti **Nastavenia** > **Ochrana siete** > **Vyriešiť blokovanú komunikáciu**.

Vyberte, či chcete zobraziť komunikáciu blokovanú pre **lokálne aplikácie** alebo blokovanú komunikáciu zo **vzdialených zariadení**.

Z roletového menu vyberte časové obdobie, v ktorom bola sieťová komunikácia zablokovaná. Zoznam nedávno blokovanej komunikácie vám poskytuje prehľad o typoch aplikácií alebo zariadení, reputácii a celkovom počte aplikácií a zariadení blokovaných v danom časovom období. Pre viac informácií o konkrétnej blokovanej komunikácii kliknite na **Podrobnosti**. Ďalším krokom je odblokovanie aplikácie alebo zariadenia, pri ktorom dochádza k problému.

Po kliknutí na tlačidlo **Odblokovať** bude povolená všetka doteraz blokovaná komunikácia. Ak problémy s aplikáciou nezmiznú alebo vaše zariadenie nefunguje podľa očakávania, skúste **vytvoriť iné pravidlo** a všetka predtým blokovaná komunikácia bude povolená. Ak problém napriek tomu pretrváva, reštartujte počítač.

Kliknutím na položku **Otvoriť pravidlá firewallu** zobrazíte pravidlá vytvorené pomocou sprievodcu. Pravidlá vytvorené sprievodcom nájdete aj v okne Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Firewall** > **Pravidlá** > **Upraviť**.

Ak sa pravidlo nedá vytvoriť, zobrazí sa chybové hlásenie. Kliknutím na tlačidlo **Skúsiť znova** a zopakovaním postupu odblokujte komunikáciu alebo vytvorte ďalšie pravidlo zo zoznamu blokovanej komunikácie.

Dočasný blacklist IP adries

Ak chcete zobraziť IP adresy, ktoré boli zachytené ako zdroj útokov a pridané na blacklist s cieľom zablokovať na určitý čas spojenie, otvorte hlavné okno programu > **Nastavenia** > **Ochrana siete** > **Vyriešiť dočasne blokované IP adresy**. Dočasne blokované IP adresy sú blokované jednu hodinu.

Stĺpce

IP adresa – zobrazuje IP adresu, ktorá bola zablokovaná.

Dôvod blokovania – typ útoku, ktorému bolo zabránené (napríklad útok skenovaním portov TCP).

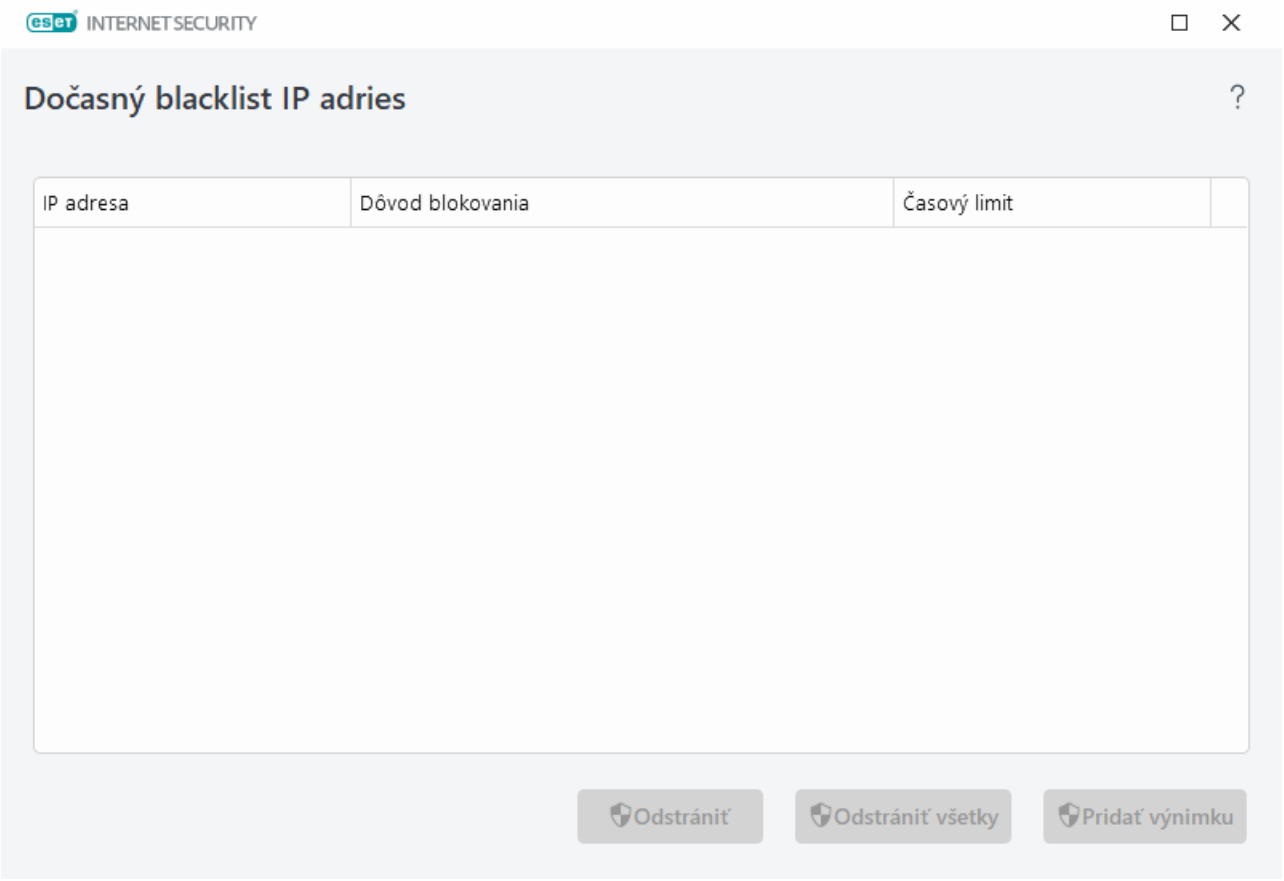
Časový limit – zobrazuje čas a dátum, kedy bude adresa vyradená zo zoznamu.

Ovládacie prvky

Odstrániť – kliknite pre odobratie adresy z blacklistu skôr, ako uplynie časový limit.

Odobrať všetky – kliknite pre odobratie všetkých adries z blacklistu.

Pridať výnimku – kliknite pre pridanie výnimky do IDS filtrovania firewallu.



Protokoly ochrany siete

Ochrana siete programu ESET Internet Security ukladá všetky dôležité udalosti do protokolu. Ak chcete zobraziť protokol, otvorte hlavné okno programu > **Nastavenia** > **Ochrana siete** > **Zobraziť protokoly**.

Súbory protokolov môžete použiť na riešenie problémov a odhalenie prienikov do systému. Protokoly ochrany siete obsahujú nasledujúce údaje:

- dátum a čas udalosti,
- názov udalosti,
- zdroj,
- cieľová sieťová adresa,
- protokol sieťovej komunikácie,
- aplikované pravidlo alebo názov červa, ak bol identifikovaný,
- cesta a názov aplikácie,
- hash,
- používateľ,
- podpisovateľ aplikácie (vydavateľ),

- názov balíka,
- názov udalosti.

Podrobná analýza týchto údajov môže pomôcť odhaliť pokusy o narušenie bezpečnosti systému. Potenciálne bezpečnostné riziká môžete včas odhaliť aj sledovaním rozličných faktorov. Napríklad príliš časté spojenia z neznámych lokalít, hromadné pokusy o nadviazanie spojenia, komunikujúce neznáme aplikácie či nezvyčajné čísla portov môžu pomôcť v odhalení útoku a minimalizovaní jeho následkov.

> **Zneužitie bezpečnostnej zraniteľnosti**
> Správa o zneužití bezpečnostnej chyby je zaznamenaná do protokolu aj v tom prípade, že je už konkrétna zraniteľnosť opravená. Pokus o zneužitie je totiž zachytený a zablokovaný na úrovni siete ešte predtým, ako by mohlo dôjsť k samotnému zneužitiu bezpečnostnej zraniteľnosti.

Riešenie problémov s Firewallom

Ak máte pri používaní programu ESET Internet Security problémy so sieťovým spojením, existuje niekoľko spôsobov, ako zistiť, či tieto problémy zapríčiňuje Firewall. Firewall vám navyše umožňuje vytvoriť nové pravidlá alebo výnimky na vyriešenie problémov s pripojením.

Viac informácií o riešení problémov s Firewallom nájdete v nasledujúcich kapitolách:

- Riešenie problémov s prístupom na sieť
- Vytváranie protokolov a pravidiel alebo výnimiek z protokolu
- Vytvorenie výnimky z oznámenia firewallu
- Vytváranie rozšírených protokolov ochrany siete
- Riešenie problémov s kontrolou sieťovej komunikácie

Vytváranie protokolov a pravidiel alebo výnimiek z protokolu

Štandardne ESET Firewall nevytvára protokol o blokovaní sieťových spojení. Ak chcete zistiť, ktoré spojenia sú blokované Ochranou siete, otvorte Rozšírené nastavenia > **Nástroje** > **Diagnostika** > **Vytváranie rozšírených protokolov** a povoľte možnosť **Zapnúť rozšírené protokoly ochrany siete**. Ak vo vytvorenom protokole nájdete spojenia, ktoré blokovať nechcete, môžete pre tieto spojenia vytvoriť pravidlo alebo IDS pravidlo kliknutím pravým tlačidlom na záznam a vybratím možnosti **Neblokovať podobné udalosti v budúcnosti**. Je potrebné mať na pamäti, že blokované spojenia môžu obsahovať tisíce údajov a môže byť veľmi ťažké nájsť špecifické spojenie, ktoré spôsobuje problém. Po vyriešení problému môžete vytváranie protokolov znova vypnúť.

Viac informácií o protokoloch nájdete v kapitole Protokoly.

> Vo vytvorenom protokole je možné vidieť poradie, v akom Ochrana siete zablokovala konkrétne sieťové spojenia. Vytváranie pravidiel priamo z protokolu vám navyše umožňuje prispôsobiť pravidlá presne podľa vašich potrieb.

Vytvorenie pravidla z protokolu

Nová verzia ESET Internet Security vám umožňuje vytvoriť pravidlo priamo z protokolu. V hlavnom okne programu kliknite na **Nástroje** > **Protokoly**. Z roletového menu vyberte položku **Ochrana siete**, pravým tlačidlom myši kliknite na protokol a z kontextového menu vyberte možnosť **Neblokovať podobné udalosti v budúcnosti**. Zobrazí sa oznámenie o vytvorení nového pravidla.

Aby bolo možné vytvárať pravidlá z protokolu, program ESET Internet Security musí byť nastavený nasledovne:

1. V sekcii **Rozšírené nastavenia** > Nástroje > **Protokoly** nastavte minimálnu úroveň podrobnosti protokolov na možnosť **Diagnostický**.

2. Zapnite možnosť **Upozorniť na prichádzajúce útoky využívajúce bezpečnostné zraniteľnosti** cez Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Ochrana pred sieťovými útokmi (IDS)** > **Pokročilé možnosti** > **Detekcia útokov**.

Vytvorenie výnimky z oznámenia firewallu

Keď ESET Firewall deteguje škodlivú aktivitu na sieti, zobrazí oznámenie s popisom udalosti. Toto oznámenie obsahuje odkaz, ktorý vám poskytne podrobnejšie informácie o udalosti a umožní vytvoriť pravidlo.

Ak sieťová aplikácia alebo zariadenie nespĺňa sieťové štandardy, môže dôjsť k opakovanému oznámeniu tej istej udalosti. Takýmto oznámeniam sa dá predísť vytvorením výnimky priamo z oznámenia na obrazovke.

Vytváranie rozšírených protokolov ochrany siete

Táto funkcionalita je navrhnutá na komplexné vytváranie protokolov pre technickú podporu spoločnosti ESET. Vzhľadom na značnú veľkosť protokolov a spomalenie počítača pri ich vytváraní použite túto možnosť, len ak vás na to vyzval pracovník technickej podpory spoločnosti ESET.

1. Prejdite do časti Rozšírené nastavenia > **Nástroje** > **Diagnostika** > **Vytváranie rozšírených protokolov** a povoľte možnosť **Zapnúť rozšírené protokoly ochrany siete**.

2. Potom sa pokúste znova vyvolať váš problém.

3. Vypnite rozšírené protokoly ochrany siete.

4. Vytvorené rozšírené PCAP protokoly ochrany siete nájdete v rovnakom adresári, do ktorého sa generujú aj diagnostické výpisy pamäte: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Riešenie problémov s kontrolou sieťovej komunikácie

Ak ste zaznamenali problémy s webovým prehliadačom alebo e□mailovým klientom, v prvom rade treba zistiť, či je problém spôsobený kontrolou sieťovej komunikácie. Na overenie tejto možnosti skúste dočasne vypnúť kontrolu sieťovej komunikácie cez Rozšírené nastavenia > **Detekčné jadro** > **Kontrola sieťovej komunikácie** (nezabudnite ju znova zapnúť, keď skončíte, v opačnom prípade ostanú webové prehliadače a e□mailové klienty nechránené). Ak sa po vypnutí filtrovania protokolov problém viac neprejavuje, je možné, že ide o jeden

z nasledujúcich problémov:

Problémy aktualizácie alebo zabezpečenia komunikácie

Ak aplikácia hlási problém s aktualizáciou alebo so zabezpečením komunikačných kanálov:

- Ak je zapnutý protokol SSL/TLS, skúste ho dočasne vypnúť. Ak to pomôže, môžete SSL/TLS naďalej používať a umožniť aktualizáciu vytvorením výnimky pre problémovú komunikáciu:
  Vypnite SSL/TLS. Spustite znova aktualizáciu. Malo by sa zobraziť dialógové okno o šifrovanej komunikácii. Uistite sa, že aplikácia v okne je tá, ktorej problém riešite, a že certifikát pochádza z aktualizačného servera. Označte možnosť Zapamätať si akciu pre tento certifikát a vyberte Ignorovať. Ak sa nezobrazia ďalšie relevantné dialógové okná, môžete prepnúť režim filtrovania späť na automatický a problém by mal byť vyriešený.

- Ak aplikácia nie je webový prehliadač alebo e□mailový klient, môžete ju kompletne vylúčiť z Ochrany prístupu na web (ak vylúčite e□mailový klient alebo webový prehliadač, vystavíte tým váš počítač riziku infiltrácie). Aplikácie, ktorých komunikácia bola predtým filtrovaná kontrolou protokolov, by už mali byť v zozname dostupnom pri pridávaní výnimky, takže manuálne pridanie by nemalo byť potrebné.

Problém s prístupom na sieťové zariadenie

Ak nemáte prístup k funkcionalitám zariadení na vašej sieti (napríklad otváranie webovej stránky webkamery alebo prehranie videa na domácom multimediálnom prehrávači), skúste pridať IPv4 a IPv6 adresy do zoznamu vylúčených adries.

Problémy s konkrétnou webovou stránkou

Na vylúčenie konkrétnych webových stránok z ochrany prístupu na web použite manažment URL adries. Napríklad, ak nemáte prístup k stránke https://www.gmail.com/intl/en/mail/help/about.html, skúste pridať *gmail.com* do zoznamu webových stránok vylúčených z kontroly.

Chyba „Niektoré podporované aplikácie na import koreňového certifikátu sú stále spustené“

Ak povolíte protokol SSL/TLS, ESET Internet Security sa postará, aby nainštalované aplikácie dôverovali spôsobu filtrovania protokolu SSL naimportovaním certifikátu do ich úložného priestoru certifikátov. Niektoré aplikácie môžu na import certifikátu vyžadovať reštartovanie, napríklad Firefox a Opera. Uistite sa preto, že nie sú spustené (najlepšie cez Správcu úloh, kde skontrolujte, či sa v zozname na karte Procesy nenachádza firefox.exe alebo opera.exe), a potom to skúste znova.

Chyba o nedôveryhodnom vydavateľovi alebo neplatnom podpise certifikátu

Toto oznámenie znamená, že import certifikátu popísaný vyššie zlyhal. V prvom rade sa uistite, že žiadna zo zmienených aplikácií nie je spustená. Potom vypnite protokol SSL/TLS a znovu ho zapnite. Tento postup znova spustí import.

> Informácie o tom, ako spravovať kontrolu sieťovej komunikácie v produkte ESET pre domácnosti (Windows), nájdete v článku Databázy znalostí.

Sieťová hrozba bola zablokovaná

Táto udalosť môže nastať v prípade, ak bezpečnostné riešenie odhalí vo vašom systéme pokus o skenovanie portov alebo ak sa niektorá aplikácia na vašom počítači pokúša neštandardne komunikovať s iným zariadením v sieti či zneužiť bezpečnostnú dieru.

Oznámenie obsahuje informácie o type hrozby a IP adresu príslušného zariadenia. Kliknutím na **Zmeniť akciu pre túto hrozbu** zobrazíte nasledujúce možnosti:

Pokračovať v blokovaní – zablokuje detegovanú hrozbu. Ak už nechcete dostávať oznámenia o tomto type hrozby z konkrétnej vzdialenej adresy, použite prepínač vedľa možnosti **Neupozorňovať** a až potom kliknite na tlačidlo **Pokračovať v blokovaní**. Tým sa vytvorí IDS pravidlo s nasledujúcou konfiguráciou: **Blokovať** – predvolené, **Oznámiť** – nie, **Zapísať do protokolu** – nie.

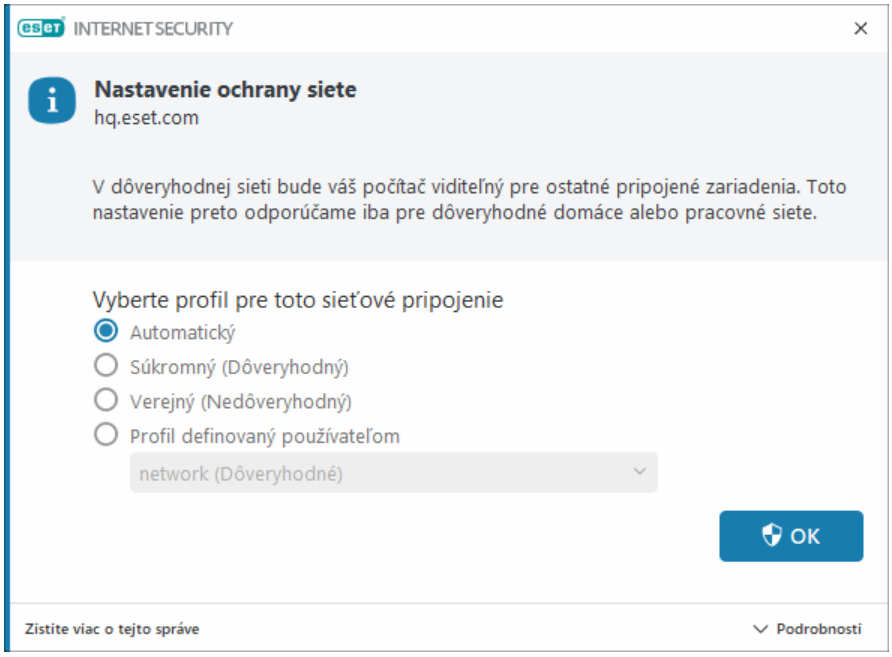
Povoliť – vytvorí sa IDS pravidlo na povolenie detegovanej hrozby. Skôr ako kliknete na **Povoliť**, vyberte jednu z nasledujúcich možností nastavenia pravidla:

- **Upozorniť iba pri zablokovaní tejto hrozby** – konfigurácia pravidla: **Blokovať** – nie, **Oznámiť** – nie, **Zapísať do protokolu** – nie.
- **Upozorniť pri každom výskyte tejto hrozby** – konfigurácia pravidla: **Blokovať** – nie, **Oznámiť** – predvolené, **Zapísať do protokolu** – predvolené.
- **Neupozorňovať** – konfigurácia pravidla: **Blokovať** – nie, **Oznámiť** – nie, **Zapísať do protokolu** – nie.

Informácia zobrazená v okne oznámení sa môže líšiť v závislosti od typu zachytenej hrozby.
Viac informácií o hrozbách a ďalších súvisiacich pojmoch nájdete v kapitole Typy vzdialených útokov alebo Typy detekcií.
Postup riešenia **duplicitných IP adries v sieti** nájdete v tomto článku Databázy znalostí spoločnosti ESET.

Zistená nová sieť

Keď sa objaví nová sieť, ESET Internet Security pre ňu v predvolenom nastavení použije konfiguráciu zo systému Windows. Ak chcete, aby sa pri nájdení novej siete zobrazilo dialógové okno, nastavte priraďovanie profilu Ochrany siete na možnosť **Spýtať sa**. K nastaveniu ochrany siete budete vyzvaný vždy, keď sa váš počítač pripojí k novej sieti.



Môžete si vybrať z nasledujúcich profilov sieťového pripojenia:

Automatický – ESET Internet Security vyberie profil automaticky na základe aktivátorov nakonfigurovaných pre každý profil.

Súkromný – pre dôveryhodné siete (domácu alebo pracovnú sieť). Váš počítač a zdieľané súbory uložené na počítači budú viditeľné zo siete a systémové prostriedky budú dostupné pre ostatných používateľov v sieti (prístup k zdieľaným súborom a tlačiarňam, ako aj prichádzajúca RPC komunikácia budú povolené a služba zdieľania pracovnej plochy bude takisto dostupná). Toto nastavenie odporúčame použiť pri bezpečných lokálnych sieťach. Tento profil sa automaticky priradí k sieťovému pripojeniu, ak je v systéme Windows použitá konfigurácia domény alebo súkromnej siete.

Verejný – pre nedôveryhodné siete (verejné siete). Súbory a priečinky uložené vo vašom systéme nebudú zdieľané ani viditeľné pre ostatných používateľov v sieti a zdieľanie systémových prostriedkov bude deaktivované. Toto nastavenie odporúčame použiť pri pripojení k bezdrôtovým sieťam. Tento profil sa automaticky priradí ku každému sieťovému pripojeniu, ktoré nie je v systéme Windows nakonfigurované ako doména alebo súkromná sieť.

Profil definovaný používateľom – z roletového menu si môžete vybrať jeden z profilov, ktoré ste vytvorili. Táto možnosť je k dispozícii len vtedy, ak ste vytvorili aspoň jeden vlastný profil.

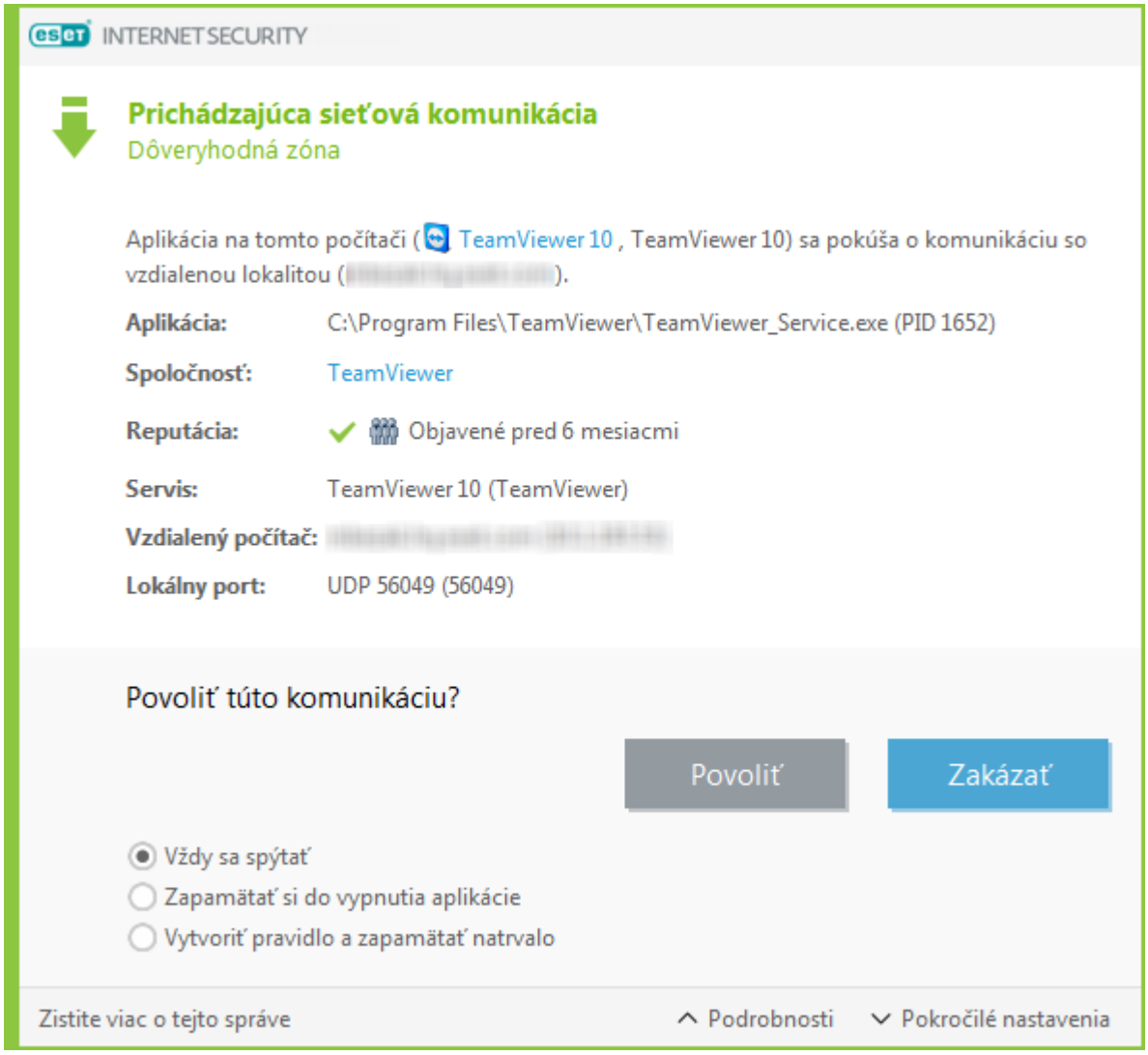
⚠ Nesprávnym nastavením siete vystavujete počítač potenciálnemu bezpečnostnému riziku.

Nadväzovanie spojenia – detekcia

Firewall deteguje každé nové sieťové spojenie. Nastavenie režimu filtrovania určuje, aké akcie sa vykonajú pri novom sieťovom spojení. Pri **Automatickom režime** alebo pri **Režime politík** firewall pracuje na základe prednastavených pravidiel a bez interakcie používateľa.

V prípade **Interaktívneho režimu** sa pri každom novom sieťovom spojení zobrazí dialógové okno, ktoré informuje o zachytení nového sieťového spojenia a poskytuje podrobné informácie o danom spojení. Pripojenie môžete **povoliť** alebo **odmietnuť** (zablokovať). V prípade, že opakovane povoľujete rovnaké sieťové spojenie, odporúčame vám vytvoriť pre toto spojenie nové pravidlo. V zobrazenom dialógovom okne označte možnosť

Vytvoriť pravidlo a zapamätať natrvalo, čím sa zvolená akcia uloží do nastavení firewallu ako nové pravidlo. V prípade, že firewall v budúcnosti zachytí rovnaké spojenie, bez potreby interakcie používateľa naň aplikuje už existujúce pravidlo.



Pri detekcii neznámych spojení a vytváraní príslušných pravidiel treba postupovať obozretne a povoľovať len tie spojenia, ktoré sú bezpečné. Firewall pri povolení všetkých spojení stráca svoje opodstatnenie. Dôležité parametre sieťových spojení:

Aplikácia – umiestnenie spustiteľného súboru a ID procesu. Neodporúčame povoliť spojenia neznámym aplikáciám a procesom.

Podpísal – názov vydavateľa aplikácie. Kliknutím na text zobrazíte bezpečnostný certifikát spoločnosti.

Reputácia – úroveň rizika daného spojenia. Spojeniam sa priraďujú tieto úrovne rizika: V poriadku (zelená), Neznáme (oranžová) alebo Riziko (červená), a to pomocou série heuristických pravidiel, ktoré skúmajú vlastnosti každého pripojenia, počet používateľov a čas prvého výskytu. Tieto informácie sú zhromažďované pomocou technológie ESET LiveGrid®.

Služba – názov služby, ak je aplikácia službou v systéme Windows.

Vzdialený počítač – adresa vzdialeného zariadenia. Povoľujte len spojenia na dôveryhodné a známe adresy.

Vzdialený port – komunikačný port. Komunikácia na známych portoch (napr. web – port číslo 80.443) je zvyčajne

bezpečná.

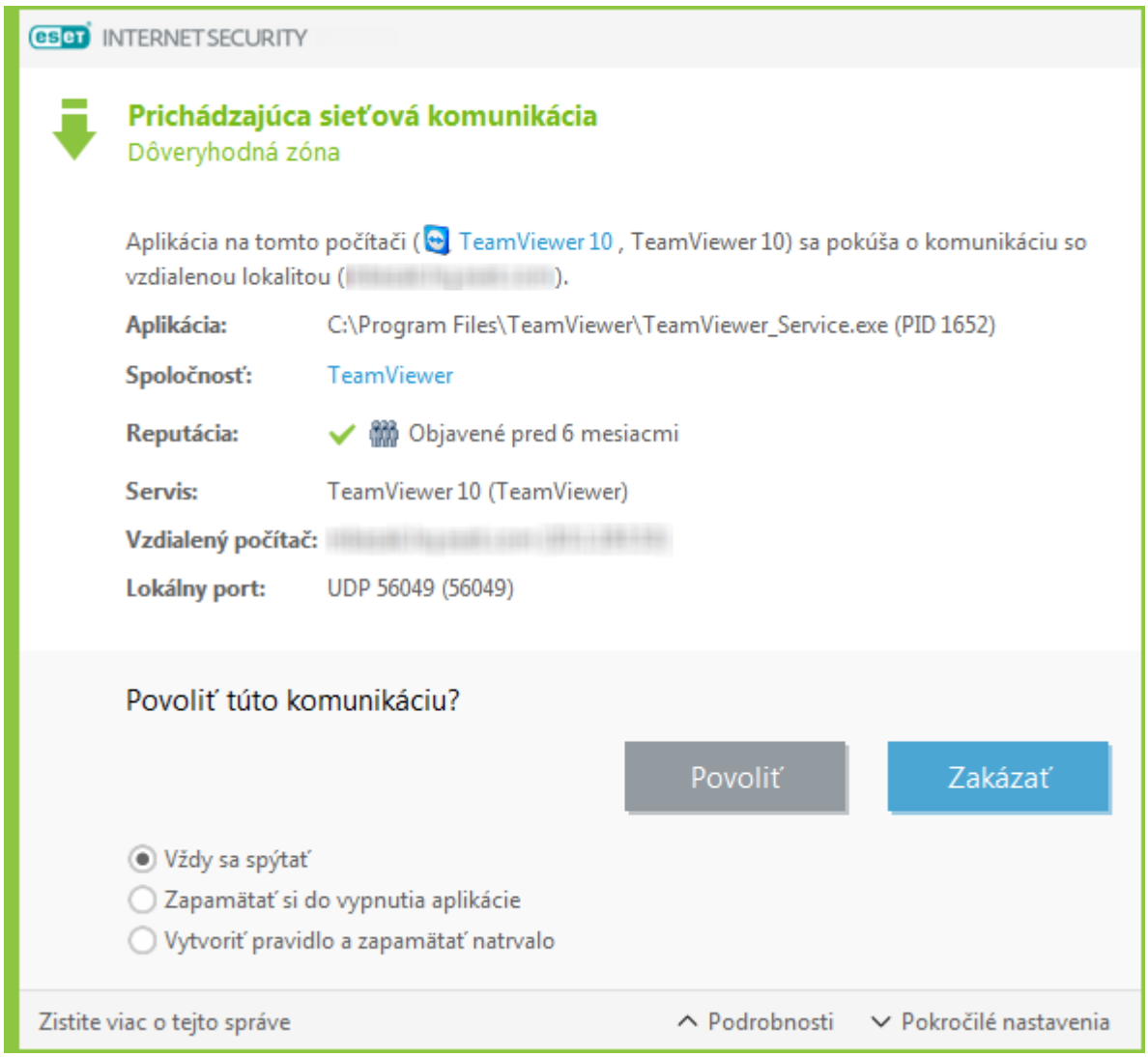
Infiltrácie na svoje šírenie vo veľkej miere využívajú internet a skryté spojenia, pomocou ktorých sú schopné infikovať vzdialené systémy. Správnym nastavením pravidiel firewallu je možné ochrániť systém pred rôznymi útokmi škodlivého kódu.

Zmena aplikácie

Firewall detegoval zmenu aplikácie, ktorá už v minulosti nadväzovala komunikáciu z vášho počítača. Aplikácia mohla byť zmenená napríklad aktualizáciou na novšiu verziu. K zmene aplikácie však mohlo dôjsť aj v dôsledku nebezpečnej infiltrácie. Ak si nie ste vedomý legitímneho dôvodu zmeny aplikácie, odporúčame komunikáciu aplikácie zakázať a následne spustiť kontrolu počítača s použitím najnovšej verzie detekčného jadra.

Prichádzajúca dôveryhodná komunikácia

Príklad prichádzajúcej komunikácie z dôveryhodnej zóny:
S aplikáciou, ktorá beží na lokálnom počítači, sa snaží komunikovať vzdialený počítač z dôveryhodnej zóny.



Aplikácia – aplikácia, s ktorou sa vzdialená strana snaží nadviazať komunikáciu.

Cesta k aplikácii – umiestnenie aplikácie.

Aplikácia z Microsoft Store – názov aplikácie v obchode Microsoft Store.

Podpísal – názov vydavateľa aplikácie. Kliknutím na text zobrazíte bezpečnostný certifikát spoločnosti.

Reputácia – reputácia aplikácie zistená pomocou technológie ESET LiveGrid®.

Služba – názov služby, ktorá je spustená na počítači.

Vzdialený počítač – vzdialený počítač sa snaží komunikovať s aplikáciou, ktorá je spustená na lokálnom počítači.

Vzdialený port – port používaný na komunikáciu.

Spýtať sa – ak je akcia v pravidle nastavená na **Spýtať sa**, po spustení pravidla sa zobrazí dialógové okno s výberom možností.

Zapamätať si do ukončenia aplikácie – ESET Internet Security si zvolenú akciu zapamätá do ďalšieho reštartu.

Vytvoriť pravidlo a zapamätať natrvalo – ak túto možnosť vyberiete predtým, ako povolíte alebo zablokujete komunikáciu, ESET Internet Security si zapamätá danú akciu a použije ju, keď bude chcieť vzdialený počítač opäť nadviazať komunikáciu s počítačom.

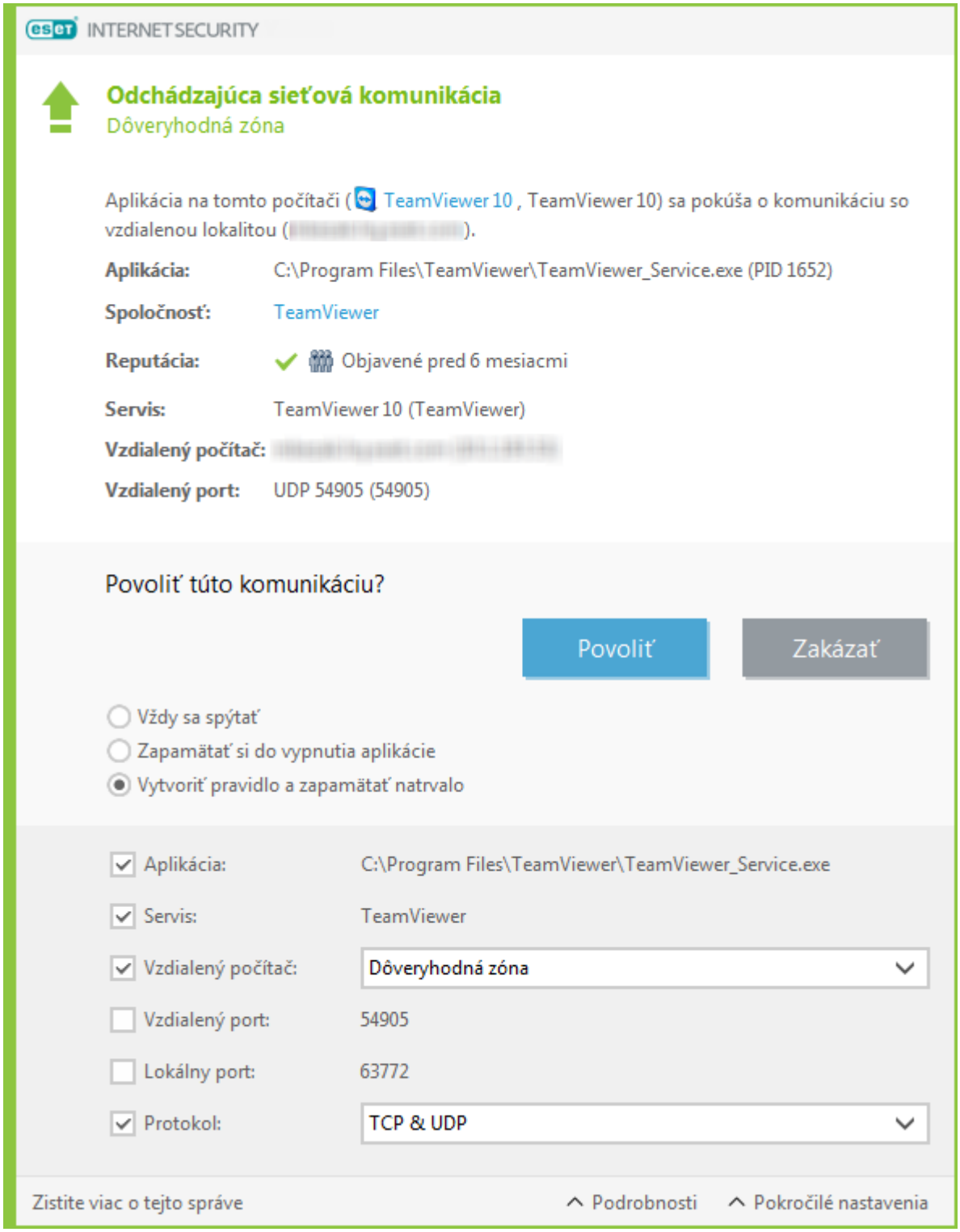
Povoliť – povolenie prichádzajúcej komunikácie.

Zakázať – zakázanie prichádzajúcej komunikácie.

Upraviť pravidlo – prispôsobenie vlastností pravidla pomocou editora pravidiel firewallu.

Odchádzajúca dôveryhodná komunikácia

Príklad odchádzajúcej komunikácie z dôveryhodnej zóny:
Aplikácia, ktorá je spustená na lokálnom počítači, sa snaží pripojiť na iný počítač v lokálnej sieti alebo sieti, ktorá bola pridaná ako dôveryhodná.



Aplikácia – aplikácia, s ktorou sa vzdialená strana snaží nadviazať komunikáciu.

Cesta k aplikácii – umiestnenie aplikácie.

Aplikácia z Microsoft Store – názov aplikácie v obchode Microsoft Store.

Podpísal – názov vydavateľa aplikácie. Kliknutím na text zobrazíte bezpečnostný certifikát spoločnosti.

Reputácia – reputácia aplikácie zistená pomocou technológie ESET LiveGrid®.

Služba – názov služby, ktorá je spustená na počítači.

Vzdialený počítač – vzdialený počítač sa snaží komunikovať s aplikáciou, ktorá je spustená na lokálnom počítači.

Vzdialený port – port používaný na komunikáciu.

Spýtať sa – ak je akcia v pravidle nastavená na **Spýtať sa**, po spustení pravidla sa zobrazí dialógové okno s výberom možností.

Zapamätať si do ukončenia aplikácie – ESET Internet Security si zvolenú akciu zapamätá do ďalšieho reštartu.

Vytvoriť pravidlo a zapamätať natrvalo – ak túto možnosť vyberiete predtým, ako povolíte alebo zablokujete komunikáciu, ESET Internet Security si zapamätá danú akciu a použije ju, keď bude chcieť vzdialený počítač opäť nadviazať komunikáciu s počítačom.

Povoliť – povolenie prichádzajúcej komunikácie.

Zakázať – zakázanie prichádzajúcej komunikácie.

Upraviť pravidlo – prispôsobenie vlastností pravidla pomocou editora pravidiel firewallu.

Prichádzajúca komunikácia

Príklad prichádzajúcej internetovej komunikácie:
S aplikáciou, ktorá je spustená na lokálnom počítači, sa snaží komunikovať vzdialený počítač.

Aplikácia – aplikácia, s ktorou sa vzdialená strana snaží nadviazať komunikáciu.

Cesta k aplikácii – umiestnenie aplikácie.

Aplikácia z Microsoft Store – názov aplikácie v obchode Microsoft Store.

Podpísal – názov vydavateľa aplikácie. Kliknutím na text zobrazíte bezpečnostný certifikát spoločnosti.

Reputácia – reputácia aplikácie zistená pomocou technológie ESET LiveGrid®.

Služba – názov služby, ktorá je spustená na počítači.

Vzdialený počítač – vzdialený počítač sa snaží komunikovať s aplikáciou, ktorá je spustená na lokálnom počítači.

Vzdialený port – port používaný na komunikáciu.

Spýtať sa – ak je akcia v pravidle nastavená na **Spýtať sa**, po spustení pravidla sa zobrazí dialógové okno s výberom možností.

Zapamätať si do ukončenia aplikácie – ESET Internet Security si zvolenú akciu zapamätá do ďalšieho reštartu.

Vytvoriť pravidlo a zapamätať natrvalo – ak túto možnosť vyberiete predtým, ako povolíte alebo zablokujete komunikáciu, ESET Internet Security si zapamätá danú akciu a použije ju, keď bude chcieť vzdialený počítač opäť nadviazať komunikáciu s počítačom.

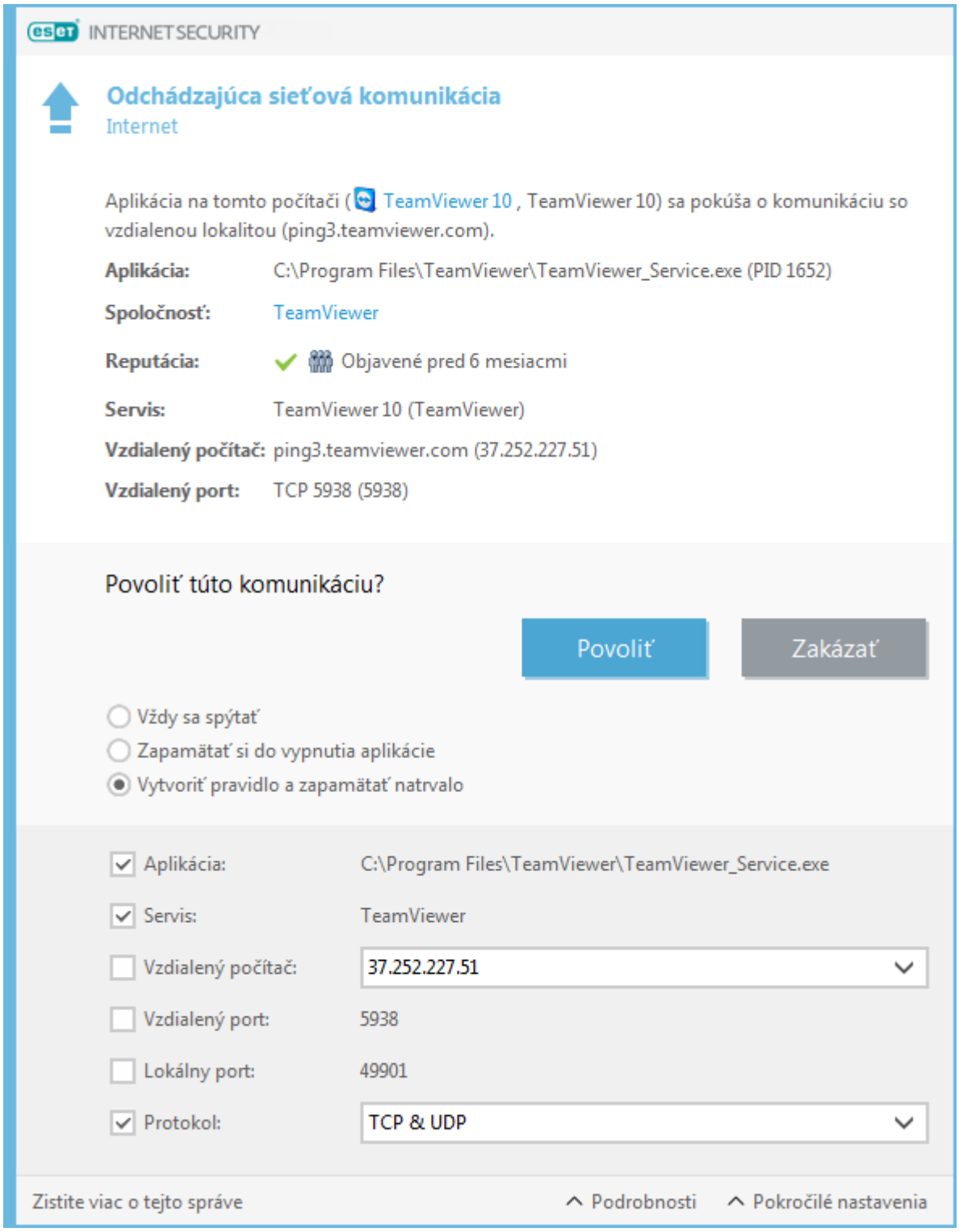
Povoliť – povolenie prichádzajúcej komunikácie.

Zakázať – zakázanie prichádzajúcej komunikácie.

Upraviť pravidlo – prispôsobenie vlastností pravidla pomocou editora pravidiel firewallu.

Odchádzajúca komunikácia

Príklad odchádzajúcej internetovej komunikácie:
Aplikácia, ktorá je spustená na lokálnom počítači, sa snaží pripojiť na internet.



Aplikácia – aplikácia, s ktorou sa vzdialená strana snaží nadviazať komunikáciu.

Cesta k aplikácii – umiestnenie aplikácie.

Aplikácia z Microsoft Store – názov aplikácie v obchode Microsoft Store.

Podpísal – názov vydavateľa aplikácie. Kliknutím na text zobrazíte bezpečnostný certifikát spoločnosti.

Reputácia – reputácia aplikácie zistená pomocou technológie ESET LiveGrid®.

Služba – názov služby, ktorá je spustená na počítači.

Vzdialený počítač – vzdialený počítač sa snaží komunikovať s aplikáciou, ktorá je spustená na lokálnom počítači.

Vzdialený port – port používaný na komunikáciu.

Spýtať sa – ak je akcia v pravidle nastavená na **Spýtať sa**, po spustení pravidla sa zobrazí dialógové okno s výberom možností.

Zapamätať si do ukončenia aplikácie – ESET Internet Security si zvolenú akciu zapamätá do ďalšieho reštartu.

Vytvoriť pravidlo a zapamätať natrvalo – ak túto možnosť vyberiete predtým, ako povolíte alebo zablokujete komunikáciu, ESET Internet Security si zapamätá danú akciu a použije ju, keď bude chcieť vzdialený počítač opäť nadviazať komunikáciu s počítačom.

Povoliť – povolenie prichádzajúcej komunikácie.

Zakázať – zakázanie prichádzajúcej komunikácie.

Upraviť pravidlo – prispôsobenie vlastností pravidla pomocou editora pravidiel firewallu.

Nastavenie zobrazovania spojení

Pravým tlačidlom myši kliknite na pripojenie a zobrazia sa vám doplňujúce možnosti:

Prekladať IP adresy na mená – pokiaľ je to možné, sieťové adresy sú uvádzané v DNS forme a nie v číselnej podobe IP adresy.

Zobrazovať iba pripojenia TCP – v zozname sa zobrazia iba tie spojenia, ktoré patria pod protokol TCP.

Zobrazovať počúvajúce pripojenia – zobrazia sa iba spojenia, pri ktorých neprebieha komunikácia, systém však má otvorený port a čaká na spojenie.

Zobrazovať pripojenia v rámci počítača – zobrazia sa iba pripojenia, ktoré majú ako vzdialenú stranu použitý lokálny systém. Týka sa to tzv. localhost pripojení.

Rýchlosť obnovovania – frekvencia, s akou sa budú obnovovať informácie o aktívnych pripojeniach.

Obnoviť teraz – obnovia sa informácie v okne **Sieťové pripojenia**.

Bezpečnostné nástroje

Otvorte hlavné okno programu > **Nastavenia** > **Bezpečnostné nástroje** a nastavte nasledujúce moduly:

Ochrana pri platbách a prehliadaní – pridáva do prehliadača dodatočnú vrstvu ochrany, ktorej cieľom je chrániť

vaše platobné údaje pri online transakciách pred zneužitím. Zapnutím možnosti **Zabezpečiť všetky prehliadače** v rámci rozšírených nastavení ochrany pri platbách a prehliadaní povolíte spúšťanie všetkých podporovaných prehliadačov v zabezpečenom režime.

Ochrana súkromia v prehliadači – zaisťuje vám súkromie a bezpečnosť pri online aktivitách bez zanechania digitálnej stopy.

Anti-Theft – zapnutím modulu Anti-Theft zabezpečíte svoj počítač pre prípad straty alebo krádeže.

Ochrana pri platbách a prehliadaní

Ochrana pri platbách a prehliadaní predstavuje dodatočnú vrstvu ochrany, ktorej cieľom je chrániť vaše online transakcie a finančné údaje pred zneužitím.

Predvolene sa všetky podporované webové prehliadače spúšťajú v zabezpečenom režime. Vďaka tomu môžete prehliadať webové stránky, používať internetové bankovníctvo, nakupovať na internete a vykonávať online transakcie v jednom zabezpečenom prehliadači, ktorý sa spustí automaticky.

Na zaistenie správneho fungovania Ochrany pri platbách a prehliadaní musí byť zapnutý reputačný systém ESET LiveGrid® (predvolene zapnutý).

Ak chcete nakonfigurovať správanie zabezpečeného prehliadača, prejdite do rozšírených nastavení ochrany pri platbách a prehliadaní. Ak vypnete nastavenie **Zabezpečiť všetky prehliadače**, môžete sa k zabezpečenému prehliadaču dostať v hlavnom okne programu po kliknutí na **Prehľad** > **Ochrana pri platbách a prehliadaní** alebo cez ikonu na ploche **Ochrana pri platbách a prehliadaní**. Prehliadač, ktorý máte v systéme Windows nastavený ako predvolený, sa spustí v zabezpečenom režime.

Na chránené prehliadanie internetu je nevyhnutné použiť šifrovaný komunikačný protokol HTTPS. Ochrana pri platbách a prehliadaní je podporovaná nasledujúcimi prehliadačmi:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Na zariadeniach s procesorom ARM sú podporované len prehliadače Firefox a Microsoft Edge.

Pre podrobnejšie informácie o funkcii Ochrana pri platbách a prehliadaní si prečítajte nasledujúce články Databázy znalostí spoločnosti ESET, ktoré sú dostupné v angličtine a niekoľkých ďalších jazykoch:

- Ako používať funkciu Ochrana pri platbách a prehliadaní v produktoch ESET?
- Ako pozastavím alebo vypnem ochranu pri platbách a prehliadaní v produkte ESET pre domácnosti so systémom Windows?
- Ochrana pri platbách a prehliadaní – bežné problémy
- Slovník pojmov ESET | Ochrana pri platbách a prehliadaní

Oznámenie v prehliadači

Zabezpečený prehliadač vás informuje o aktuálnom stave prostredníctvom oznámení v prehliadači a farby orámovania okolo okna prehliadača.

Oznámenia v prehliadači sa zobrazujú na karte na pravej strane okna prehliadača.

Kliknutím na ikonu ESET rozbalíte aktuálne oznámenie v prehliadači. Ak chcete oznámenie minimalizovať, kliknite na text oznámenia. Oznámenie a zelené orámovanie prehliadača môžete zrušiť kliknutím na ikonu .

Zrušiť možno len informatívne oznámenie a zelené orámovanie prehliadača.

Oznámenia v prehliadači

Typ oznámenia	Stav
Informatívne oznámenie a zelené orámovanie prehliadača	Zabezpečená je maximálna ochrana a oznámenie v prehliadači je predvolene minimalizované. Rozbaľte oznámenie v prehliadači a kliknutím na položku **Nastavenia** otvorte nastavenie bezpečnostných nástrojov.
Upozornenie a oranžové orámovanie prehliadača	Zabezpečený prehliadač si vyžaduje vašu pozornosť z dôvodu problému, ktorý však nie je kritický. Pre viac informácií o probléme a jeho riešení postupujte podľa pokynov uvedených priamo v oznámení v prehliadači.
Bezpečnostné upozornenia a červené orámovanie prehliadača	Prehliadač nie je chránený funkciou Ochrana pri platbách a prehliadaní od spoločnosti ESET. Reštartujte prehliadač, aby sa ochrana aktivovala. Ak chcete vyriešiť konflikty so súbormi načítanými v prehliadači, otvorte Protokoly > **Ochrana pri platbách a prehliadaní** a zabezpečte, aby sa protokoly pri ďalšom spustení prehliadača nenačítali. Ak sa vám nedarí problém vyriešiť, kontaktujte technickú podporu spoločnosti ESET podľa inštrukcií v našom článku Databázy znalostí.

Ochrana súkromia v prehliadači

Funkcia ochrany súkromia v prehliadači sa aktivuje prostredníctvom rozšírenia, ktoré je dostupné v podporovaných prehliadačoch (Google Chrome, Mozilla Firefox a Microsoft Edge).

Ak chcete rozšírenie nainštalovať a aktivovať, postupujte nasledovne:

1. Uistite sa, že používate najnovšiu verziu ESET Internet Security a po aktualizácii reštartujte počítač.
2. Otvorte webový prehliadač.
3. Rozšírenie sa nainštaluje do prehliadača.
4. Povoľte rozšírenie a v prehliadači sa zobrazí stránka s podrobnosťami o rozšírení.

Hlavné menu pre rozšírenie Ochrana súkromia v prehliadači je rozdelené na nasledujúce sekcie:

Prehľad

Bezpečné vyhľadávanie

Túto funkciu zapnete kliknutím na ikonu prepínača  vedľa možnosti **Kontrolovať výsledky vyhľadávania**. Následne uvidíte, na ktoré výsledky vyhľadávania je možné bezpečne kliknúť. Bezpečné vyhľadávanie vyhodnocuje adresy odkazov uvedené vo výsledkoch vyhľadávania. Označenie výsledku za bezpečný však nemusí nevyhnutne znamenať, že webová stránka neobsahuje malvér. Kontrolu prítomnosti malvéru na stránke zabezpečí naše detekčné jadro.

Čistenie prehliadača

Odstráňte údaje prehliadania alebo nastavte pravidelné čistenie. Ak chcete na vybraných webových stránkach zostať prihlásený a prijímať súbory cookie aj po vyčistení prehliadača, **pridajte ich do zoznamu**.

- **Jednorazové čistenie** – z roletového menu vyberte želaný časový rozsah a typ údajov, ktoré chcete vymazať. Môžete sa rozhodnúť vymazať všetky údaje, súkromné údaje alebo vlastný výber.

- **Pravidelné čistenie** – túto funkciu zapnete kliknutím na ikonu prepínača  vedľa možnosti **Pravidelné čistenie**. Z roletového menu vyberte želaný časový rozsah a typ údajov, ktoré chcete pravidelne mazať. Môžete sa rozhodnúť vymazať všetky údaje, súkromné údaje alebo vlastný výber.

Možnosť **Vlastné údaje** obsahuje tieto kategórie:

- História prehliadania
- História sťahovania
- Súbory cookie a údaje webových stránok
- Obrázky a súbory vo vyrovnávacej pamäti
- Heslá a prihlasovacie údaje
- Údaje automatického vypĺňania formulárov

Kontrola nastavení webových stránok

Vďaka jednoduchému prístupu k povoleniam webových stránok a ich správe nastavte, ktoré informácie môžu webové stránky používať.

- **Oznámenia** – skontrolujte, na ktorých webových stránkach chcete **povoliť/blokovať** oznámenia, prípadne či chcete, aby sa vás rozšírenie prehliadača zakaždým spýtalo na váš výber (možnosť **Vždy sa opýtať**).

Rozšírené nastavenia

Čistenie prehliadača

Pokročilé nastavenia súborov cookie

Zoznam webových stránok, na ktorých chcete prijímať súbory cookie a zostať prihlásený aj po vyčistení prehliadača. URL adresu vybranej stránky stačí zadať do textového poľa a kliknúť na tlačidlo **Pridať**. Kedykoľvek ju

môžete zo zoznamu odstrániť kliknutím na ikonu znamienka mínus vedľa konkrétnej webovej stránky.

V spodnej časti stránky sa nachádza zoznam navrhovaných domén na základe kariet, ktoré máte aktuálne otvorené v prehliadači. Ak v ňom nevidíte konkrétnu webovú stránku, kliknite na možnosť **obnovenia zoznamu** a následne stránku pridajte kliknutím na ikonu znamienka plus .

Kontrola nastavení webových stránok

Vďaka jednoduchému prístupu k povoleniam webových stránok a ich správe nastavte, ktoré informácie môžu webové stránky používať.

- **Oznámenia** – skontrolujte, na ktorých webových stránkach chcete **povoliť/blokovať** oznámenia, prípadne či chcete, aby sa vás rozšírenie prehliadača zakaždým spýtalo na váš výber (možnosť **Vždy sa opýtať**).

Vzhľad

Prispôsobte si farebný motív grafického rozhrania podľa svojich preferencií. Môžete si vybrať medzi **Svetlým** a **Tmavým** motívom.

Anti-Theft

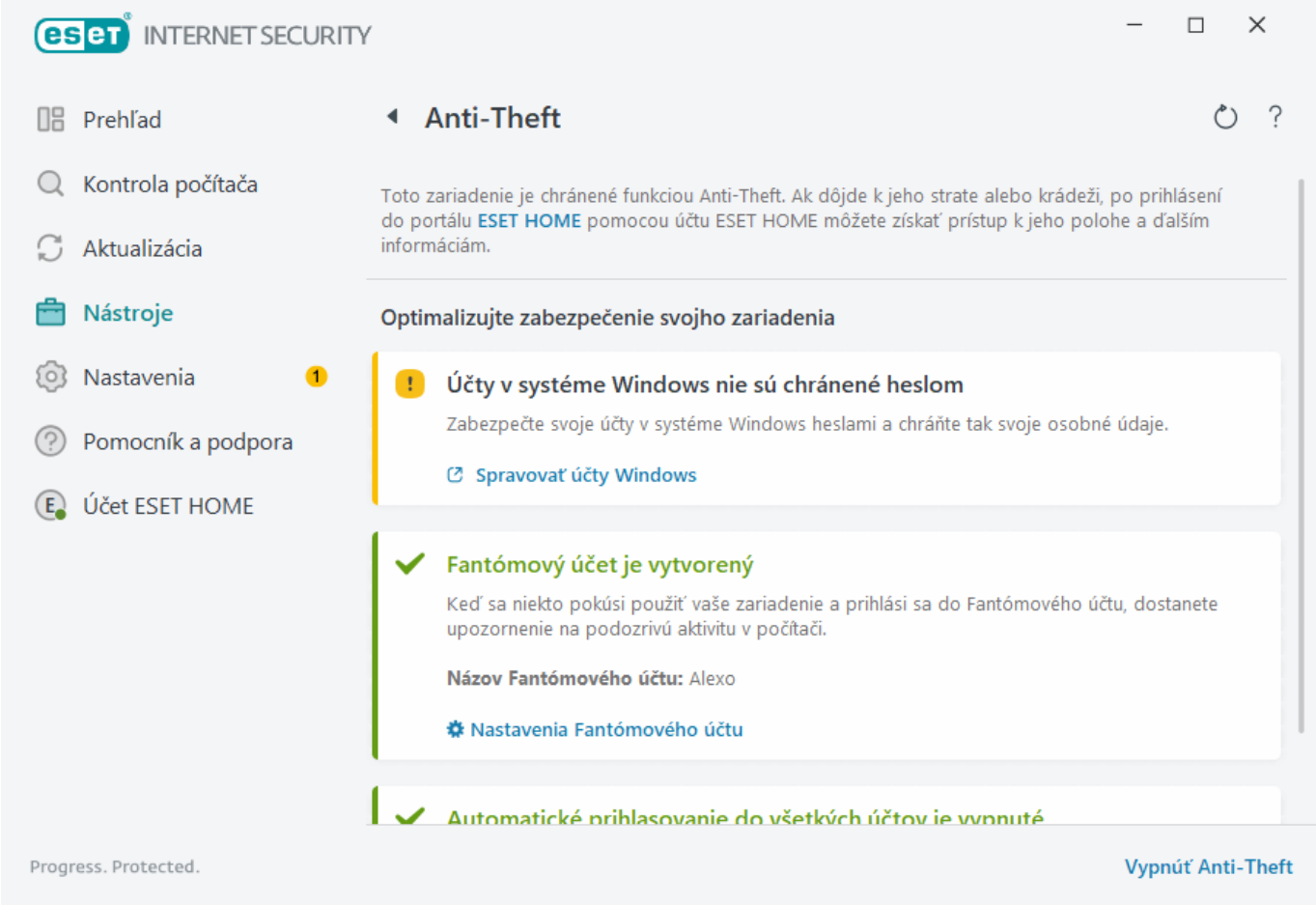
Pri každodennom cestovaní z domova do práce alebo iných verejných miest sú osobné zariadenia neustále vystavené riziku odcudzenia alebo straty. Anti-Theft je funkcia, ktorá výrazne zvyšuje zabezpečenie zariadenia v prípade jeho straty alebo krádeže. Anti-Theft vám umožní cez účet ESET HOME sledovať, či zariadenie niekto používa, a takisto vám ukáže polohu alebo IP adresy, z ktorých sa vaše zariadenie pripája na internet. Pomôže vám tak vystopovať zariadenie a ochrániť súkromné dáta.

Pomocou moderných technológií ako IP geolokácia, snímanie fotografií z webkamery, ochrana používateľských účtov a monitorovanie zariadenia dokáže Anti-Theft výrazne pomôcť pri hľadaní strateného zariadenia alebo pri odhalení krádeže. Cez ESET HOME môžete vidieť, aká aktivita prebieha na vašom počítači alebo zariadení.

Ak sa chcete dozvedieť viac informácií o funkcii Anti-Theft v rámci ESET HOME, pozrite si Online pomocníka pre ESET HOME.

Anti-Theft nemusí správne fungovať na počítačoch v doménach, a to z dôvodu obmedzení v správe používateľských účtov.

Po zapnutí funkcie Anti-Theft môžete optimalizovať zabezpečenie svojho zariadenia v hlavnom okne programu v sekcii **Nastavenia** > **Bezpečnostné nástroje** > **Anti-Theft**.



Možnosti optimalizácie

Nie je vytvorený žiadny Fantómový účet

Vytvorenie Fantómového účtu vám zvýši šancu, že nájdete svoje stratené alebo odcudzené zariadenie. Keď označíte zariadenie ako stratené, Anti-Theft zablokuje prístup k vašim aktívnym používateľským účtom v systéme, aby vaše súkromné dáta zostali v bezpečí. Každý, kto sa pokúsi zariadenie používať, bude mať prístup iba k Fantómovému účtu. Fantómový účet je formou hosťovského účtu s obmedzenými oprávneniami. Bude sa používať ako predvolený systémový účet, až kým zariadenie neoznačíte ako nájdené. Týmto sa neoprávneným osobám zabráni v prístupe k ostatným používateľským účtom alebo k údajom používateľa.

Ak sa niekto prihlási do Fantómového účtu, keď je váš počítač v normálnom stave, dostanete e-mailom upozornenie s informáciami o podozrivej aktivite na počítači. Po prijatí e-mailového oznámenia máte možnosť označiť zariadenie ako stratené.

Ak chcete vytvoriť Fantómový účet, kliknite na možnosť **Vytvoriť Fantómový účet**, do textového poľa zadajte **Názov Fantómového účtu** a kliknite na tlačidlo **Vytvoriť**.

Ak už máte Fantómový účet vytvorený, kliknutím na možnosť **Nastavenia Fantómového účtu** ho môžete premenovať alebo odstrániť.

Zabezpečenie účtov Windows heslom

Váš používateľský účet Windows nie je chránený heslom. Toto upozornenie týkajúce sa optimalizácie sa zobrazí v prípade, že najmenej jeden používateľský účet nie je chránený heslom. Tento problém môžete vyriešiť vytvorením hesla pre všetkých používateľov počítača (okrem **Fantómového účtu**).

Ak chcete vytvoriť heslo pre používateľský účet, kliknite na možnosť **Spravovať účty Windows** alebo postupujte podľa pokynov uvedených nižšie:

1. Stlačte klávesovú kombináciu CTRL+Alt+Delete.
2. Kliknite na možnosť **Zmeniť heslo**.
3. Textové pole **Staré heslo** ponechajte prázdne.
4. Do textových polí **Nové heslo** a **Potvrdiť heslo** vpíšte svoje nové heslo a stlačte **Enter**.

Automatické prihlasovanie do účtov Windows

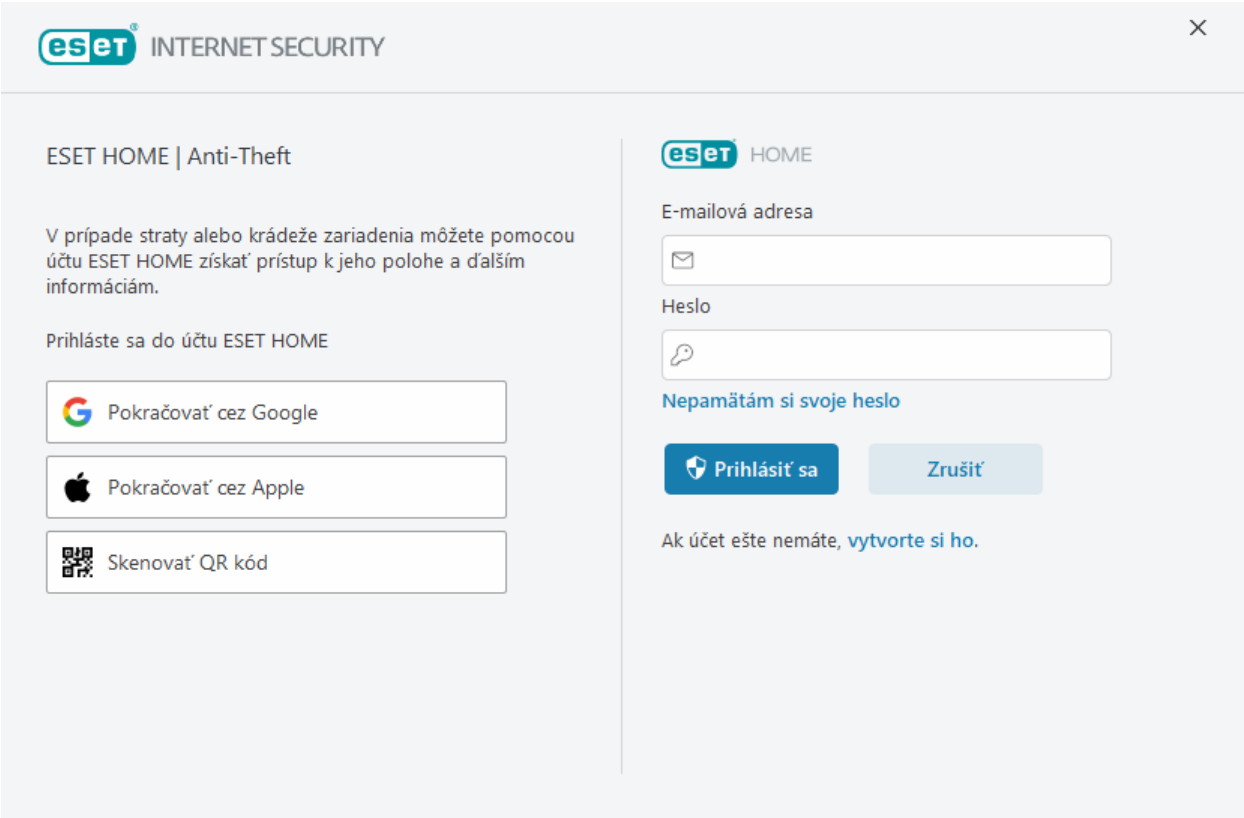
Váš používateľský účet má povolené automatické prihlasovanie, preto nie je chránený pred neoprávneným prístupom. Toto upozornenie týkajúce sa optimalizácie sa zobrazí v prípade, že najmenej jeden používateľský účet má povolené automatické prihlasovanie. Pre vyriešenie tohto problému kliknite na **Vypnúť automatické prihlasovanie**.

Automatické prihlasovanie do Fantómového účtu

Pre **Fantómový účet** na vašom zariadení je povolené automatické prihlasovanie. Keď je zariadenie v normálnom stave, neodporúčame povoliť automatické prihlasovanie, pretože to môže spôsobiť problémy s prihlásením do vášho skutočného používateľského účtu a zasielanie falošných upozornení o strate/krádeži vášho počítača. Pre vyriešenie tohto problému kliknite na **Vypnúť automatické prihlasovanie**.

Prihláste sa do svojho účtu ESET HOME.

Ak chcete zapnúť/vypnúť Anti-Theft alebo získať prístup k polohe zariadenia a informáciám v ESET HOME, prihláste sa do svojho účtu ESET HOME.



Existuje niekoľko spôsobov, ako sa môžete prihlásiť do svojho účtu ESET HOME:

- **Použite e□mailovú adresu a heslo priradené k účtu ESET HOME** – zadajte **E□mailovú adresu** a **Heslo**, ktoré ste použili na vytvorenie účtu ESET HOME, a kliknite na **Prihlásiť sa**.

- **Použite účet Google/AppleID** – kliknite na **Pokračovať cez Google** alebo **Pokračovať cez Apple** a prihláste sa do príslušného účtu. Po úspešnom prihlásení vás presmerujeme na potvrdzujúcu webovú stránku ESET HOME. Ak chcete pokračovať, vráťte sa do okna programu ESET. Viac informácií o prihlásení pomocou účtu Google/AppleID nájdete v Online pomocníkovi pre ESET HOME.

- **Skenovať QR kód** – kliknutím na **Skenovať QR kód** sa zobrazí QR kód. Otvorte mobilnú aplikáciu ESET HOME a naskenujte QR kód, prípadne môžete použiť fotoaparát na zariadení. Viac informácií nájdete v Online pomocníkovi pre ESET HOME.

Bežné chyby pri prihlasovaní

Ak účet ESET HOME ešte nemáte, kliknite na možnosť **Vytvoriť účet** a zaregistrujte sa. Inštrukcie nájdete na stránke Online pomocníka ESET HOME.
V prípade, že si neviete spomenúť na svoje heslo, kliknite na možnosť **Nepamätám si svoje heslo** a riaďte sa pokynmi na obrazovke, prípadne prejdite na stránku Online pomocníka ESET HOME.

Anti-Theft nie je podporovaný na operačnom systéme Microsoft Windows Home Server.

Zadajte názov zariadenia

Pole **Názov zariadenia** predstavuje názov vášho počítača (zariadenia), pod ktorým sa bude zobrazovať v rámci všetkých služieb ESET HOME. Predvolenou hodnotou v tomto poli je názov vášho počítača zo systému. Zadajte názov zariadenia alebo použite predvolený názov a kliknite na **Pokračovať**.

Anti-Theft bol zapnutý/vypnutý

Keď zapnete/vypnete Anti-Theft, zobrazí sa toto okno s potvrdzovacou správou:

- Zapnuté – toto zariadenie je teraz chránené funkciou Anti-Theft. Jeho zabezpečenie môžete spravovať vzdialene na portáli ESET HOME prostredníctvom svojho účtu.

- Vypnuté – Anti-Theft je na tomto zariadení vypnutý a z portálu ESET HOME sa vymažú všetky údaje týkajúce sa funkcie <%ESET_ANTTHEFT%> na tomto zariadení.

Nepodarilo sa pridať nové zariadenie

Pri zapínaní funkcie Anti-Theft došlo k chybe.

Najčastejšie ide o niektorú z nasledujúcich príčin:

- Chyba pri prihlásení sa do účtu ESET HOME

- Nenašlo sa žiadne pripojenie na internet (resp. internet nie je momentálne funkčný)

Ak sa vám nedarí vyriešiť tento problém, kontaktujte technickú podporu spoločnosti ESET.

Import a export nastavení

V rámci sekcie **Nastavenia** môžete importovať alebo exportovať nastavenia programu ESET Internet Security z/do súboru .xml.

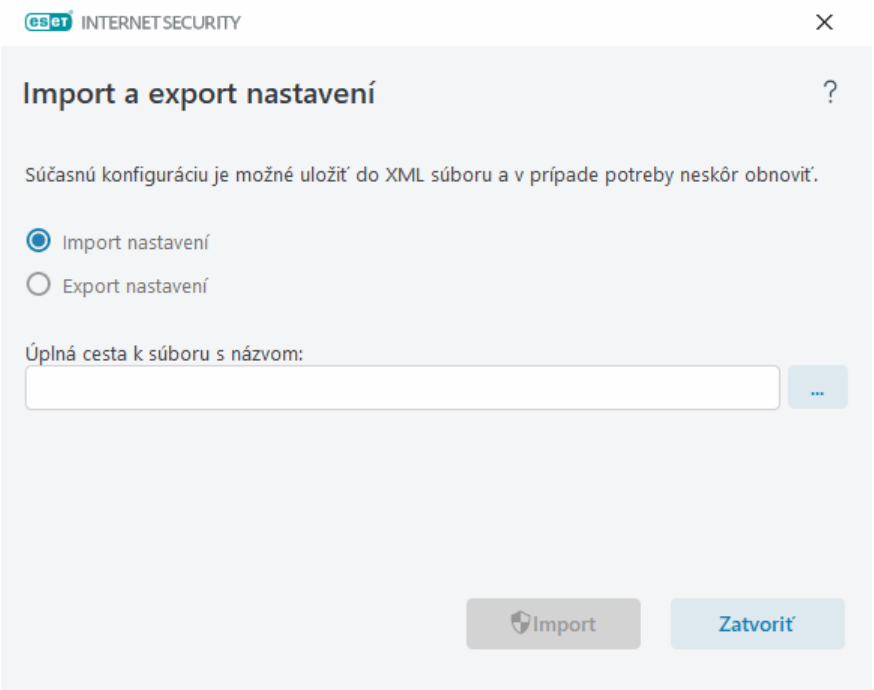
> **Ilustrované inštrukcie**
> Pozrite si náš článok Databázy znalostí s ilustrovanými inštrukciami o tom, ako importovať alebo exportovať nastavenia bezpečnostného produktu ESET pomocou konfiguračného súboru .xml.

Importovanie a exportovanie konfiguračných súborov je potrebné napríklad pri zálohovaní aktuálnych nastavení produktu ESET Internet Security, ku ktorým sa chce používateľ neskôr vrátiť. Export nastavení určite oceníte aj vtedy, keď chcete na viacerých počítačoch použiť jednotné nastavenia. V takom prípade stačí do nainštalovaného programu importovať súbor .xml s nastaveniami.

Ak chcete importovať nastavenia, v hlavnom okne programu kliknite na **Nastavenia** > **Import/export nastavení** a vyberte možnosť **Import nastavení**. Zadajte názov konfiguračného súboru alebo kliknutím na **...** vyhľadajte súbor, ktorý chcete importovať.

Ak chcete nastavenia exportovať, v hlavnom okne programu kliknite na **Nastavenia** > **Import/export nastavení**. Vyberte možnosť **Export nastavení** a zadajte úplnú cestu k súboru s názvom. Kliknutím na **...** zvoľte miesto na disku, kam chcete súbor s nastaveniami uložiť.

> Pri exporte nastavení sa môže objaviť chybové hlásenie, ak nemáte potrebné práva na zápis do príslušného adresára.



Pomocník a podpora

Kliknutím na položku **Pomocník a podpora** v hlavnom okne programu zobrazíte informácie o podpore a nástroje na riešenie problémov, ktoré vám pomôžu vyriešiť potenciálne problémy.

Predplatné

- Riešenie problémov s predplatným – po kliknutí na tento odkaz sa otvorí kapitola pomocníka, ktorá sa venuje riešeniu problémov s aktiváciou alebo zmenou predplatného.
- Zmeniť predplatné – kliknutím na túto možnosť otvoríte okno na aktiváciu produktu. Ak máte zariadenie pripojené k účtu ESET HOME, vyberte predplatné zo svojho účtu ESET HOME alebo pridajte nové predplatné.

Nainštalovaný produkt

- Čo je nové – po kliknutí na túto možnosť sa otvorí okno s informáciami o nových a vylepšených funkciách.
- O ESET Internet Security – zobrazuje informácie o vašej kópii programu ESET Internet Security.
- Riešenie problémov s produktom – po kliknutí na tento odkaz sa otvorí kapitola pomocníka, ktorá sa venuje riešeniu najčastejších problémov s produktom.
- **Zmeniť produkt** – kliknutím na túto možnosť si môžete overiť, či je možné v rámci vášho súčasného predplatného zameniť ESET Internet Security za iný produkt.

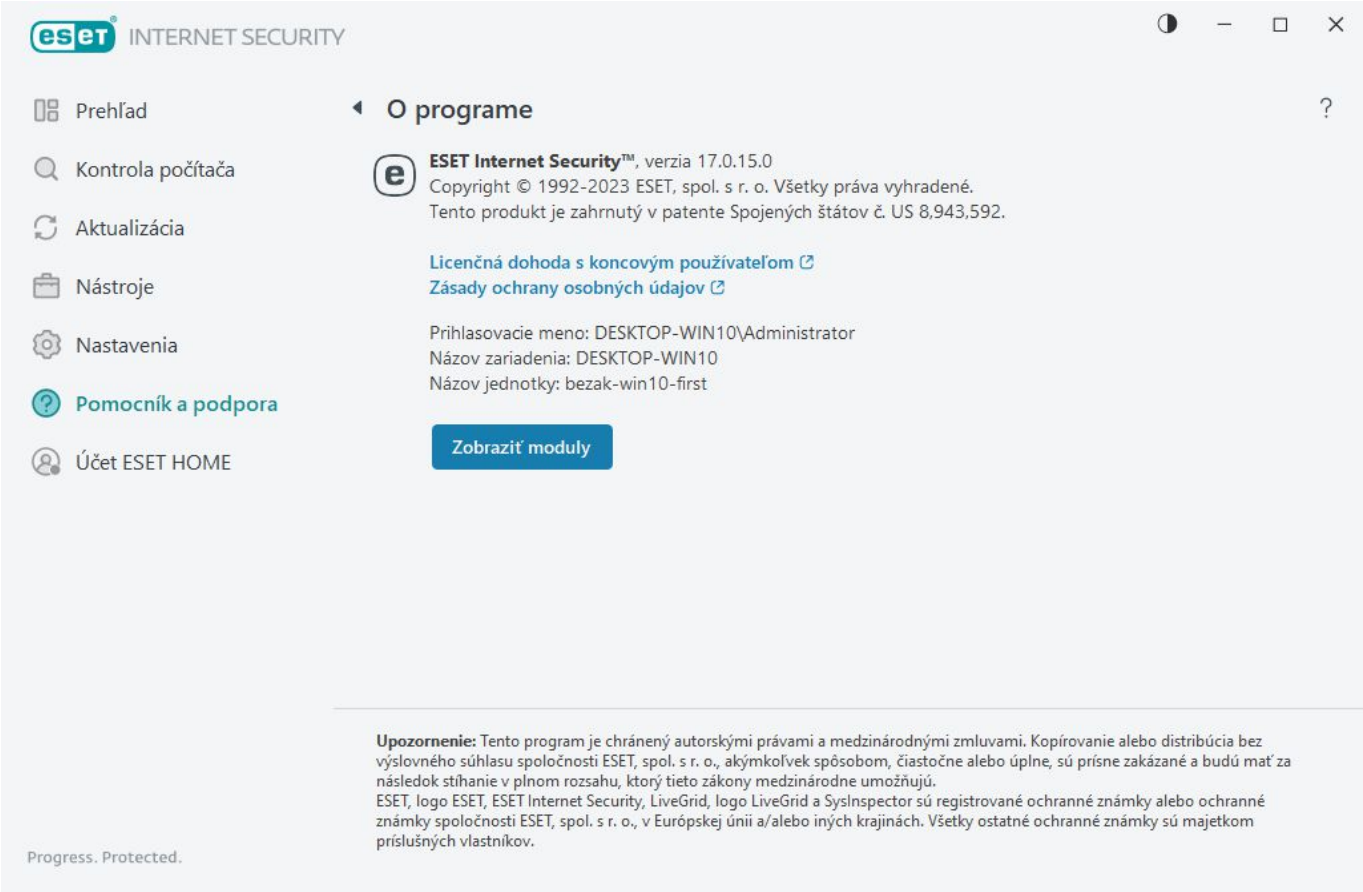
Stránka pomocníka – kliknutím na tento odkaz otvoríte pomocníka pre ESET Internet Security.

Technická podpora

Databáza znalostí – databáza znalostí spoločnosti ESET obsahuje odpovede na najčastejšie kladené otázky, ako aj odporúčané riešenia rozličných problémov. Pravidelná aktualizácia databázy znalostí pracovníkmi spoločnosti ESET z nej robí najefektívnejší nástroj na riešenie rozličných problémov.

O ESET Internet Security

V tomto okne nájdete podrobné informácie o nainštalovanej verzii ESET Internet Security a o vašom počítači.



Kliknutím na možnosť **Zobraziť moduly** zobrazíte zoznam načítaných modulov programu.

- Tieto informácie môžete skopírovať do schránky kliknutím na **Kopírovať**. Toto môže byť užitočné pri riešení problémov alebo pri kontaktovaní technickej podpory.

- Ak v okne Moduly kliknete na možnosť **Detekčné jadro**, otvorí sa stránka ESET Virus Radar, ktorá obsahuje informácie o jednotlivých verziách detekčného jadra spoločnosti ESET.

Novinky ESET

V tomto okne vás program ESET Internet Security pravidelne informuje o novinkách od spoločnosti ESET.

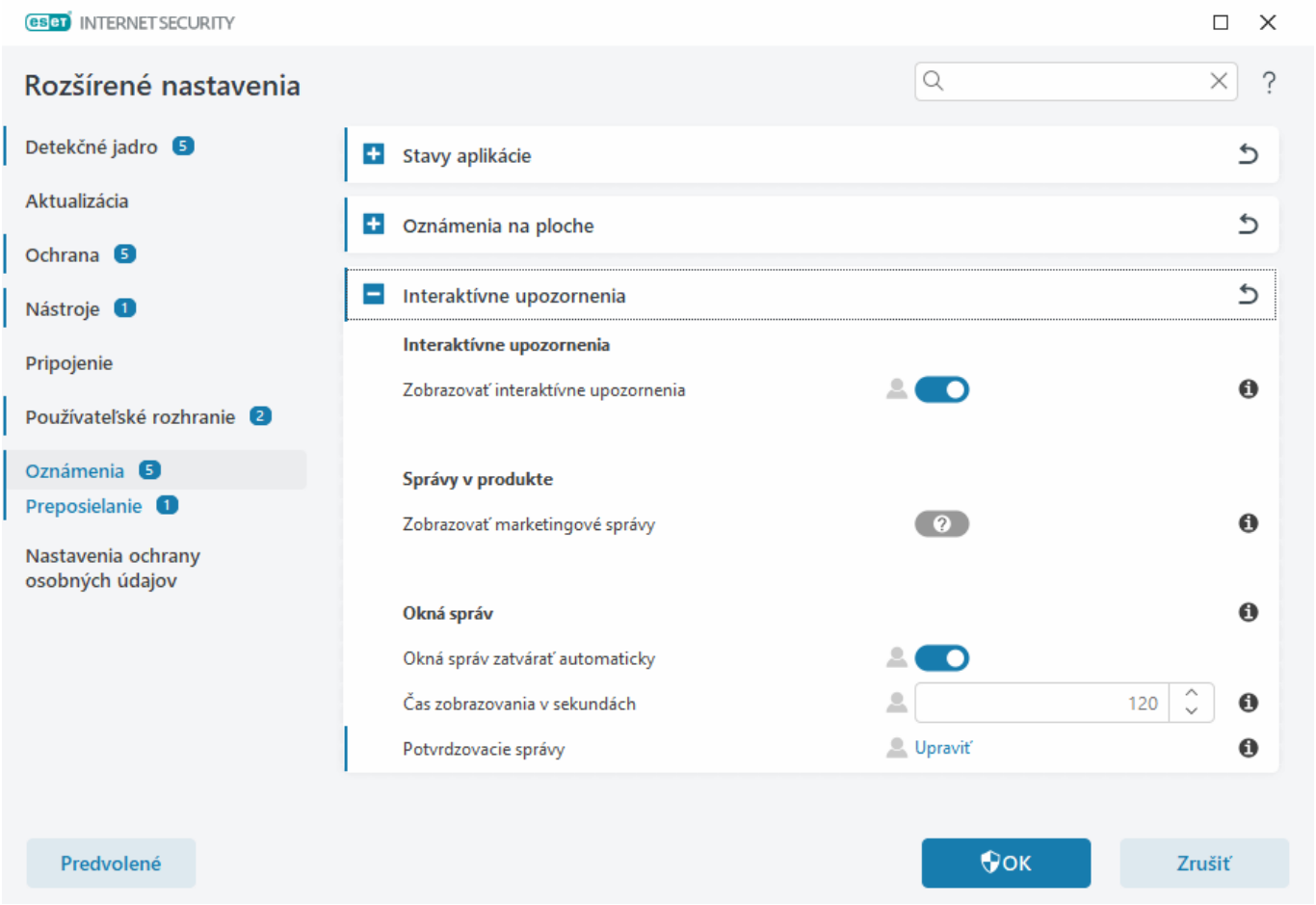
Správy umiestňované priamo v produkte sú prostriedkom, ako môžeme používateľov informovať o novinkách a akciách od spoločnosti ESET. Zasielanie týchto marketingových informácií vyžaduje váš súhlas. Preto vám na základe predvolených nastavení nie sú zasielané žiadne marketingové správy (zobrazuje sa ikona otáznika). Aktivovaním tejto možnosti vyjadríte svoj súhlas s prijímaním marketingových informácií. Ak si takýto druh informácií neprajete dostávať, možnosť **Zobrazovať marketingové správy** deaktivujte.

Ak chcete povoliť alebo zakázať zobrazovanie marketingových správ formou okien s oznámeniami, postupujte podľa pokynov nižšie.

1. Otvorte rozšírené nastavenia.

2. Kliknite na **Oznámenia** > **Interaktívne upozornenia**.

3. Zapnite alebo vypnite možnosť **Zobrazovať marketingové správy**.



Odoslať systémové nastavenia

Na účely poskytnutia čo možno najrýchlejšej a najpresnejšej pomoci bude od vás spoločnosť ESET vyžadovať informácie o konfigurácii vášho produktu ESET Internet Security, podrobné systémové informácie, spustené procesy (protokol nástroja ESET SysInspector) a tiež údaje z databázy Registry. Spoločnosť ESET použije tieto informácie len na účely poskytnutia technickej podpory.

Po vyplnení webového formulára budú vaše systémové nastavenia odoslané spoločnosti ESET. Zvoľte možnosť **Vždy odoslať tieto informácie**, ak chcete, aby si program výber tejto akcie zapamätal. Ak spolu s webovým formulárom nechcete odoslať žiadne informácie, kliknite na možnosť **Neodoslať informácie** a pokračujte ďalej.

Odosielanie informácií o systémových nastaveniach môžete nakonfigurovať cez Rozšírené nastavenia > **Nástroje** > **Diagnostika** > Technická podpora.

Ak ste sa rozhodli odoslať systémové nastavenia, je potrebné vyplniť a odoslať webový formulár. V opačnom prípade sa žiadosť o technickú podporu nevytvorí a informácie o systémových nastaveniach sa stratia. Ak systémové nastavenia nie je možné odoslať, vyplňte webový formulár a počkajte na pokyny od pracovníka technickej podpory.

Technická podpora

V hlavnom okne programu kliknite na **Pomocník a podpora** > **Technická podpora**.

Kontaktovať technickú podporu

Požiadať o technickú podporu – v prípade problému, na ktorý nenájdete odpoveď, je možné kontaktovať oddelenie technickej podpory spoločnosti ESET prostredníctvom formulára na webovej stránke. V závislosti od konfigurácie programu sa ešte pred vyplnením webového formulára zobrazí okno s možnosťou odoslať údaje o systémových nastaveniach.

Získať informácie pre technickú podporu

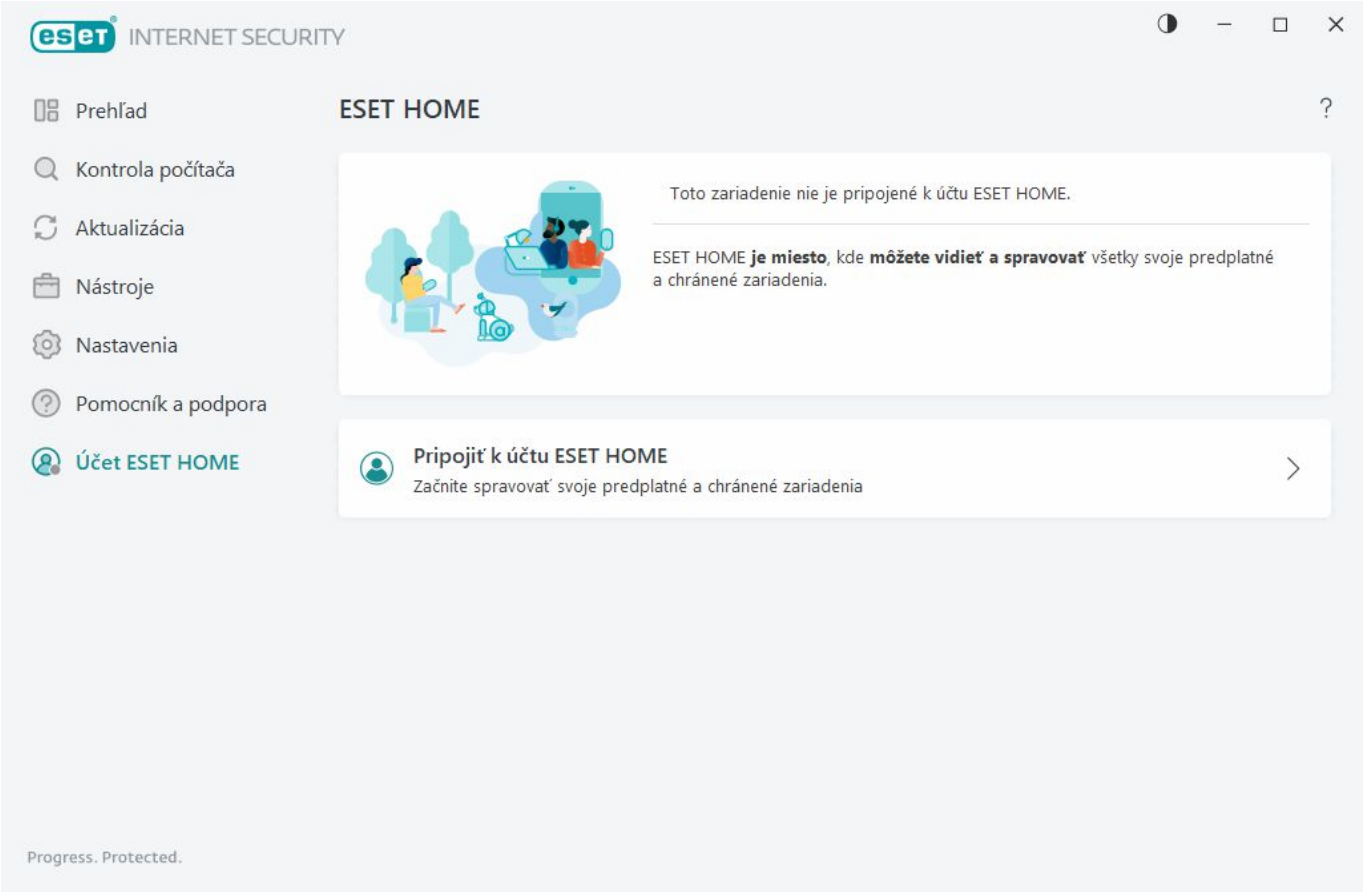
Podrobnosti pre technickú podporu – použite túto možnosť, ak vás technická podpora spoločnosti ESET požiada o skopírovanie a zaslanie základných informácií (zahŕňa napríklad podrobnosti o predplatnom, názov produktu, verziu produktu, operačný systém a informácie o počítači).

ESET Log Collector – odkaz na článok Databázy znalostí spoločnosti ESET, kde si môžete stiahnuť aplikáciu ESET Log Collector, ktorá slúži na automatické zbieranie informácií a protokolov z počítača, čo umožňuje rýchlejšie riešenie problémov. Bližšie informácie nájdete v online príručke pre ESET Log Collector.

Na vytvorenie podrobných protokolov pre všetky dostupné funkcie programu aktivujte možnosť Vytváranie rozšírených protokolov. Takéto protokoly našim vývojárom uľahčia diagnostiku problému a jeho následné riešenie. Úroveň podrobnosti zaznamenávaných informácií je v tomto prípade nastavená na hodnotu **Diagnostické**. Vytváranie rozšírených protokolov sa automaticky vypne po dvoch hodinách, ak tak nespravíte skôr kliknutím na **Prestať zapisovať do rozšírených protokolov**. Po vytvorení všetkých protokolov sa zobrazí okno oznámenia, v ktorom nájdete odkaz pre priamy prístup k priečinku s diagnostickými protokolmi.

Účet ESET HOME

Stav pripojenia k účtu ESET HOME môžete skontrolovať v hlavnom okne programu > **Účet ESET HOME**.



Toto zariadenie nie je pripojené k účtu ESET HOME

Kliknutím na Pripojiť k účtu ESET HOME pripojte zariadenie k účtu ESET HOME a spravujte svoje predplatné a chránené zariadenia. Predplatné si tu môžete jednoducho obnoviť, rozšíriť alebo zmeniť na vyšší produkt a tiež si môžete pozrieť dôležité informácie o predplatnom. V portáli na správu alebo mobilnej aplikácii ESET HOME môžete pridávať predplatné, sťahovať produkty do svojich zariadení a sledovať ich bezpečnostný stav, prípadne zdieľať predplatné s rodinou či priateľmi prostredníctvom e-mailu. Viac informácií nájdete na stránkach Online pomocníka pre ESET HOME.

Toto zariadenie je pripojené k účtu ESET HOME

Bezpečnosť zariadenia môžete spravovať na diaľku pomocou portálu ESET HOME alebo mobilnej aplikácie. Kliknutím na **App Store** alebo **Google Play** sa zobrazí QR kód, ktorý môžete naskenovať mobilným telefónom a následne si stiahnuť mobilnú aplikáciu ESET HOME.

Účet ESET HOME – názov vášho účtu ESET HOME.

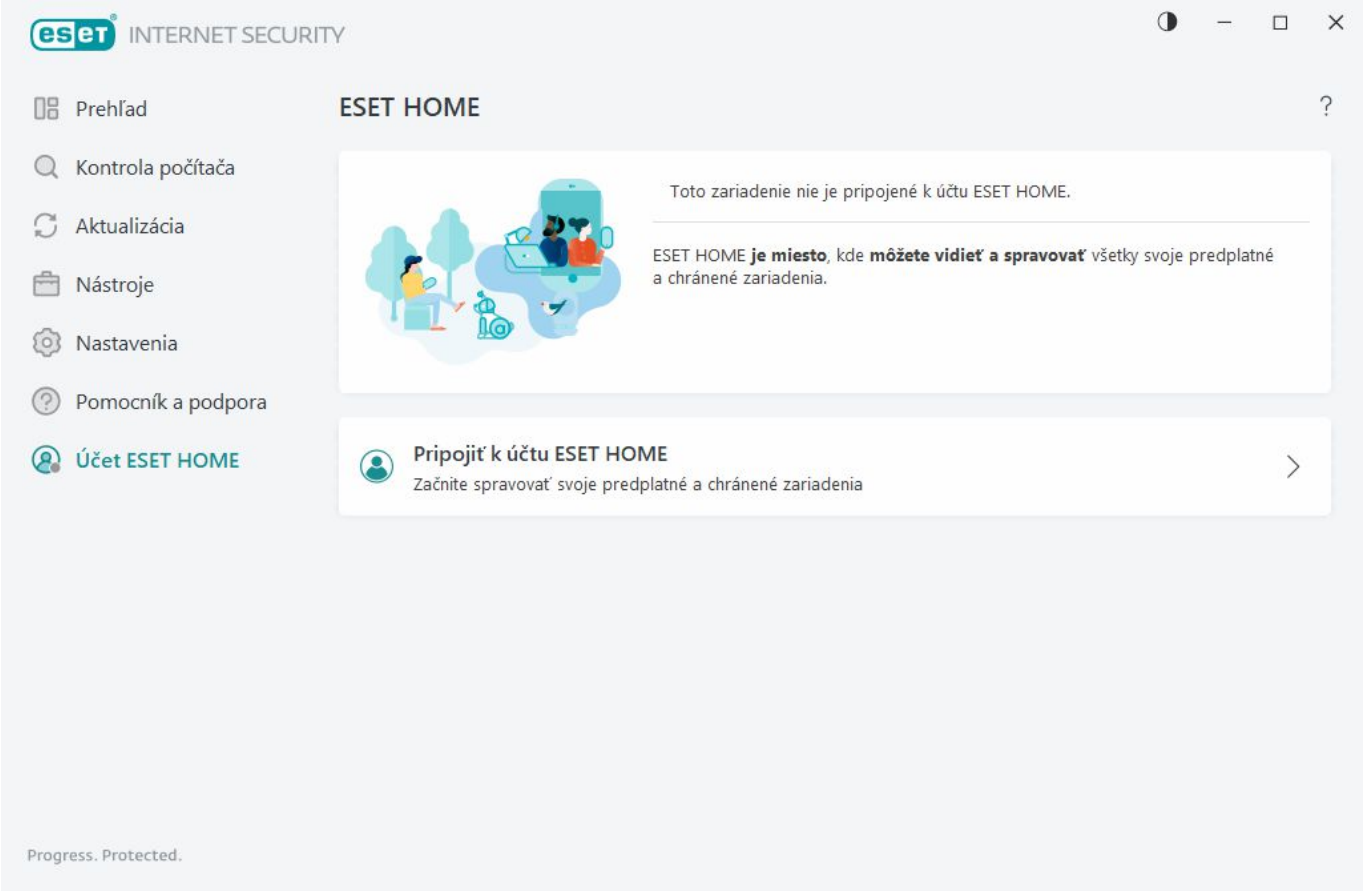
Názov zariadenia – názov tohto zariadenia zobrazený v účte ESET HOME.

Otvoriť ESET HOME – otvorí sa portál na správu ESET HOME.

Ak chcete odpojiť zariadenie od účtu ESET HOME, kliknite na **Odpojiť od účtu ESET HOME** > **Odpojiť**. Predplatné použité na aktiváciu zostane aktívne a vaše zariadenie bude chránené.

Pripojenie k účtu ESET HOME

Pripojte svoje zariadenie k portálu ESET HOME, cez ktorý si môžete pozrieť a spravovať všetky svoje aktivované predplatné od spoločnosti ESET a chránené zariadenia. Predplatné si tu môžete jednoducho obnoviť, rozšíriť alebo zmeniť na vyšší produkt a tiež si môžete pozrieť dôležité informácie o predplatnom. V portáli na správu alebo mobilnej aplikácii ESET HOME môžete pridávať predplatné, sťahovať produkty do svojich zariadení a sledovať ich bezpečnostný stav, prípadne zdieľať predplatné s rodinou či priateľmi prostredníctvom e-mailu. Viac informácií nájdete na stránkach Online pomocníka pre ESET HOME.



Ak chcete pripojiť svoje zariadenie k účtu ESET HOME, postupujte podľa týchto krokov:

Ak sa pripájate k účtu ESET HOME počas inštalácie alebo keď ako spôsob aktivácie zvolíte možnosť **Použiť účet ESET HOME**, postupujte podľa inštrukcií v kapitole Použitie účtu ESET HOME.
Ak ste si už nainštalovali produkt ESET Internet Security a aktivovali ho pomocou predplatného pridaného do vášho účtu ESET HOME, môžete zariadenie pripojiť k účtu ESET HOME cez portál ESET HOME. Postupujte podľa inštrukcií v Online pomocníkovi pre ESET HOME a povoľte pripojenie k účtu v programe ESET Internet Security.

1. V hlavnom okne programu kliknite na **Účet ESET HOME** > **Pripojiť k účtu ESET HOME** alebo môžete v oznámení **Pripojte toto zariadenie k účtu ESET HOME** kliknúť na možnosť **Pripojiť k účtu ESET HOME**.

2. Prihláste sa do svojho účtu ESET HOME.

Ak účet ESET HOME ešte nemáte, kliknite na možnosť **Vytvoriť účet** a zaregistrujte sa. Inštrukcie nájdete na stránke Online pomocníka ESET HOME.
V prípade, že si neviete spomenúť na svoje heslo, kliknite na možnosť **Nepamätám si svoje heslo** a riaďte sa pokynmi na obrazovke, prípadne prejdite na stránku Online pomocníka ESET HOME.

3. Nastavte **Názov zariadenia** a následne kliknite na **Pokračovať**.

4. Po úspešnom pripojení sa zobrazí okno s podrobnosťami. Kliknite na **Hotovo**.

Prihlásenie do účtu ESET HOME

Existuje niekoľko spôsobov, ako sa môžete prihlásiť do svojho účtu ESET HOME:

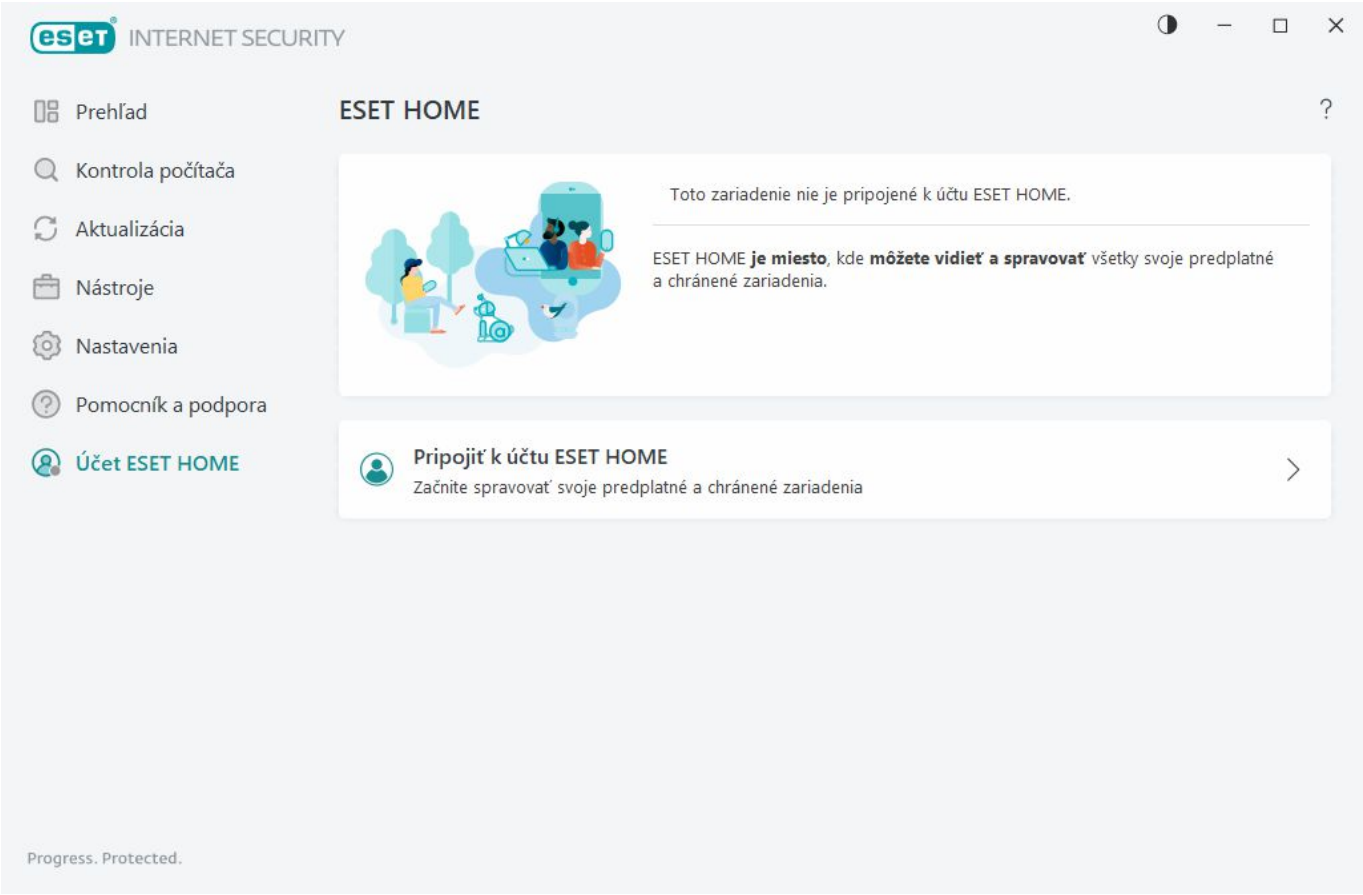
• **Použite e‍mailovú adresu a heslo priradené k účtu ESET HOME** – zadajte **E‍mailovú adresu** a **Heslo**, ktoré ste použili na vytvorenie účtu ESET HOME, a kliknite na **Prihlásiť sa**.

• **Použite účet Google/AppleID** – kliknite na **Pokračovať cez Google** alebo **Pokračovať cez Apple** a prihláste sa do príslušného účtu. Po úspešnom prihlásení vás presmerujeme na potvrdzujúcu webovú stránku ESET HOME. Ak chcete pokračovať, vráťte sa do okna programu ESET. Viac informácií o prihlásení pomocou účtu Google/AppleID nájdete v Online pomocníkovi pre ESET HOME.

• **Skenovať QR kód** – kliknutím na **Skenovať QR kód** sa zobrazí QR kód. Otvorte mobilnú aplikáciu ESET HOME a naskenujte QR kód, prípadne môžete použiť fotoaparát na zariadení. Viac informácií nájdete v Online pomocníkovi pre ESET HOME.

Ak účet ESET HOME ešte nemáte, kliknite na možnosť **Vytvoriť účet** a zaregistrujte sa. Inštrukcie nájdete na stránke Online pomocníka ESET HOME.
V prípade, že si neviete spomenúť na svoje heslo, kliknite na možnosť **Nepamätám si svoje heslo** a riaďte sa pokynmi na obrazovke, prípadne prejdite na stránku Online pomocníka ESET HOME.

Bežné chyby pri prihlasovaní



Bežné chyby pri prihlasovaní

Nepodarilo sa nám nájsť účet, ktorý zodpovedá zadanej e□mailovej adrese.

Zadaná e□mailová adresa sa nezhoduje so žiadnym účtom ESET HOME. Kliknite na **Späť** a zadajte správnu e□mailovú adresu a heslo.

Ak sa chcete prihlásiť, musíte mať vytvorený účet ESET HOME. Ak účet ESET HOME ešte nemáte, kliknite na **Späť** > **Vytvoriť účet** alebo si prečítajte viac o vytvorení nového účtu ESET HOME.

Prihlasovacie meno a heslo sa nezhodujú.

Vložené heslo nezodpovedá zadanej e□mailovej adrese. Kliknite na **Späť**, vložte správne heslo a overte správnosť zadanej e□mailovej adresy. Ak sa vám stále nepodarí prihlásiť, obnovte svoje heslo kliknutím na **Späť** > **Nepamätám si svoje heslo** a postupujte podľa pokynov na obrazovke. Môžete si tiež prečítať viac o tom, ako postupovať v prípade zabudnutého hesla k účtu ESET HOME.

Vybraná možnosť prihlásenia nezodpovedá vášmu účtu.

Váš účet je prepojený s vaším účtom na sociálnych médiách. Ak sa chcete prihlásiť do účtu ESET HOME, kliknite na **Pokračovať cez Google** alebo **Pokračovať cez Apple** a prihláste sa do príslušného účtu. Po úspešnom prihlásení vás presmerujeme na potvrdzujúcu webovú stránku ESET HOME. Ak chcete odpojiť svoj účet na sociálnych médiách od účtu ESET HOME, môžete tak spraviť na portáli ESET HOME.

Nesprávne heslo

Táto chyba sa môže vyskytnúť, keď už máte produkt ESET Internet Security pripojený k účtu ESET HOME a rozhodnete sa urobiť zmeny, ktoré si vyžadujú prihlásenie (napr. vypnutie funkcie Anti-Theft), no zadáte heslo, ktoré sa nezhoduje s vaším účtom. Kliknite na **Späť** a zadajte správne heslo. Ak sa vám stále nepodarí prihlásiť, obnovte svoje heslo kliknutím na **Späť** > **Nepamätám si svoje heslo** a postupujte podľa pokynov na obrazovke. Môžete si tiež prečítať viac o tom, ako postupovať v prípade zabudnutého hesla k účtu ESET HOME.

Pridanie zariadenia v účte ESET HOME

Ak ste si už nainštalovali produkt ESET Internet Security a aktivovali ho pomocou predplatného pridaného do vášho účtu ESET HOME, môžete zariadenie pripojiť k účtu ESET HOME cez portál ESET HOME:

1. Odošlite na zariadenie žiadosť o pripojenie.

2. ESET Internet Security otvorí dialógové okno **Pripojte toto zariadenie k účtu ESET HOME** s názvom účtu ESET HOME. Kliknutím na **Povoliť** pripojíte zariadenie k uvedenému účtu ESET HOME.

Ak nedôjde k žiadnej interakcii, žiadosť o pripojenie bude automaticky zrušená po približne 30 minútach.

Rozšírené nastavenia

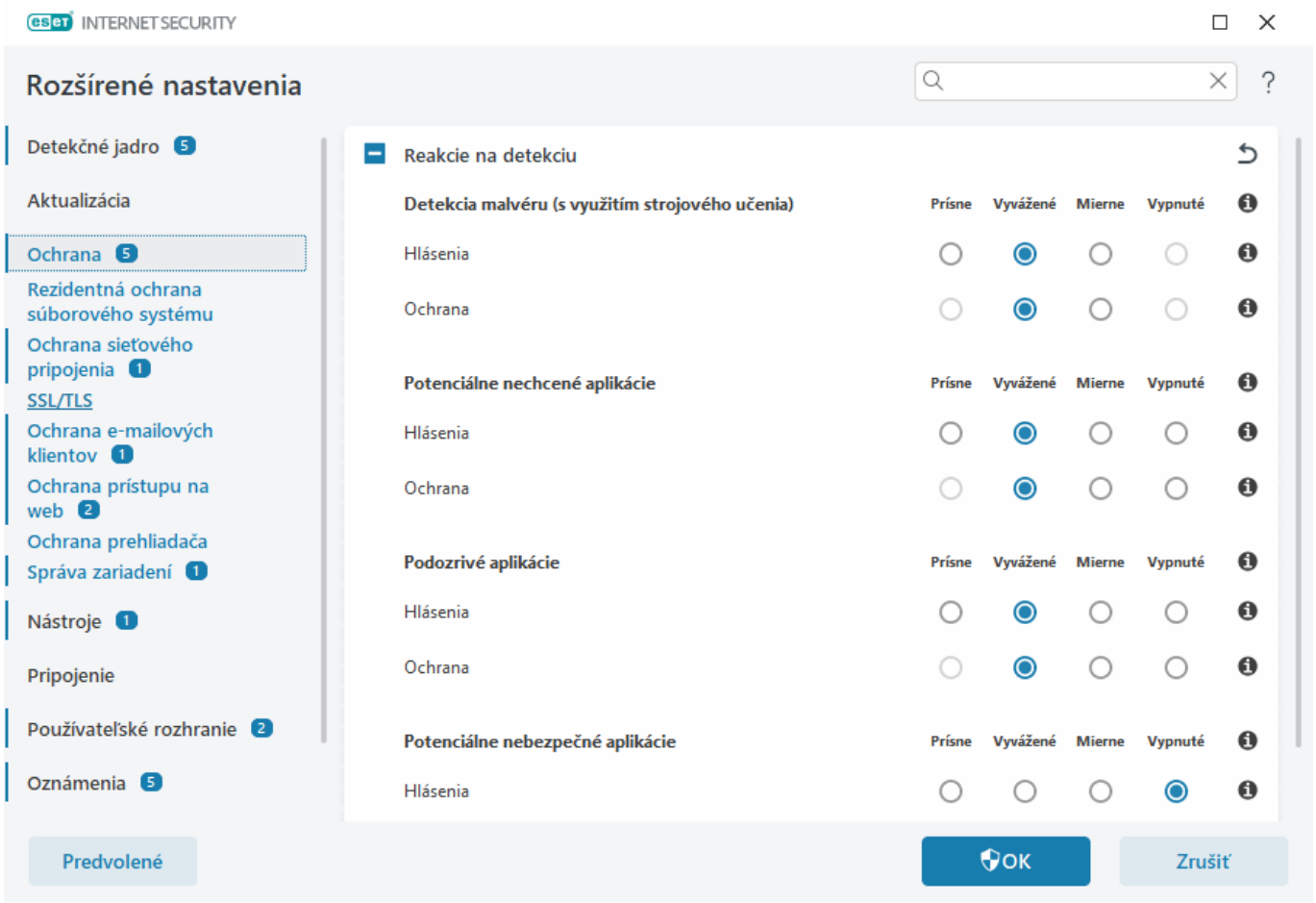
Sekcia rozšírených nastavení vám umožňuje konfigurovať podrobné nastavenia produktu ESET Internet Security podľa vašich potrieb.

Ak chcete otvoriť rozšírené nastavenia, prejdite do hlavného okna programu a stlačte kláves **F5** na klávesnici alebo kliknite na položku **Nastavenia** > **Rozšírené nastavenia**.

> V závislosti od vašich nastavení prístupu sa môže zobraziť výzva na zadanie hesla, ktoré chráni prístup k rozšíreným nastaveniam.

V rozšírených nastaveniach je možné konfigurovať nasledujúce kategórie:

- Detekčné jadro
- Aktualizácia
- Ochrana
- Nástroje
- Pripojenie
- Používateľské rozhranie
- Oznámenia
- Nastavenia ochrany osobných údajov



Detekčné jadro

Cez Rozšírené nastavenia > **Detekčné jadro** môžete konfigurovať nasledujúce možnosti:

- Vylúčenia
- Pokročilé možnosti
- Kontrola sieťovej komunikácie

Vylúčenia

Vylúčenia vám umožňujú vylúčiť konkrétne objekty z detekčného jadra. Aby bola zabezpečená kontrola všetkých objektov, neodporúčame túto možnosť používať, ak to nie je naozaj nevyhnutné. Môžu však nastať situácie, keď je potrebné niektoré objekty z kontroly vylúčiť, napríklad v prípade veľkých databázových súborov, ktorých kontrola by mohla spomaľovať počítač, prípadne niektorých programov, ktoré by mohli byť v konflikte s priebehom kontroly.

Výkonnostné vylúčenia vám umožňujú vybrať súbory a priečinky, ktoré nemajú byť podrobené kontrole. Výkonnostné vylúčenia sú užitočné, ak chcete z kontroly vylúčiť herné aplikácie na úrovni konkrétnych súborov, ak pri kontrole dochádza k nezvyčajnému správaniu systému, prípadne ak chcete týmto spôsobom zvýšiť výkon.

Vylúčenia detekcií vám umožňujú vylúčiť objekty z detekcie podľa názvu detekcie, cesty k objektu alebo hodnoty hash. Vylúčenia detekcií na rozdiel od výkonnostných vylúčení neslúžia na vylúčenie súborov a priečinkov z

kontroly. Vylúčenia detekcií vylúčia iba objekty zachytené detekčným jadrom, pre ktoré sa v zozname vylúčení nachádza zodpovedajúce pravidlo.

Spomenuté vylúčenia si nezamieňajte ani s ďalšími typmi vylúčení:

- Vylúčenia procesov – z kontroly sú vylúčené všetky operácie so súbormi, ktoré sa týkajú vylúčených aplikačných procesov (toto môže byť užitočné pre zvýšenie rýchlosti zálohovania a zlepšenie dostupnosti služieb),
- Prípony súborov vylúčené z kontroly,
- HIPS vylúčenia,
- Filter vylúčení pre ochranu s podporou cloudu.

Výkonnostné vylúčenia

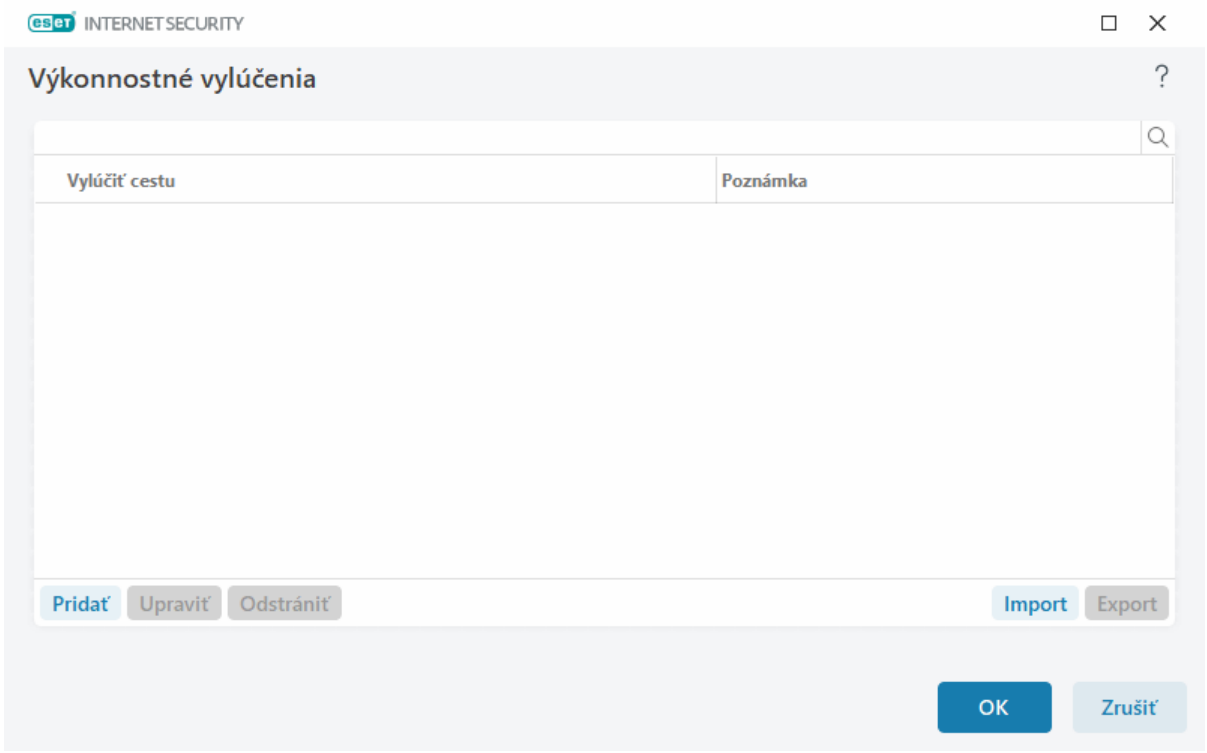
Výkonnostné vylúčenia umožňujú vybrať súbory alebo priečinky, ktoré nemajú byť podrobené kontrole.

Za normálnych okolností sa neodporúča nastavovať vylúčenia z kontroly, ak si chcete byť istý, že všetky objekty budú skontrolované na prítomnosť hrozieb. Môžu nastať situácie, keď je potrebné niektoré objekty z kontroly vylúčiť. Napríklad kontrola veľkých databázových súborov môže spomaliť počítač alebo databázový softvér môže byť v konflikte s priebehom kontroly.

Do zoznamu vylúčení môžete pridať súbory a priečinky, a to v sekcii Rozšírené nastavenia > **Detekčné jadro** > **Vylúčenia** > **Výkonnostné vylúčenia** > **Upraviť**.

> Tento typ vylúčení si nezamieňajte s vylúčeniami detekcií, príponami súborov vylúčených z kontroly, HIPS vylúčeniami a vylúčeniami procesov.

Ak chcete vylúčiť objekt (cesta: súbor alebo priečinok) z kontroly, kliknite na **Pridať** a zadajte cestu k objektu, prípadne ho vyberte v stromovej štruktúre.



Ak súbor spĺňa kritériá vylúčenia z kontroly, moduly **Rezidentná ochrana súborového systému** a **Kontrola počítača** nebudú hrozbu v takomto súbore detegovať.

Ovládacie prvky

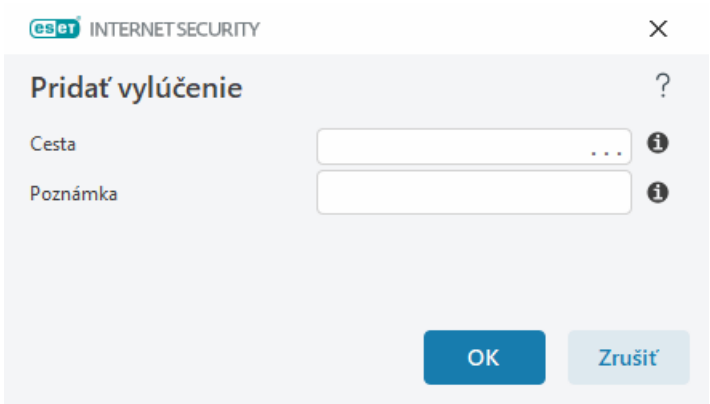
- **Pridať** – pridanie objektu na vylúčenie z detekcie.
- **Upraviť** – úprava zvolených položiek.
- **Odstrániť** – odstránenie zvolených položiek (pri podržaní klávesu CTRL môžete kliknutím označiť viacero položiek).

Pridanie alebo úprava výkonnostných vylúčení

V tomto dialógovom okne môžete vylúčiť konkrétnu cestu (k súboru alebo adresáru) v rámci počítača.

Výber alebo manuálne zadanie cesty

Požadovanú cestu zvolíte kliknutím na **...** v poli **Cesta**.
V prípade manuálneho zadávania si pozrite príklady formátov vylúčení uvedené nižšie.



Pri vylúčení súborov z kontroly môžu byť použité zástupné znaky pre pokrytie skupiny súborov. Otáznik (*?*) slúži na nahradenie jedného ľubovoľného znaku a hviezdička (***) nahrádza ľubovoľný reťazec v dĺžke nula až niekoľko znakov.

Formát vylúčenia

• Ak chcete vylúčiť vo zvolenom adresári všetky súbory a podpriečinky, zadajte cestu k adresáru a použite masku ***
• V prípade vylúčenia všetkých súborov .doc použite masku **.doc*
• Ak má názov spustiteľného súboru určitý počet znakov a vy viete s istotou len začiatočný znak (napr. „D“), použite nasledujúci formát:
D????.exe (otázniky zastupujú chýbajúce/neznáme znaky)
Príklady:
• *C:\Tools** – cesta musí končiť spätnou lomkou (\) a hviezdičkou (*), ak má označovať, že ide o priečinok a všetok jeho obsah (súbory a podpriečinky) bude vylúčený.
• *C:\Tools*.** – funguje rovnako ako *C:\Tools**
• *C:\Tools* – priečinok *Tools* nebude vylúčený. Z pohľadu kontroly by totiž *Tools* mohol byť aj názov súboru.
• *C:\Tools*.dat* – budú vylúčené súbory .dat v priečinku *Tools*.
• *C:\Tools\sg.dat* – bude vylúčený tento konkrétny súbor v danom umiestnení.

Systémové premenné vo vylúčeniach

Pri vytváraní vylúčení z kontroly môžete použiť aj systémové premenné ako %PROGRAMFILES%.
• Ak chcete vylúčiť celý priečinok Program Files pomocou príslušnej systémovej premennej, použite pri vytváraní vylúčenia cestu *%PROGRAMFILES%** (nezabudnite na spätnú lomku a hviezdičku na konci).
• Ak chcete vylúčiť všetky súbory a priečinky v konkrétnom podadresári v rámci *%PROGRAMFILES%*, použite cestu *%PROGRAMFILES%\Vyluceny_podadresar**

Rozbaliť zoznam podporovaných systémových premenných

Vo formáte vylúčenia cesty je možné používať nasledujúce premenné:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
Nie sú podporované premenné špecifické pre používateľa (ako *%TEMP%* alebo *%USERPROFILE%*) alebo premenné prostredia (ako *%PATH%*).

Zástupné znaky uprostred zadávanej cesty nie sú podporované

Používanie zástupných znakov uprostred zadávanej cesty (napríklad *C:\Tools*\Data\file.dat*), môže fungovať, ale pre výkonnostné vylúčenia nie je oficiálne podporované.
V prípade vylúčení detekcií neplatia žiadne obmedzenia pre používanie zástupných znakov uprostred zadávanej cesty.

Poradie vylúčení

- Prioritu vylúčení nie je možné nastaviť či meniť pomocou šípok alebo tlačidiel nahor/nadol (ako napr. v prípade pravidiel firewallu, ktoré sú spúšťané smerom zhora nadol).
- Keď sa pri kontrole uplatní prvé zodpovedajúce pravidlo, ďalšie pravidlo nebude vyhodnocované.
- Čím menej pravidiel, tým lepší výkon kontroly.
- Vyhnite sa vytváraniu súbežných pravidiel.

Formát vylúčenia cesty

Pri vylúčení súborov z kontroly môžu byť použité zástupné znaky pre pokrytie skupiny súborov. Otáznik (*?*) slúži na nahradenie jedného ľubovoľného znaku a hviezdička (***) nahrádza ľubovoľný reťazec v dĺžke nula až niekoľko znakov.

Formát vylúčenia

- Ak chcete vylúčiť vo zvolenom adresári všetky súbory a podpriečinky, zadajte cestu k adresáru a použite masku ***
- V prípade vylúčenia všetkých súborov .doc použite masku **.doc*
- Ak má názov spustiteľného súboru určitý počet znakov a vy viete s istotou len začiatočný znak (napr. „D“), použite nasledujúci formát:

D????.exe (otázniky zastupujú chýbajúce/neznáme znaky)

Príklady:

- *C:\Tools** – cesta musí končiť spätnou lomkou (\) a hviezdičkou (*), ak má označovať, že ide o priečinok a všetok jeho obsah (súbory a podpriečinky) bude vylúčený.
- *C:\Tools*.** – funguje rovnako ako *C:\Tools**
- *C:\Tools* – priečinok *Tools* nebude vylúčený. Z pohľadu kontroly by totiž *Tools* mohol byť aj názov súboru.
- *C:\Tools*.dat* – budú vylúčené súbory .dat v priečinku *Tools*.
- *C:\Tools\sg.dat* – bude vylúčený tento konkrétny súbor v danom umiestnení.

Systémové premenné vo vylúčeniach

Pri vytváraní vylúčení z kontroly môžete použiť aj systémové premenné ako %PROGRAMFILES%.

- Ak chcete vylúčiť celý priečinok Program Files pomocou príslušnej systémovej premennej, použite pri vytváraní vylúčenia cestu *%PROGRAMFILES%** (nezabudnite na spätnú lomku a hviezdičku na konci).
- Ak chcete vylúčiť všetky súbory a priečinky v konkrétnom podadresári v rámci *%PROGRAMFILES%*, použite cestu *%PROGRAMFILES%\Vyluceny_podadresar**

Rozbaliť zoznam podporovaných systémových premenných

Vo formáte vylúčenia cesty je možné používať nasledujúce premenné:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

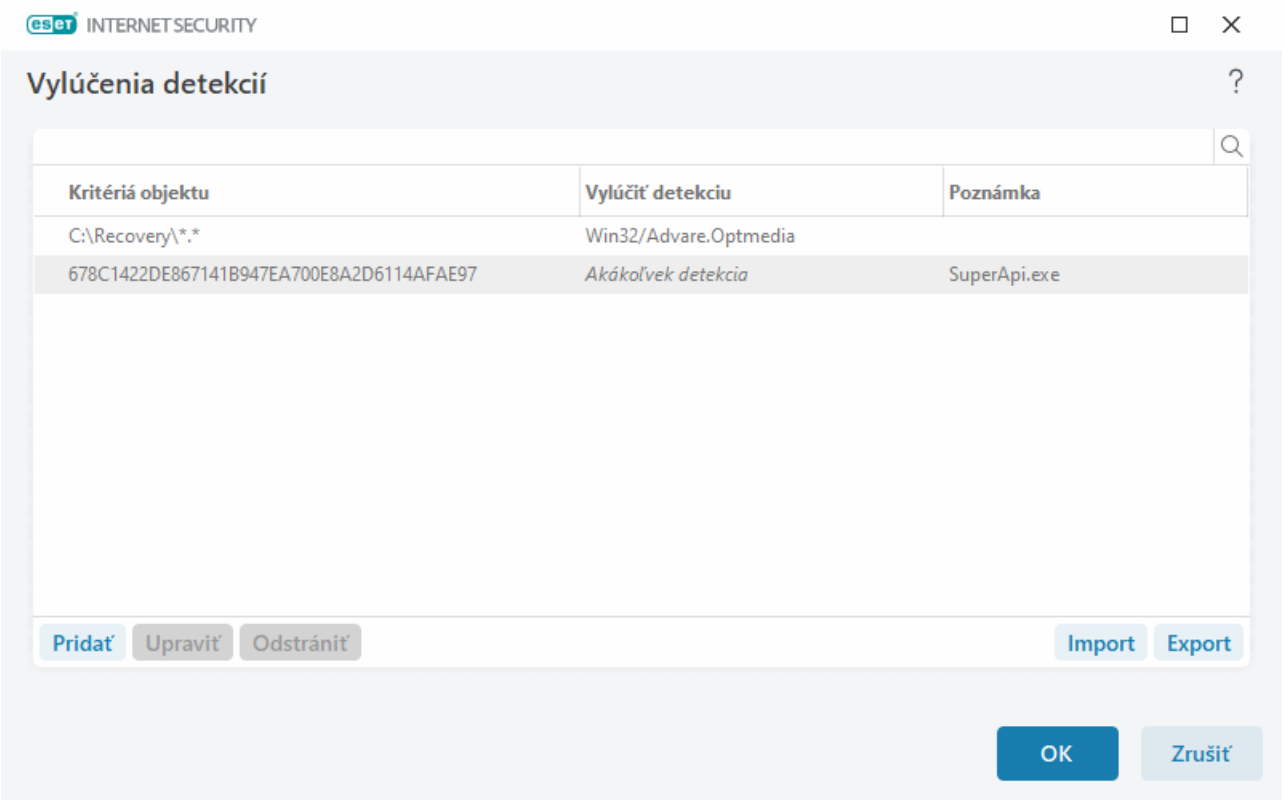
Nie sú podporované premenné špecifické pre používateľa (ako *%TEMP%* alebo *%USERPROFILE%*) alebo premenné prostredia (ako *%PATH%*).

Vylúčenia detekcií

Vylúčenia detekcií umožňujú vylúčiť objekty z detekcie filtrovaním názvu detekcie, cesty k objektu alebo hodnoty hash.

Ako fungujú vylúčenia detekcií

Vylúčenia detekcií na rozdiel od výkonnostných vylúčení neslúžia na vylúčenie súborov a priečinkov z kontroly. Vylúčenia detekcií vylúčia iba objekty zachytené detekčným jadrom, pre ktoré sa v zozname vylúčení nachádza zodpovedajúce pravidlo.
Napríklad podľa prvého riadku na obrázku nižšie, ak je objekt detegovaný ako Win32/Adware.Optmedia a cesta k detegovanému súboru je *C:\Recovery\file.exe*, tento súbor bude vylúčený z detekčného jadra. Druhý riadok znamená, že každý súbor, ktorý má zhodujúci sa hash SHA-1, bude vždy vylúčený bez ohľadu na názov detekcie.



Aby bolo zabezpečené zachytávanie všetkých hrozieb, odporúčame vylúčenia detekcií vytvárať len v tom prípade, že je to naozaj nevyhnutné.

Ak chcete do zoznamu vylúčení pridať súbory a priečinky, prejdite do sekcie Rozšírené nastavenia > **Detekčné jadro** > **Vylúčenia** > **Vylúčenia detekcií** > **Upraviť**.

Tento typ vylúčení si nezamieňajte s výkonnostnými vylúčeniami, príponami súborov vylúčených z kontroly, HIPS vylúčeniami a vylúčeniami procesov.

Ak chcete vylúčiť objekt (podľa názvu detekcie alebo hash) z detekčného jadra, kliknite na možnosť **Pridať**.

Pre potenciálne nechcené aplikácie a potenciálne nebezpečné aplikácie je možné vytvoriť vylúčenie podľa názvu detekcie aj nasledujúcim spôsobom:

- Vo výstražnom okne informujúcom o detekcii kliknite na **Zobraziť pokročilé možnosti** a vyberte možnosť

Vylúčiť z detekcie.

- V kontextovom menu v okne Protokoly použite Sprievodcu vytvorením vylúčenia detekcie.

- V hlavnom okne programu v časti **Nástroje** > **Karanténa** kliknite pravým tlačidlom myši na súbor v karanténe a v kontextovom menu označte možnosť **Obnoviť a vylúčiť z kontroly**.

Kritériá pre vylúčenie detegovaného objektu

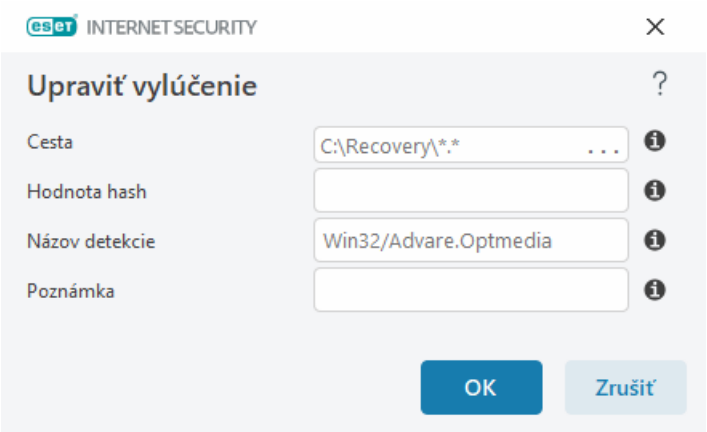
- **Cesta** – umožňuje obmedziť vylúčenie len na konkrétnu cestu.
- **Názov detekcie** – ak je vedľa vylúčeného súboru zobrazený názov detekcie, znamená to, že súbor je vylúčený z kontroly len pre danú detekciu, nie ako celok. Ak by teda došlo k infikovaniu takto vylúčeného súboru iným malvérom, ten bude detekčným jadrom riadne zachytený.
- **Hash** – môžete vylúčiť konkrétny súbor na základe jeho hashu (SHA-1) bez ohľadu na typ súboru, umiestnenie, názov alebo súborovú príponu.

Pridanie alebo úprava vylúčení detekcií

Vylúčenie detekcie

Mali by ste zadávať platný názov, pod ktorým ESET zachytil detekciu. Tento názov nájdete v sekcii Protokoly po zvolení možnosti **Detekcie** z roletového menu Protokoly. Takéto vylúčenie môže byť užitočné napríklad v prípade, že v programe ESET Internet Security dôjde k nesprávnej detekcii vzorky (falošný poplach). Vylúčenie skutočných infiltrácií je však veľmi nebezpečné, zvážte preto vylúčenie len zasiahnutých súborov/adresárov kliknutím na **...** v poli **Cesta** a/alebo vytvorte vylúčenie len na dočasné obdobie. Vylúčenia je možné vytvárať aj pre potenciálne nechcené aplikácie, potenciálne nebezpečné aplikácie a podozrivé aplikácie.

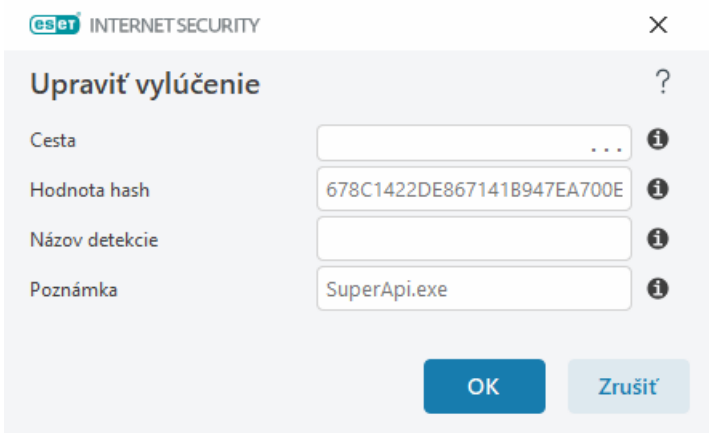
Prečítajte si tiež Formát vylúčenia cesty.



Pozrite si tiež príklad vylúčenia detekcie nižšie.

Vylúčiť hash

Umožní vám vylúčiť konkrétny súbor na základe jeho hashu (SHA-1) bez ohľadu na typ súboru, umiestnenie, názov alebo súborovú príponu.



Vylúčenia podľa názvu detekcie
Ak chcete vylúčiť konkrétnu detekciu podľa jej názvu, zadajte platný názov danej detekcie: Win32/Adware.Optmedia
Ak vytvárate vylúčenie detekcie z okna upozornenia, ktoré zobrazil ESET Internet Security, môžete použiť aj nasledujúci formát:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Ovládacie prvky

- **Pridať** – pridanie objektu na vylúčenie z detekcie.
- **Upraviť** – úprava zvolených položiek.
- **Odstrániť** – odstránenie zvolených položiek (pri podržaní klávesu CTRL môžete kliknutím označiť viacero položiek).

Sprievodca vytvorením vylúčenia detekcie

Vylúčenie detekcie je možné vytvoriť aj z kontextového menu v okne Protokoly (táto možnosť nie je dostupná pre detekcie malvéru):

1. V hlavnom okne programu kliknite na **Nástroje** > **Protokoly**.
2. Kliknite pravým tlačidlom myši na zvolený detegovaný objekt v protokole s názvom **Detekcie**.
3. Kliknite v kontextovom menu na možnosť **Vytvoriť vylúčenie**.

Pre vylúčenie jednej alebo viacerých detekcií na základe **Kritérií vylúčenia** kliknite na možnosť **Zmeniť kritériá**:

- **Konkrétne súbory** – vylúči sa každý súbor podľa jeho hodnoty SHA-1 hash.
- **Detekcia** – vylúči sa každý súbor podľa názvu detekcie.
- **Cesta + detekcia** – vylúči sa každý súbor podľa názvu detekcie a cesty vrátane názvu súboru (napr. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Odporúčaná možnosť je prednastavená na základe typu detekcie.

Pred kliknutím na tlačidlo **Vytvoriť vylúčenie** môžete voliteľne pridať aj **Poznámku**.

Detekčné jadro – pokročilé možnosti

Zapnúť rozšírenú kontrolu prostredníctvom AMSI – nástroj Antimalware Scan Interface (AMSI) spoločnosti Microsoft umožňuje kontrolovať skripty PowerShell, skripty spúšťané programom Windows Script Host a dáta skontrolované použitím AMSI SDK.

Kontrola sieťovej komunikácie

Kontrola sieťovej komunikácie poskytuje ochranu pred malvérom pre aplikačné protokoly, pričom integruje viacero pokročilých techník detekcie škodlivého softvéru. Kontrola protokolov HTTP(S), POP3(S) a IMAP(S) prebieha automaticky a nezávisle od použitého internetového prehliadača alebo e‑mailového klienta. Kontrolu sieťovej komunikácie môžete zapnúť alebo vypnúť v sekcii Rozšírené nastavenia > **Detekčné jadro** > **Kontrola sieťovej komunikácie**.

Zapnúť kontrolu sieťovej komunikácie – ak toto nastavenie vypnete, protokoly HTTP(S), POP3(S) a IMAP(S) sa nebudú kontrolovať. Upozorňujeme, že nasledujúce funkcie programu ESET Internet Security vyžadujú zapnutú kontrolu sieťovej komunikácie:

- Ochrana prístupu na web
- Rodičovská kontrola
- Ochrana súkromia v prehliadači
- Ochrana pri platbách a prehliadaní
- SSL/TLS
- Antiphishingová ochrana
- Ochrana e‑mailových klientov

Ochrana s podporou cloudu

ESET LiveGrid® (založený na pokročilom systéme včasného varovania ThreatSense.Net) pracuje s dátami získanými od používateľov bezpečnostných produktov ESET z celého sveta a tieto dáta zasiela do výskumného laboratória spoločnosti ESET. Vďaka prijatým vzorkám podozrivého softvéru a príslušným metadátam nám ESET LiveGrid® umožňuje okamžite reagovať na najnovšie hrozby, ako aj na požiadavky našich zákazníkov.

K dispozícii sú nasledujúce možnosti:

Zapnúť reputačný systém ESET LiveGrid®

Reputačný systém ESET LiveGrid® poskytuje možnosť cloudového whitelistingu a blacklistingu.

Reputáciu súborov a spustených procesov môžete skontrolovať priamo z používateľského prostredia programu alebo z kontextového menu, cez ktoré je možné získať podrobnejšie informácie zo systému ESET LiveGrid®.

Zapnúť systém spätnej väzby ESET LiveGrid®

Na rozdiel od reputačného systému ESET LiveGrid®, systém spätnej väzby ESET LiveGrid® zozbiera z vášho počítača len tie informácie, ktoré sa týkajú novej hrozby. Môže to byť:

- vzorka alebo kópia súboru, v ktorom sa infiltrácia objavila,
- cesta k súboru,
- názov súboru,
- dátum a čas,
- spôsob, akým sa infiltrácia dostala do vášho počítača,
- informácie o operačnom systéme počítača.

Na základe predvolených nastavení ESET Internet Security odosiela podozrivé vzorky na analýzu do výskumného laboratória spoločnosti ESET. Súbory s niektorými príponami, napríklad *.doc* alebo *.xls*, sa nikdy neodosielajú. Medzi výnimky môžete doplniť aj ďalšie prípony súborov, pri ktorých sa špeciálne chcete vyhnúť možnosti odoslania.

Viac informácií o odosielaní príslušných údajov nájdete v Zásadách ochrany osobných údajov.

Môžete sa rozhodnúť nezapnúť ESET LiveGrid®

Neprídete tým o žiadnu funkcionalitu programu, avšak pri zapnutom systéme ESET LiveGrid® dokáže ESET Internet Security v niektorých prípadoch na nové hrozby reagovať skôr. Ak ste mali zapnutý ESET LiveGrid® a neskôr ste ho vypli, môže sa stať, že v počítači sú už pripravené dátové balíky na odoslanie. Tieto balíky budú odoslané spoločnosti ESET aj po vypnutí systému. Po odoslaní všetkých aktuálnych informácií sa už ďalšie balíky nevytvoria.

Viac o technológii ESET LiveGrid® sa dočítate v slovníku pojmov.
Pozrite si náš článok Databázy znalostí s ilustrovanými inštrukciami o tom, ako zapnúť alebo vypnúť ESET LiveGrid® v produkte ESET Internet Security.

Nastavenia ochrany s podporou cloudu v Rozšírených nastaveniach

Nastavenia funkcie ESET LiveGrid® sú dostupné cez Rozšírené nastavenia > **Detekčné jadro** > **Ochrana s podporou cloudu**.

- **Zapnúť reputačný systém ESET LiveGrid® (odporúčané)** – reputačný systém ESET LiveGrid® zvyšuje efektivitu antimalvérových riešení spoločnosti ESET pomocou porovnávania kontrolovaných súborov s cloudovou databázou dôveryhodných a blokovaných súborov.

- **Zapnúť systém spätnej väzby ESET LiveGrid®** – odosiela do výskumného laboratória ESET Research Lab na ďalšiu analýzu relevantné údaje o vzorkách (popísané nižšie v sekcii **Odosielanie vzoriek**) spolu so správami o

zlyhaní a štatistikami.

• **Odosielať správy o zlyhaniach a diagnostické dáta** – do spoločnosti ESET sa budú odosielať diagnostické dáta súvisiace so systémom ESET LiveGrid®, ako sú správy o zlyhaniach a výpisy pamäte modulov. Pomôže nám to diagnostikovať problémy, ako aj zlepšovať naše produkty a ochranu koncových používateľov.

• **Odosielať anonymné štatistiky** – povoľte spoločnosti ESET zbierať informácie o novonájdených hrozbách, ako ich názov, čas detekcie, spôsob detekcie a súvisiace metadáta, verziu a nastavenie produktu či informácie o vašom systéme.

• **Kontaktný e□mail (nepovinný údaj)** – zadaný kontaktný e□mail bude môcť byť odoslaný spoločne s podozrivým súborom a môže byť použitý na vyžiadanie ďalších informácií. Pracovníci výskumného laboratória ESET vás spätne kontaktujú iba v tom prípade, ak budú potrebovať doplňujúce informácie.

Odosielanie vzoriek

Manuálne odosielanie vzoriek – umožňuje manuálne odosielať vzorky na analýzu do spoločnosti ESET priamo z kontextového menu, karantény alebo sekcie Nástroje.

Automatické odosielanie zachytených vzoriek

Vyberte, ktoré typy vzoriek budú zasielané do spoločnosti ESET na analýzu, čím tiež prispejete k zlepšovaniu detekcie do budúcnosti (predvolená maximálna veľkosť vzorky je 64 MB). K dispozícii sú nasledujúce možnosti:

• **Všetky zachytené vzorky** – všetky objekty zachytené detekčným jadrom (vrátane potenciálne nechcených aplikácií, ak je to povolené v nastaveniach kontroly).

• **Všetky vzorky okrem dokumentov** – všetky zachytené objekty okrem **dokumentov** (pozri nižšie).

• **Neposielať** – zachytené objekty sa nebudú odosielať spoločnosti ESET.

Automatické odosielanie podozrivých vzoriek

Tieto vzorky sa budú do spoločnosti ESET zasielať aj v prípade, že ich detekčné jadro nezachytí. Ide napríklad o vzorky, ktoré tesne unikli detekcii alebo ktoré niektorý z modulov ochrany ESET Internet Security považuje za podozrivé, prípadne o vzorky s nejasným správaním (predvolená maximálna veľkosť vzorky je 64 MB).

• **Spustiteľné súbory** – zahŕňa typy spustiteľných súborov ako .exe, .dll, .sys.

• **Archívy** – zahŕňa typy archívnych súborov ako .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Skripty** – zahŕňa typy súborov ako .bat, .cmd, .hta, .js, .vbs, .ps1.

• **Iné** – zahŕňa typy súborov ako .jar, .reg, .msi, .sfw, .lnk.

• **Potenciálne spamové e□maily** – umožňuje odosielanie častí alebo celých potenciálnych spamových e□mailov s prílohami do spoločnosti ESET na ďalšiu analýzu. Povolenie tejto možnosti nám umožňuje zlepšovať globálnu detekciu spamu, ako aj do budúcna prinášať lepšiu detekciu spamu.

• **Dokumenty** – zahŕňa dokumenty Microsoft Office alebo PDF s aktívnym obsahom aj bez neho.

Rozbaliť zoznam všetkých zahrnutých typov súborov

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Vylúčenia

Pomocou filtra vylúčení môžete z odosielania vylúčiť súbory/priečinky (toto môže byť užitočné pri súboroch obsahujúcich dôverné či citlivé informácie, ako sú dokumenty alebo tabuľky). Súbory pridané do vylúčení nebudú nikdy odoslané na analýzu do laboratórií spoločnosti ESET, a to ani za predpokladu, že obsahujú podozrivý kód. Najbežnejšie typy súborov sú predvolene vylúčené (napr. súbory s príponou .doc). Do zoznamu vylúčení môžete pridávať ľubovoľné typy súborov.

Ak chcete vylúčiť súbory stiahnuté z `download.domain.com`, otvorte Rozšírené nastavenia > **Detekčné jadro** > **Ochrana s podporou cloudu** > **Odosielanie vzoriek** a následne kliknite na možnosť **Upraviť** vedľa popisu **Vylúčenia**. Pridajte vylúčenie `.download.domain.com`.

Maximálna veľkosť vzoriek (MB) – definuje maximálnu veľkosť automaticky odosielaných vzoriek (1 – 64 MB).

Filter vylúčení pre ochranu s podporou cloudu

Filter vylúčení umožňuje nastaviť súbory a priečinky, ktoré sa nemajú odosielať ako vzorky. Súbory pridané do vylúčení nebudú nikdy odoslané na analýzu do laboratórií spoločnosti ESET, a to ani za predpokladu, že obsahujú podozrivý kód. Bežné typy súborov (napríklad .doc) sú predvolene vylúčené.

Táto funkcia je užitočná pri vylúčení súborov, v ktorých sa zvyčajne nachádzajú dôverné informácie, napríklad textové dokumenty a tabuľkové hárky.

Ak chcete vylúčiť súbory stiahnuté z download.domain.com, kliknite na Rozšírené nastavenia > **Detekčné jadro** > **Ochrana s podporou cloudu** > **Odosielanie vzoriek** > **Vylúčenia** a pridajte vylúčenie *download.domain.com*.

Detekcia malvéru

Sekcia **Detekcia malvéru** je dostupná v Rozšírených nastaveniach po kliknutí na **Detekčné jadro** > **Detekcia malvéru** a umožňuje konfigurovať parametre kontroly pre profily kontroly.

Manuálna kontrola

Aktívny profil – určuje názov profilu, ktorého nastavenia sa použijú pri manuálne spustenej kontrole. Pridať nový profil je možné prostredníctvom tlačidla **Upraviť** v časti **Zoznam profilov**. Viac informácií nájdete v kapitole Profily kontroly.

Po výbere profilu kontroly môžete nakonfigurovať nasledujúce možnosti:

Ciele kontroly – ak si želáte skontrolovať konkrétny súbor alebo skupinu súborov na disku, kliknite na **Upraviť** vedľa popisu **Ciele kontroly** a z adresárovej štruktúry vyberte príslušnú možnosť. Viac informácií nájdete v kapitole Ciele kontroly.

Manuálna kontrola s využitím strojového učenia – pre každý profil kontroly možno nakonfigurovať úrovne hlásení a ochrany. Profily kontroly predvolene používajú rovnaké nastavenie ako je definované v rámci Rezidentnej ochrany súborového systému. Deaktivujte možnosť **Použiť nastavenia rezidentnej ochrany** na konfiguráciu vlastných úrovní hlásení a ochrany. Podrobné vysvetlenie úrovní hlásení a ochrany nájdete v kapitole Ochrana.

ThreatSense – rozšírené možnosti nastavenia, napríklad prípony súborov, ktoré chcete kontrolovať, a používané metódy detekcie. Ďalšie informácie nájdete v kapitole ThreatSense.

Profily kontroly

ESET Internet Security ponúka 4 prednastavené profily kontroly:

- **Smart kontrola** – toto je predvolený profil pokročilej kontroly. Profil Smart kontroly využíva technológiu Smart optimalizácie na vylúčenie súborov, ktoré boli počas predchádzajúcej kontroly vyhodnotené ako neškodné a odvtedy neboli zmenené. Vďaka tomu je čas kontroly kratší, pričom vplyv na bezpečnosť systému je minimálny.

- **Kontrola z kontextového menu** – kontrolu ľubovoľného súboru môžete spustiť manuálne z kontextového menu. Profil Kontroly z kontextového menu umožňuje nastaviť konfiguráciu kontroly, ktorá bude použitá pri spustení kontroly.

- **Hĺbková kontrola** – profil Hĺbkovej kontroly štandardne nevyužíva Smart optimalizáciu, čo znamená, že ak použijete tento profil, z kontroly nebudú vylúčené žiadne súbory.

- **Kontrola počítača** – toto je predvolený profil použitý pri štandardnej kontrole počítača.

Preferované nastavenia kontroly je možné uložiť do profilov pre budúce použitie. Odporúčame vám, aby ste vždy vytvorili nový profil (s rôznymi cieľmi kontroly, metódami kontroly a ďalšími parametrami) pre každú pravidelne používanú kontrolu.

Na vytvorenie nového profilu otvorte Rozšírené nastavenia > **Detekčné jadro** > **Detekcia malvéru** > **Manuálna kontrola** > **Zoznam profilov** > **Upraviť**. Otvorí sa okno **Manažér profilov**, v ktorom sa nachádza roletové menu **Aktívny profil** obsahujúce zoznam existujúcich profilov kontroly, ako aj možnosť vytvoriť nový profil kontroly. Pre objasnenie ako vytvoriť profil kontroly podľa vašich predstáv si pozrite kapitolu ThreatSense, ktorá obsahuje popis každého parametra kontroly.

> Povedzme, že chcete vytvoriť vlastný profil kontroly a čiastočne vám vyhovujú nastavenia predvoleného profilu používaného v prípade funkcie **Skontrolovať váš počítač**. Nechcete však kontrolovať runtime archívy či potenciálne nebezpečné aplikácie a chcete tiež použiť nastavenie **Vždy vyriešiť detekciu**. Zadajte názov nového profilu do okna **Manažér profilov** a kliknite na **Pridať**. Označte svoj nový profil v roletovom menu **Aktívny profil**, upravte ostatné parametre tak, aby vám vyhovovali, a profil uložte kliknutím na **OK**.

Ciele kontroly

Roletové menu **Ciele kontroly** umožňuje vybrať na kontrolu preddefinované objekty.

- **Podľa nastavenia profilu** – vykoná výber cieľov uložených v profile.
- **Vymeniteľné médiá** – vyberie diskety, CD/DVD, USB kľúče atď.

- **Lokálne disky** – vyberie lokálne pevné disky v počítači.
- **Sieťové disky** – vyberie mapované sieťové disky.
- **Vlastný výber** – zruší celý predchádzajúci výber.

Adresárová (stromová) štruktúra tiež obsahuje konkrétne ciele kontroly.

- **Operačná pamäť** – skontrolujú sa všetky procesy a dáta aktuálne používané operačnou pamäťou.
- **Zavádzacie sektory/UEFI** – skontrolujú sa zavádzacie sektory a UEFI na prítomnosť malvéru. Viac o kontrole UEFI sa dočítate v slovníku pojmov.
- **Databáza WMI** – skontroluje sa celá databáza služby Windows Management Instrumentation (WMI), všetky priestory názvov, všetky inštancie triedy a vlastnosti. Vyhľadajú sa odkazy na infikované súbory alebo malvér vložený ako dáta.
- **Systémová databáza Registry** – skontroluje sa celá systémová databáza Registry, všetky kľúče a podkľúče. Vyhľadajú sa odkazy na infikované súbory alebo malvér vložený ako dáta. Pri liečení detekcie zostane v databáze Registry odkaz, aby sa zabránilo strate dôležitých dát.

Ak chcete rýchlo prejsť k požadovanému cieľu kontroly (súbor alebo priečinok), zadajte jeho cestu do textového poľa pod stromovou štruktúrou. V ceste sa rozlišujú veľké a malé písmená. Označením políčka v stromovej štruktúre pridáte daný cieľ do zoznamu cieľov, ktoré sa majú skontrolovať.

Kontrola v nečinnosti

Kontrolu v nečinnosti môžete povoliť v Rozšírených nastaveniach v časti **Detekčné jadro** > **Detekcia malvéru** > **Kontrola v nečinnosti**.

Kontrola v nečinnosti

Túto funkciu zapnete pomocou prepínacieho tlačidla vedľa popisu **Zapnúť kontrolu v nečinnosti**. Ak je počítač v nečinnosti, na pozadí sa spúšťa kontrola všetkých diskov počítača.

Na základe predvolených nastavení programu sa kontrola v nečinnosti nespúšťa, ak je počítač (laptop) napájaný z batérie. Toto nastavenie môžete prepísať zapnutím funkcie **Spustiť, aj keď je počítač napájaný z batérie** v okne Rozšírených nastavení.

Ak chcete z kontroly počítača vytvárať protokol, v Rozšírených nastaveniach kliknite na prepínacie tlačidlo **Vytvárať protokol**. Tento protokol potom nájdete v sekcii Protokoly (v hlavnom okne programu kliknite na **Nástroje** > **Protokoly** a z roletového menu **Protokoly** vyberte možnosť **Kontrola počítača**).

Detekcia stavu nečinnosti

O podmienkach spustenia kontroly v nečinnosti sa dočítate v kapitole Detekcia stavu nečinnosti.

ThreatSense – rozšírené možnosti nastavenia, napríklad prípony súborov, ktoré chcete kontrolovať, a používané metódy detekcie. Viac informácií nájdete v kapitole ThreatSense.

Detekcia stavu nečinnosti

Nastavenia detekcie stavu nečinnosti sa nachádzajú v Rozšírených nastaveniach v sekcii **Detekčné jadro** > **Detekcia malvéru** > **Kontrola v nečinnosti** > **Detekcia stavu nečinnosti**. Tieto nastavenia špecifikujú spúšťač pre kontrolu v nečinnosti:

- **Vypnutá obrazovka alebo šetrič obrazovky**
- **Uzamknutie počítača**
- **Odhlásenie používateľa**

Pomocou prepínacích tlačidiel pri týchto možnostiach môžete zapnúť alebo vypnúť dané spúšťače kontroly v nečinnosti.

Kontrola pri štarte

Na základe predvolených nastavení programu bude po štarte systému a počas aktualizácií detekčného jadra vykonaná automatická kontrola súborov spúšťaných pri štarte. Táto kontrola závisí od nastavení plánovača a úloh.

Nastavenia tejto kontroly sú súčasťou plánovanej úlohy s názvom **Kontrola súborov spúšťaných pri štarte počítača**. Ak chcete zmeniť nastavenia úlohy, prejdite do sekcie **Nástroje** > **Plánovač**, označte položku **Kontrola súborov spúšťaných pri štarte počítača** a kliknite na **Upraviť**. V poslednom kroku sa zobrazí okno Kontrola súborov spúšťaných pri štarte počítača. Podrobné inštrukcie týkajúce sa vytvárania a správy plánovaných úloh nájdete v časti o vytváraní nových úloh.

ThreatSense – rozšírené možnosti nastavenia, napríklad prípony súborov, ktoré chcete kontrolovať, a používané metódy detekcie. Viac informácií nájdete v kapitole ThreatSense.

Kontrola súborov spúšťaných pri štarte počítača

Pri vytváraní úlohy Kontrola súborov spúšťaných pri štarte počítača v plánovači máte na výber nasledujúce možnosti:

V roletovom menu **Cieľ kontroly** sa určuje hĺbka kontroly súborov spúšťaných pri štarte operačného systému. Ich poradie je určené podľa počtu kontrolovaných súborov:

- **Všetky registrované súbory** (najviac kontrolovaných súborov)
- **Zriedkavo používané súbory**
- **Bežne používané súbory**
- **Často používané súbory**
- **Iba najčastejšie používané súbory** (najmenej kontrolovaných súborov)

Patria sem aj dve špeciálne skupiny:

- **Súbory spúšťané pred prihlásením používateľa** – obsahuje množstvo súborov z umiestnení, z ktorých sa môžu spúšťať súbory bez toho, aby bol používateľ prihlásený (zahŕňa takmer všetky startup lokácie, ako napr. služby, pomocné objekty prehľadávača, winlogon notify, položky plánovača systému Windows, známe dll súbory atď.).

- **Súbory spúšťané po prihlásení používateľa** – obsahuje súbory z umiestnení, ku ktorým možno pristupovať len po prihlásení používateľa (zahŕňa súbory spúšťané iba konkrétnym používateľom, napr. súbory v umiestnení *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Zoznamy súborov, ktoré sa majú kontrolovať, sú stanovené pre každú skupinu vyššie. Ak pre súbory spúšťané pri štarte operačného systému vyberiete nižšiu hĺbku kontroly, neskontrolované súbory sa budú kontrolovať po otvorení alebo spustení.

Priorita kontroly – priorita, s ktorou bude spustená kontrola:

- **Počas nečinnosti** – v momente, keď nie sú vykonávané žiadne iné činnosti.

- **Najnižší** – zaťaženie systému je najnižšie možné,

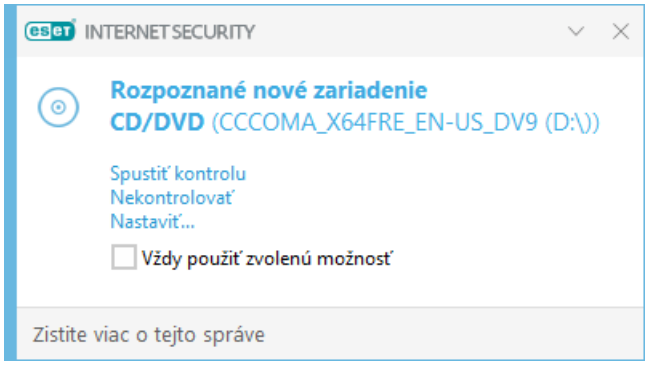
- **Nižší** – zaťaženie systému je nižšie,

- **Normálny** – zaťaženie systému je normálne,

Vymeniteľné médiá

ESET Internet Security poskytuje automatickú kontrolu vložených alebo pripojených vymeniteľných médií (CD/DVD/USB...). Toto môže byť užitočné v prípade, že chce správca zabrániť používateľom vložiť alebo pripojiť do počítača vymeniteľné médium s nežiaducim obsahom.

Ak je v sekcii Rozšírené nastavenia > **Detekčné jadro** > **Detekcia malvéru** > **Vymeniteľné médiá** nastavená akcia **Zobraziť možnosti kontroly**, po vložení alebo pripojení vymeniteľného média sa zobrazí nasledujúce dialógové okno:



Toto dialógové okno ponúka nasledujúce možnosti:

- **Kontrolovať teraz** – spustí sa kontrola vymeniteľného média.

- **Nekontrolovať** – vymeniteľné médiá nebudú kontrolované.

- **Nastavenia** — otvorí sa okno s Rozšírenými nastaveniami.

- **Vždy použiť zvolenú možnosť** – ak začiarknete túto možnosť, rovnaká akcia bude vykonaná pri ďalšom vložení alebo pripojení vymeniteľného média do počítača.

ESET Internet Security navyše obsahuje funkciu Správa zariadení, ktorá vám umožňuje vytvárať pravidlá pre používanie externých zariadení na danom počítači. Viac informácií nájdete v kapitole Správa zariadení.

Nastavenia kontroly vymeniteľných médií sú dostupné cez Rozšírené nastavenia > **Detekčné jadro** > **Detekcia malvéru** > **Vymeniteľné médiá**.

Vykonať akciu po pripojení vymeniteľného média – vyberte predvolenú akciu, ktorá bude automaticky vykonaná po pripojení vymeniteľného média do počítača (CD/DVD/USB). Vyberte požadovanú akciu, ktorá sa má vykonať po vložení alebo pripojení vymeniteľného média do počítača:

- **Nekontrolovať** – nevykoná sa žiadna akcia a okno **Rozpoznané nové zariadenie** sa neotvorí.
- **Automaticky skontrolovať zariadenie** – spustí sa kontrola vloženého zariadenia.
- **Zobraziť možnosti kontroly** – zobrazia sa nastavenia kontroly **vymeniteľných médií**.

Ochrana dokumentov

Modul ochrany dokumentov kontroluje dokumenty Microsoft Office pred ich otvorením a kontroluje objekty pri automatickom sťahovaní pomocou programu Internet Explorer, napríklad prvky Microsoft ActiveX. Ochrana dokumentov poskytuje dodatočnú vrstvu ochrany k modulu Rezidentnej ochrany súborového systému. Ochranu dokumentov možno vypnúť s cieľom zvýšiť výkon na systémoch, kde sa nepracuje s veľkým počtom dokumentov balíka Microsoft Office.

Ak chcete aktivovať Ochranu dokumentov, otvorte Rozšírené nastavenia > **Detekčné jadro** > **Detekcia malvéru** > **Ochrana dokumentov** a kliknite na prepínacie tlačidlo vedľa možnosti **Zapnúť ochranu dokumentov**.

ThreatSense – rozšírené možnosti nastavenia, napríklad prípony súborov, ktoré chcete kontrolovať, a používané metódy detekcie. Viac informácií nájdete v kapitole ThreatSense.

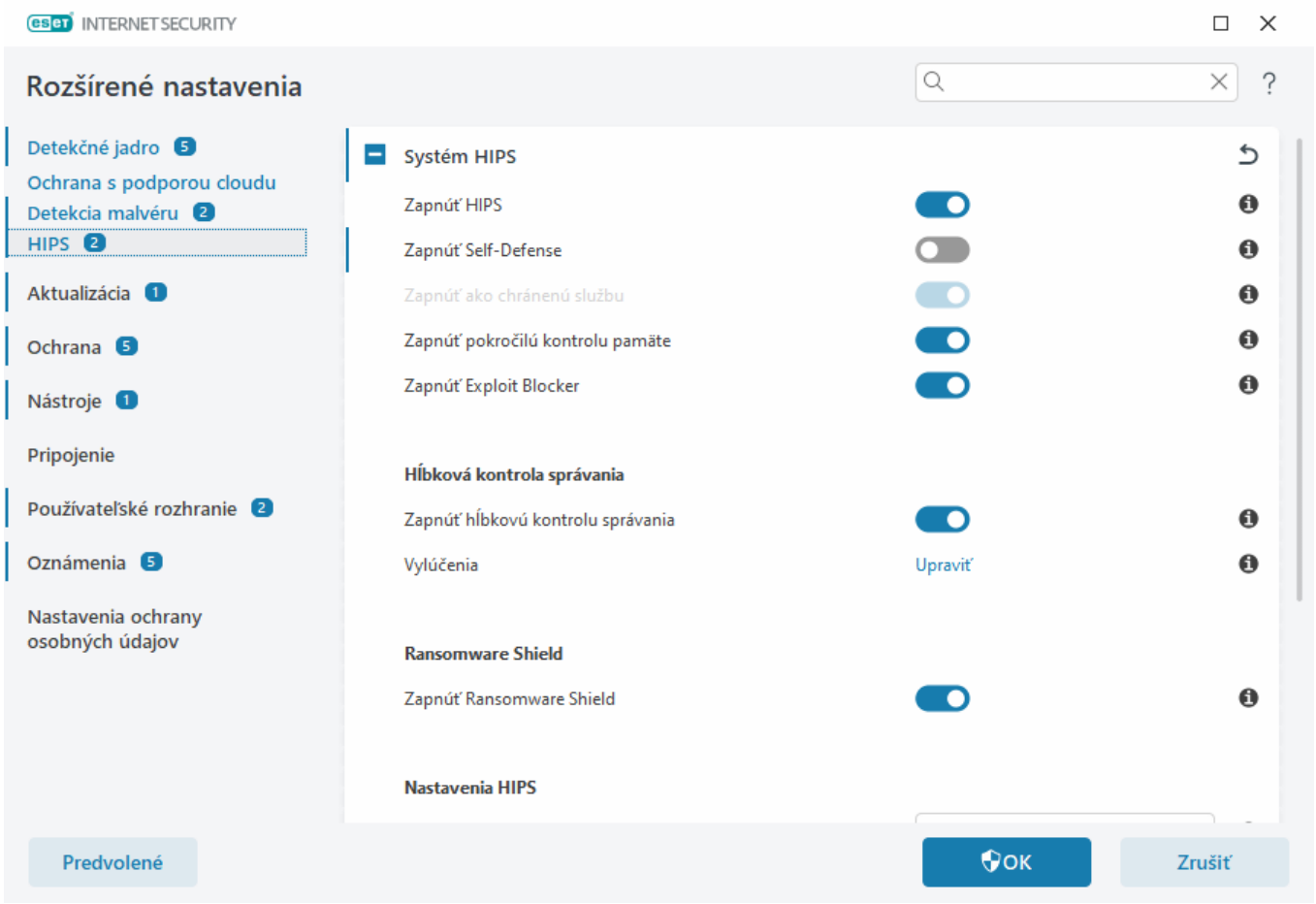
Tento modul pracuje iba s aplikáciami, ktoré podporujú rozhranie Microsoft Antivirus API (napríklad Microsoft Office 2000 a novšie verzie alebo Microsoft Internet Explorer 5.0 a novšie verzie).

Systém HIPS – Host Intrusion Prevention System

Zmeny v nastaveniach systému HIPS odporúčame robiť len skúseným používateľom. Nesprávne nastavenia v sekcii HIPS môžu spôsobiť nestabilitu systému.

Host Intrusion Prevention System (HIPS) chráni pred malvérom a nechcenou aktivitou, ktorá môže negatívne pôsobiť na systém. Používa pokročilú analýzu správania, ktorá spolu s detekčnými schopnosťami sieťového filtra zabezpečuje efektívne sledovanie spustených procesov, súborov a záznamov v registroch, čo umožňuje aktívne blokovať takéto pokusy a predchádzať im. HIPS pracuje oddelene od firewallu a rezidentnej ochrany súborového systému, pričom sleduje len procesy spustené v rámci operačného systému.

Nastavenia HIPS môžete nakonfigurovať v časti Rozšírené nastavenia > **Detekčné jadro** > **HIPS** > **Host Intrusion Prevention System**. Stav modulu HIPS (zapnutý/vypnutý) je zobrazený v hlavnom okne programu ESET Internet Security v časti **Nastavenia** > **Ochrana počítača**.



Systém HIPS

Zapnúť HIPS – HIPS je v ESET Internet Security predvolene zapnutý. Vypnutie systému HIPS spôsobí vypnutie aj jeho funkcií, ako napr. Exploit Blocker.

Zapnúť Self-Defense – ESET Internet Security má ako súčasť systému HIPS vstavanú technológiu **Self-Defense**, ktorej cieľom je zabrániť škodlivému softvéru narušiť alebo deaktivovať antivírusovú a antispyvérovú ochranu. Self-Defense chráni dôležité procesy v rámci systému a programu ESET, súbory a záznamy v databáze Registry pred neoprávnenými zmenami.

Zapnúť ako chránenú službu – povoľuje ochranu pre službu ESET (ekrn.exe). Ak je táto možnosť povolená, služba je spustená ako zabezpečený proces systému Windows s cieľom poskytnúť ochranu pred malvérom.

Zapnúť pokročilú kontrolu pamäte – spolu s funkciou Exploit Blocker poskytuje lepšiu ochranu pred malvérom, ktorý bol navrhnutý tak, aby maskovaním alebo šifrovaním obišiel detekciu bezpečnostných produktov. Pokročilá kontrola pamäte je v predvolených nastaveniach povolená. Viac o tomto type ochrany sa dočítate v slovníku pojmov.

Zapnúť Exploit Blocker – táto funkcia slúži na ochranu najčastejšie zneužívaných aplikácií, ako sú webové prehliadače, softvér na zobrazovanie PDF dokumentov, e-mailové klienty a súčasti balíka Microsoft Office. Exploit Blocker je v predvolených nastaveniach zapnutý. Viac o tomto type ochrany sa dočítate v slovníku pojmov.

Hĺbková kontrola správania

Zapnúť hĺbkovú kontrolu správania – dodatočná vrstva ochrany, ktorá funguje ako súčasť funkcie HIPS. Jej úlohou je analyzovať správanie všetkých procesov spustených na počítači a upozorniť vás na zachytené škodlivé správanie.

HIPS vylúčenia z hĺbkovej kontroly správania vám umožňujú nastaviť procesy, ktoré nemajú byť podrobené analýze. Aby bola zaručená kontrola všetkých procesov na prítomnosť hrozieb, neodporúčame vylúčenia vytvárať, ak to nie je naozaj nevyhnutné.

Ransomware Shield

Zapnúť Ransomware Shield – dodatočná vrstva ochrany, ktorá funguje ako súčasť funkcie HIPS. Aby mohol Ransomware Shield fungovať, je potrebné mať povolený systém ESET LiveGrid®. Viac o tomto type ochrany sa môžete dočítať tu.

Zapnúť Intel® Threat Detection Technology – táto technológia pomáha odhaľovať útoky ransomvéru pomocou jedinečnej telemetrie na úrovni procesora Intel, ktorá zvyšuje účinnosť detekcie, znižuje počet falošných poplachov a rozširuje možnosti zachytávania pokročilých malvérových techník obchádzania detekcie v pamäti. Pozrite si podporované procesory.

Nastavenia HIPS

Režim filtrovania umožňuje nastaviť filtrovanie do jedného z nasledujúcich režimov:

Režim filtrovania	Popis
Automatický režim	Operácie budú povolené s výnimkou takých, ktoré sú blokované prednastavenými pravidlami chrániacimi systém.
Smart režim	Používateľ bude upozornený len v prípade skutočne podozrivých udalostí v systéme.
Interaktívny režim	Používateľ bude vyzvaný na potvrdenie operácií.
Režim politík	Blokuje všetky operácie, ktoré nie sú definované konkrétnym pravidlom, ktoré ich povoľuje.
Učiaci sa režim	Operácie sú povolené a zároveň sa po každej operácii vytvorí pravidlo. Pravidlá vytvorené v tomto režime sú viditeľné v editore **pravidiel HIPS**, ale majú nižšiu prioritu ako pravidlá vytvorené manuálne alebo v automatickom režime. Keď z roletového menu **Režim filtrovania** vyberiete možnosť **Učiaci sa režim**, sprístupní sa nastavenie s popisom **Učiaci sa režim skončí**, ktoré vám umožňuje definovať dátum a čas ukončenia tohto režimu. Nastavte obdobie, počas ktorého bude zapnutý učiaci sa režim (maximálne 14 dní). Po uplynutí nastaveného časového obdobia budete vyzvaný na úpravu pravidiel, ktoré boli vytvorené počas učiaceho sa režimu. Môžete tiež zvoliť iný režim filtrovania alebo oddialiť svoje rozhodnutie a používať učiaci sa režim aj naďalej.

Režim, ktorý sa nastaví po skončení učiaceho sa režimu – vyberte režim filtrovania, ktorý bude aktivovaný po ukončení učiaceho sa režimu. Možnosť **Spýtať sa používateľa** vyžaduje oprávnenia správcu, ak chcete vykonávať zmeny režimu filtrovania HIPS.

Systém HIPS monitoruje udalosti vnútri operačného systému a reaguje na ne podľa pravidiel, ktoré sú štruktúrou podobné pravidlám firewallu. Kliknutím na **Upraviť** vedľa položky **Pravidlá** otvoríte editor **pravidiel HIPS**. V tomto okne môžete označiť, pridať, upraviť alebo odstrániť pravidlá. Viac informácií o vytváraní pravidiel a operáciách HIPS nájdete v kapitole Úprava pravidla HIPS.

HIPS vylúčenia

Tieto vylúčenia vám umožňujú vyňať konkrétne procesy z hĺbkovej behaviorálnej kontroly v rámci systému HIPS.

Ak chcete upraviť vylúčenia HIPS, otvorte Rozšírené nastavenia > **Detekčné jadro** > **HIPS** > **Host Intrusion Prevention System** > **Vylúčenia** > **Upraviť**.

> Tento typ vylúčení si nezamieňajte s príponami súborov vylúčených z kontroly, vylúčeniami detekcií, výkonnostnými vylúčeniami a vylúčeniami procesov.

Na vylúčenie objektu kliknite na **Pridať** a zadajte cestu k objektu, prípadne ho vyberte v stromovej štruktúre. Môžete tiež Upraviť alebo Odstrániť vybrané položky.

Rozšírené nastavenia HIPS

Nasledujúce možnosti sú užitočné pre ladenie (debugovanie) a analýzu správania aplikácií:

Ovládače s povolením vždy sa načítať – zobrazené ovládače majú vždy povolené načítanie bez ohľadu na zvolený režim filtrovania, pokiaľ nie sú blokované špecifickým používateľským pravidlom.

Zapisovať všetky zablokované operácie do protokolu – všetky zablokované operácie sa zapíšu do protokolu HIPS. Vzhľadom na značnú veľkosť protokolu a spomalenie počítača pri jeho vytváraní použite túto možnosť, len ak vás na to vyzval pracovník technickej podpory spoločnosti ESET.

Upozorňovať na zmeny v zozname aplikácií automaticky spúšťaných pri štarte – ak pribudne alebo ubudne aplikácia zo zoznamu aplikácií spúšťaných pri štarte, zobrazí sa upozornenie.

Ovládače s povolením vždy sa načítať

Ovládače v tomto zozname majú vždy povolené načítanie bez ohľadu na zvolený HIPS režim filtrovania, pokiaľ nie sú blokované špecifickým používateľským pravidlom.

Pridať – pridať nový ovládač.

Upraviť – upraviť zvolený ovládač.

Odstrániť – odstrániť ovládač zo zoznamu.

Obnoviť – načítať len zoznam systémových ovládačov.

> Kliknite na **Obnoviť** pre odstránenie ovládačov pridaných používateľom. Táto možnosť je užitočná, ak ste pridali väčší počet ovládačov a neviete ich odstrániť zo zoznamu manuálne.

> Po inštalácii je zoznam ovládačov prázdny. ESET Internet Security ho časom automaticky doplní.

Interaktívne okno HIPS

Notifikačné okno HIPS vám umožňuje vytvoriť pravidlo na základe nových akcií, ktoré HIPS deteguje, a definovať podmienky, za ktorých bude konkrétna akcia povolená alebo zakázaná.

Pravidlá vytvorené pomocou notifikačného okna sú rovnocenné pravidlám vytvoreným manuálne. Pravidlo vytvorené z notifikačného okna môže byť menej špecifické ako pravidlo, ktoré vyvolalo dané dialógové okno. To znamená, že po vytvorení pravidla v dialógovom okne môže rovnaká operácia vyvolávať rovnaké okno. Viac informácií nájdete v kapitole Manažment pravidiel HIPS.

Ak je akcia v pravidle nastavená na **Vždy sa opýtať**, po spustení pravidla sa zobrazí dialógové okno s výberom možností. Operáciu môžete buď **Zakázať**, alebo **Povoliť**. Ak používateľ nezvolí odpoveď vo vyhradenom čase, vyberie sa na základe pravidiel nová akcia.

Možnosť **Zapamätať si do ukončenia aplikácie** spôsobí, že zvolená akcia (**Povoliť/Zakázať**) bude platná a používaná len do najbližšej zmeny pravidiel, režimu filtrovania, aktualizácie HIPS modulu alebo reštartu systému. Po vykonaní ktorejkoľvek z týchto akcií budú dočasné pravidlá zmazané.

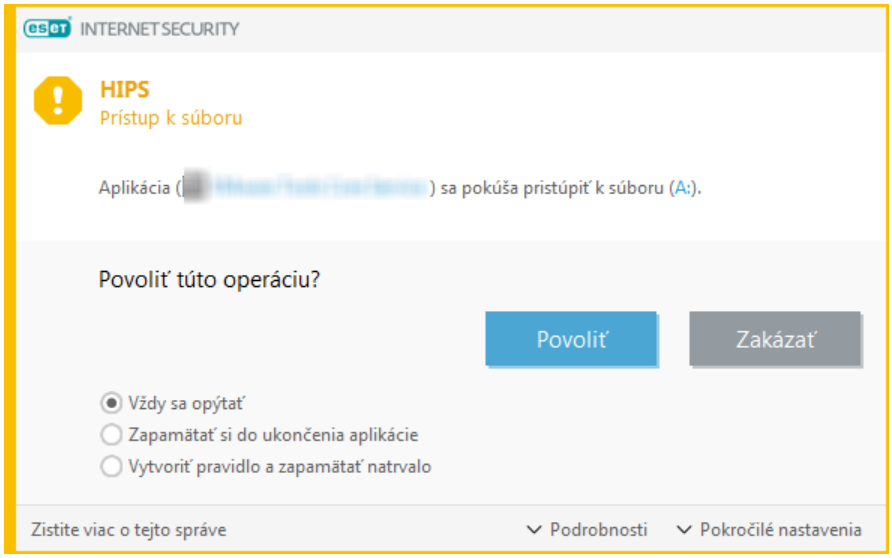
Možnosť **Vytvoriť pravidlo a zapamätať natrvalo** vytvorí nové pravidlo HIPS, ktoré môže byť neskôr zmenené v sekcii Manažment pravidiel HIPS (toto si vyžaduje oprávnenia správcu).

Kliknutím na **Podrobnosti** v dolnej časti zistíte, ktorá aplikácia spúšťa operáciu, aká je reputácia súboru, prípadne aký typ operácie sa chystáte povoliť alebo zakázať.

Nastavenia podrobnejších parametrov pravidla sú dostupné po kliknutí na **Pokročilé možnosti**. Ak vyberiete možnosť **Vytvoriť pravidlo a zapamätať natrvalo**, budú dostupné nasledujúce nastavenia:

- **Pravidlo sa bude týkať len tejto aplikácie** – ak zrušíte označenie tejto možnosti, pravidlo sa vytvorí pre všetky zdrojové aplikácie.
- **Len pre operáciu** – vyberte operáciu pre súbor/aplikáciu/register. Popis všetkých operácií HIPS nájdete tu.
- **Len pre cieľ** – vyberte, či bude pravidlo uplatnené pre súbor/aplikáciu/register.

> **Zobrazuje sa vám príliš veľa HIPS oznámení?**
> Ak chcete zastaviť zobrazovanie oznámení, zmeňte režim filtrovania na **Automatický** v časti Rozšírené nastavenia > **Detekčné jadro** > **HIPS** > **Host Intrusion Prevention System**.



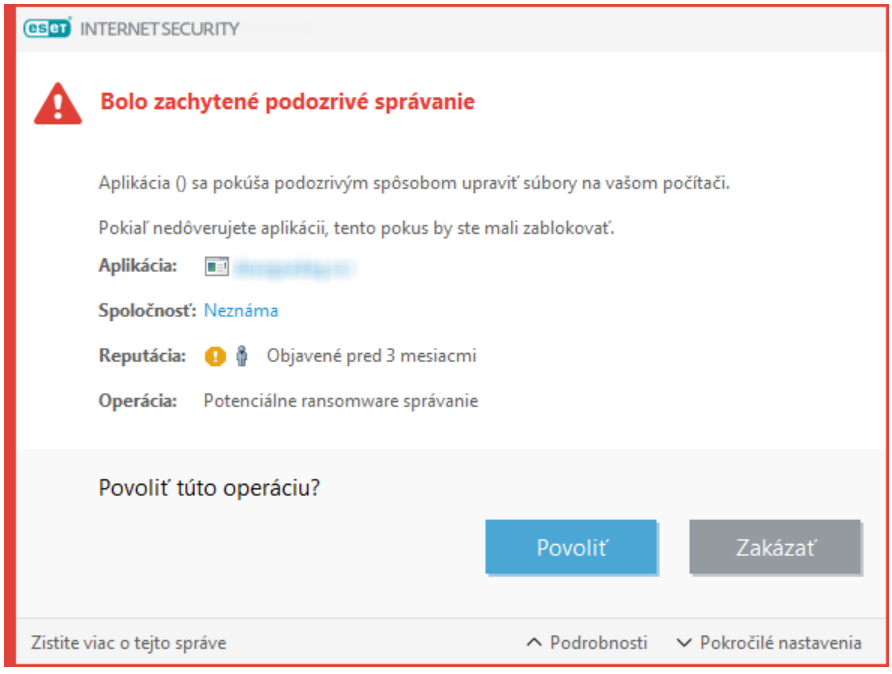
Učiaci sa režim skončil

Učiaci sa režim automaticky vytvára a ukladá pravidlá. Všetky vytvorené pravidlá môžete skontrolovať v nastaveniach pravidiel HIPS. Tento režim je vhodný na prvotné nastavenie systému HIPS, ale nemal by zostať zapnutý na dlhší čas. Vytvorenie pravidiel prebehne bez interakcie s používateľom, keďže ESET Internet Security ukladá pravidlá na základe prednastavených parametrov. Po vytvorení všetkých pravidiel pre požadované procesy spustené v operačnom systéme prepnite Učiaci sa režim na **Interaktívny režim** alebo **Režim politík**, aby ste predišli možným bezpečnostným rizikám.

Ak nechcete zmeniť nastavenia, môžete toto rozhodnutie odložiť.

Bola zachytená potenciálna aktivita ransomvéru

Toto interaktívne okno sa zobrazí v prípade, že bola zachytená potenciálna aktivita ransomvéru. Operáciu môžete buď **Zakázať**, alebo **Povoliť**.



Kliknutím na **Podrobnosti** zobrazíte konkrétne parametre detekcie. Pomocou dialógového okna môžete súbor **odoslať na analýzu** alebo ho **vylúčiť z detekcie**.

Aby mohla ochrana pred ransomvérom správne fungovať, musí byť aktivovaná služba ESET LiveGrid®.

Manažment pravidiel HIPS

Toto je zoznam používateľských a automaticky vytvorených pravidiel systému HIPS. Viac informácií o vytváraní pravidiel a operáciách HIPS nájdete v kapitole Nastavenie pravidiel HIPS. Prečítajte si tiež kapitolu HIPS (Host-based Intrusion Prevention System).

Stĺpce

Pravidlo – používateľom definovaný alebo automaticky zvolený názov pravidla.

Zapnuté – deaktivujte túto možnosť, ak pravidlo nechcete používať, no želáte si ho ponechať v zozname.

Akcia – bližšie špecifikuje akciu (**Povoliť**, **Blokovať** alebo **Spýtať sa**), ktorá sa vykoná, ak budú splnené podmienky pravidla.

Zdroje – pravidlo sa použije iba v prípade, ak bude udalosť spustená aplikáciou.

Ciele – pravidlo sa použije iba v prípade, ak je operácia spojená s konkrétnym súborom, aplikáciou alebo položkou databázy Registry.

Závažnosť zapisovania do protokolu – ak aktivujete túto možnosť, budú informácie o danom pravidle zapisované do protokolu HIPS.

Oznámiť – v prípade, že dôjde k zodpovedajúcej udalosti, sa v pravom dolnom rohu automaticky zobrazí malé okno s oznámením.

Ovládacie prvky

Pridať – pridanie nového pravidla.

Upraviť – úprava zvolených položiek.

Odstrániť – odstránenie zvolených položiek.

Priorita pravidiel HIPS

Nie je možné nastaviť či meniť prioritu HIPS pravidiel pomocou šípok alebo tlačidiel pre zmenu poradia nahor/nadol (ako napr. v prípade pravidiel firewallu, ktoré sú spúšťané smerom zhora nadol).

- Všetky pravidlá, ktoré vytvoríte, majú rovnakú prioritu.
- Čím je pravidlo konkrétnejšie, tým vyššia je jeho priorita (napr. pravidlo pre konkrétnu aplikáciu má vyššiu prioritu ako pravidlo pre všetky aplikácie).
- Interne HIPS obsahuje pravidlá s vyššou prioritou, ku ktorým však nemáte prístup (napr. nie je možné

prepísať definované pravidlá Self-Defense).

• Ak vytvoríte pravidlo, ktoré môže spôsobiť zamŕzanie vášho operačného systému, takéto pravidlo sa nebude aplikovať (bude mať najnižšiu prioritu).

Úprava pravidla HIPS

Skôr ako začnete nastavovať pravidlá HIPS, prečítajte si kapitolu Manažment pravidiel HIPS.

Názov pravidla – názov zadaný používateľom alebo automaticky zvolený názov pravidla.

Akcia – špecifikuje akciu (**Povoliť**, **Blokovať** alebo **Spýtať sa**), ktorá sa vykoná, ak budú splnené podmienky pravidla.

Ovplyvnené operácie – vyberte typ operácií, pre ktoré bude pravidlo aplikované. Pravidlo sa uplatní len pre tento typ operácie a pre zvolený cieľ.

Zapnuté – deaktivujte túto možnosť, ak pravidlo nechcete používať, no želáte si ho ponechať v zozname.

Závažnosť zapisovania do protokolu – ak aktivujete túto možnosť, budú informácie o danom pravidle zapisované do protokolu HIPS.

Upozorniť používateľa – v prípade, že dôjde k zodpovedajúcej udalosti, sa v pravom dolnom rohu automaticky zobrazí malé okno s oznámením.

Pravidlo pozostáva z častí, ktoré popisujú podmienky, za ktorých sa pravidlo spustí:

Zdrojové aplikácie – pravidlo sa uplatní, len ak udalosť vyvolajú dané aplikácie. Ak chcete vybrať určité aplikácie, z roletového menu zvoľte **Konkrétne aplikácie** a kliknite na **Pridať**. Ak chcete pridať všetky aplikácie, z roletového menu vyberte **Všetky aplikácie**.

Cieľové súbory – pravidlo sa uplatní len v prípade, že sa operácia týka vybraného cieľa. Ak chcete vybrať určité súbory alebo priečinky, z roletového menu zvoľte **Konkrétne súbory** a kliknite na **Pridať**. Ak chcete pridať všetky súbory, z roletového menu vyberte **Všetky súbory**.

Aplikácie – pravidlo sa uplatní len v prípade, že sa operácia týka tohto cieľa. Ak chcete pridať nové súbory alebo priečinky, z roletového menu vyberte **Konkrétne aplikácie** a kliknite na **Pridať**. Ak chcete pridať všetky aplikácie, z roletového menu vyberte **Všetky aplikácie**.

Položky databázy Registry – pravidlo sa uplatní len v prípade, že sa operácia týka tohto cieľa. Ak chcete položky zadať manuálne, z roletového menu vyberte **Konkrétne položky** a kliknite na **Pridať** alebo kliknite na **Otvoriť Editor databázy Registry** a vyberte položky z registrov. V roletovom menu môžete tiež zvoliť možnosť **Všetky položky** a pridať všetky aplikácie.

> Niektoré operácie špecifických pravidiel prednastavených modulom HIPS nemôžu byť zablokované a sú na základe predvolených nastavení povolené. Rovnako platí, že HIPS nemonitoruje všetky systémové operácie. HIPS monitoruje tie operácie, ktoré môžu byť nebezpečné.

Popis dôležitých operácií:

Súborové operácie

- **Vymazať súbor** – aplikácia žiada o povolenie zmazať cieľový súbor.

- **Zapísať do súboru** – aplikácia žiada o povolenie zapisovať do cieľového súboru.

- **Priamy prístup na disk** – aplikácia sa snaží čítať z disku alebo naň zapisovať neštandardným spôsobom, ktorý obchádza bežné procesy Windows. Výsledkom môže byť zmena súboru bez aplikácie príslušného pravidla. Táto operácia môže byť spôsobená škodlivým kódom, ktorý sa snaží vyhnúť detekcii, zálohovacím programom, ktorý kopíruje celý obsah pevného disku, alebo správcom partícií, ktorý reorganizuje diskové zväzky.

- **Nainštalovať globálny hook** – volanie funkcie SetWindowsHookEx z MSDN knižnice pomocou danej aplikácie.

- **Načítať ovládač** – inštalácia a načítanie ovládača do systému.

Aplikačné operácie

- **Ladiť inú aplikáciu** – pripojí ladiaci nástroj (debugger) k procesu. Pri ladení aplikácie sa dá pozorovať alebo meniť jej správanie. Tiež je možné pristupovať k jej dátam.

- **Zachytávať udalosti inej aplikácie** – zdrojová aplikácia sa pokúša zachytiť udalosti cieľovej aplikácie (napríklad, ak sa keylogger snaží zachytiť aktivitu webového prehliadača).

- **Ukončiť/pozastaviť inú aplikáciu** – pozastavenie, obnovenie alebo ukončenie procesu (môže byť vyvolané priamo cez Process Explorer alebo zo záložky Procesy).

- **Spustiť novú aplikáciu** – spustenie novej aplikácie alebo procesu.

- **Zmeniť stav inej aplikácie** – zdrojová aplikácia sa pokúša zapisovať do pamäte cieľovej aplikácie, prípadne sa snaží spustiť kód v jej mene. Táto funkcionalita je užitočná na ochranu dôležitej aplikácie, ak ju nastavíte ako cieľovú aplikáciu pri pravidle, ktoré blokuje tieto operácie.

Operácie s databázou Registry

- **Zmena nastavení spustenia** – všetky zmeny v nastaveniach definujúcich, ktoré aplikácie budú spúšťané pri štarte operačného systému Windows. Tieto možno vyhľadať napríklad zadaním kľúča Run do vyhľadávania v databáze Registry systému Windows.

- **Vymazanie z databázy Registry** – zmazanie kľúča alebo hodnoty v danom kľúči.

- **Premenovanie kľúča databázy Registry** – premenovanie konkrétneho kľúča.

- **Úprava v databáze Registry** – vytváranie nových hodnôt kľúčov alebo zmena dát asociovaných s hodnotou, zmena umiestnenia dát v rámci stromu databázy a nastavovanie používateľských alebo skupinových práv daného kľúča.

Pri zadávaní cieľa je možné s istými obmedzeniami používať zástupné znaky. Namiesto konkrétneho kľúča môžete v ceste k databáze Registry použiť zástupný znak *. Napríklad *HKEY_USERS*\software* môže znamenať *HKEY_USER\.default\software*, ale nie *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** je nesprávne uvedená cesta. Registrový cieľ ukončený * má špeciálny význam, znamená „tento kľúč alebo ľubovoľný podkľúč ľubovoľne hlboko“. Pri súborových cieľoch sa dá používať hviezdička len týmto druhým spôsobom. Platí, že najskôr sa vyhodnocuje špecifická časť cesty a potom cesta po zástupnom znaku (*).

Ak vytvoríte príliš všeobecné pravidlo, zobrazí sa príslušné upozornenie.

V nasledujúcom príklade si ukážeme, ako obmedziť neželané správanie konkrétnej aplikácie:

1. Zadajte názov pravidla a vyberte možnosť **Blokovať** (alebo **Spýtať sa**, ak si želáte vybrať akciu neskôr) z roletového menu **Akcia**.

2. Prepínacím tlačidlom vedľa možnosti **Upozorniť používateľa** aktivujte zobrazenie upozornenia v prípade, že sa pravidlo použije.

3. Vyberte aspoň jednu operáciu v sekcii **Ovplyvnené operácie**, pre ktorú bude pravidlo aplikované.

4. Kliknite na tlačidlo **Ďalej**.

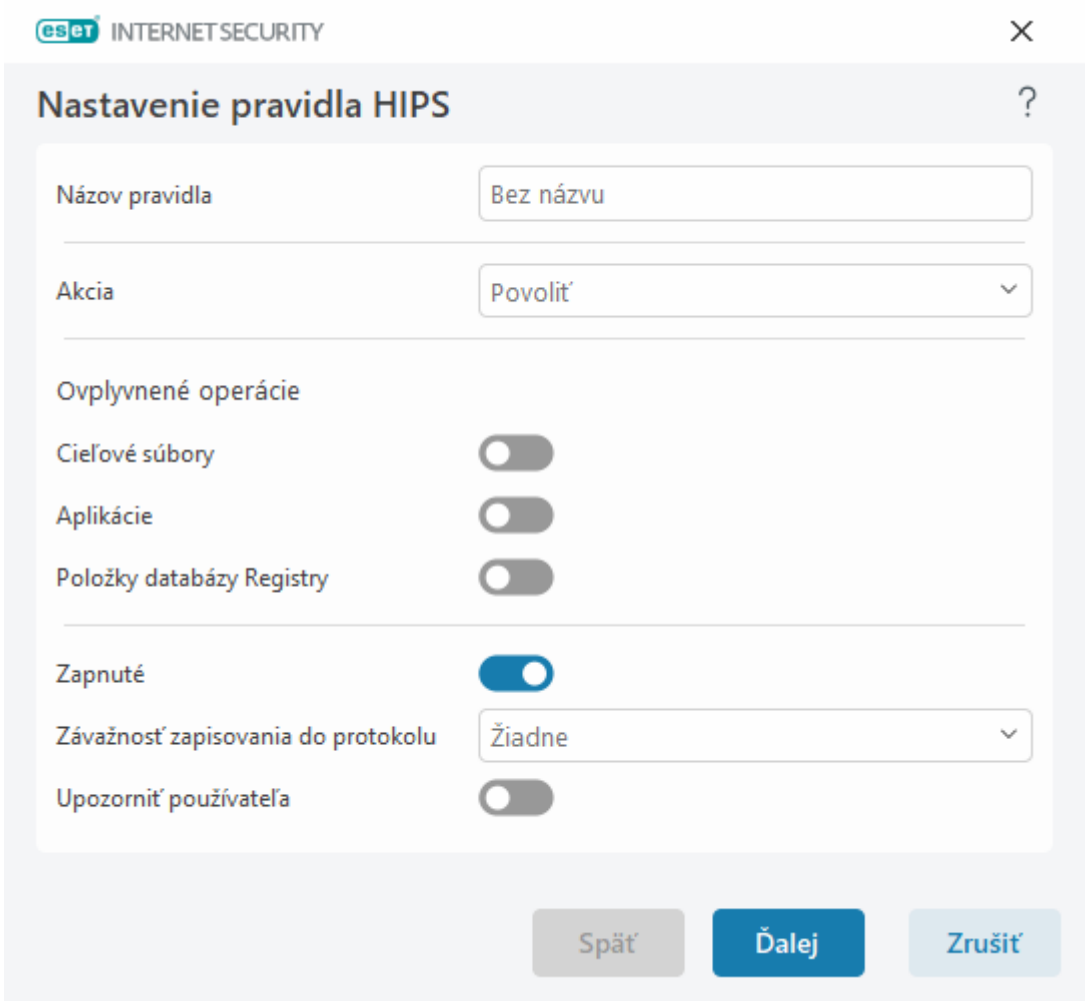
5. V okne **Zdrojové aplikácie** vyberte z roletového menu možnosť **Všetky aplikácie**, aby sa nové pravidlo uplatnilo pre všetky aplikácie, ktoré sa pokúšajú vykonať jednu zo zvolených operácií na vami vybraných aplikáciách.

6. Kliknite na **Pridať**, pomocou **...** následne vyberte cestu ku konkrétnej aplikácii a kliknite na **OK**. V prípade potreby pridajte ďalšie aplikácie.
Napríklad: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Vyberte operáciu **Zapísať do súboru**.

8. Z roletového menu vyberte možnosť **Všetky súbory**. Týmto sa zablokujú akékoľvek pokusy o zápis do súborov aplikáciou zvolenou v predchádzajúcom kroku.

9. Kliknite na **Dokončiť** pre uloženie pravidla.



Pridať cestu k aplikácii/položke v registri pre HIPS

Ikona **...** umožňuje vybrať cestu k súboru aplikácie. Ak vyberiete priečinok, všetky aplikácie v tomto priečinku budú zahrnuté do daného pravidla.

Možnosť **Otvoriť Editor databázy Registry** spustí Windows Registry Editor (regedit). Pri pridávaní cesty k položke v databáze Registry zadajte správne umiestnenie do poľa **Hodnota**.

Príklad cesty k súboru alebo položke v databáze Registry:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Aktualizácia

Možnosti nastavenia aktualizácie sú dostupné cez Rozšírené nastavenia > **Aktualizácia**. Nastavenie aktualizácie pozostáva zo špecifikácie zdroja aktualizácie, teda z nastavenia aktualizačných serverov a autentifikácie voči týmto serverom.

Aktualizácia

Aktualizačný profil, ktorý je momentálne aktívny, je zobrazený v roletovom menu **Vybrať predvolený aktualizačný profil**.

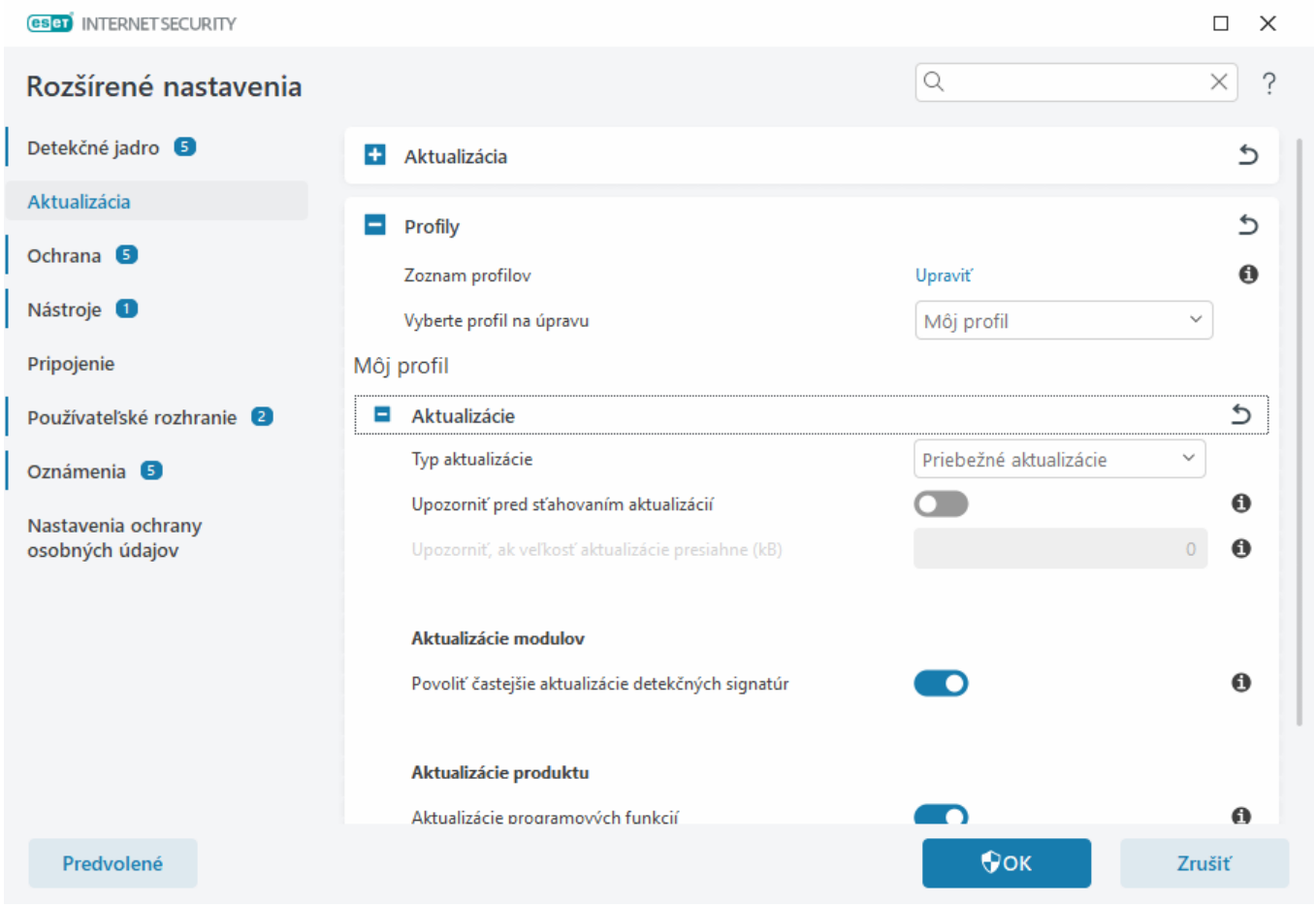
Na vytvorenie nového profilu prejdite do sekcie Aktualizačné profily.

Automatické prepínanie profilu – umožňuje priradiť aktualizačný profil konkrétnemu profilu sieťového pripojenia.

Ak sa vyskytnú problémy so sťahovaním detekčného jadra alebo aktualizácií modulov, kliknite na **Vyčistiť** vedľa možnosti **Vyčistiť aktualizačnú vyrovnávaciu pamäť** na vymazanie dočasných aktualizačných súborov/vyčistenie vyrovnávacej pamäte.

Vrátenie zmien modulov

Ak máte podozrenie, že nová aktualizácia detekčného jadra alebo programových modulov môže byť nestabilná alebo poškodená, môžete program vrátiť späť do predchádzajúceho stavu a zakázať aktualizácie na určený časový interval.



Pre správne fungovanie aktualizácií je nevyhnutné mať všetky parametre nastavené správne. Ak používate firewall, treba zaistiť, aby mal program ESET povolenú komunikáciu cez internet (napríklad HTTP komunikáciu).

Profily

V prípade potreby si môžete vytvoriť pre každú situáciu samostatný aktualizačný profil s rozdielnou konfiguráciou. Vytvorenie rôznych aktualizačných profilov má význam predovšetkým pre používateľov, ktorí veľa cestujú

a pripájajú sa do rozdielnych sietí.

Roletové menu **Vyberte profil na úpravu** zobrazuje momentálne vybraný profil. Predvolenou možnosťou je **Môj profil**. Vytvoriť nový profil je možné prostredníctvom tlačidla **Upraviť** vedľa položky **Zoznam profilov**. Zadajte **Názov profilu** a kliknite na **Pridať**.

Aktualizácie

Predvolenou možnosťou v roletovom menu **Typ aktualizácie** sú **Priebežné aktualizácie**, ktoré zabezpečujú priebežné sťahovanie aktualizačných súborov zo serverov spoločnosti ESET tak, aby pritom čo najmenej zaťažovali sieť. **Predbežné aktualizácie** sú aktualizácie, ktoré prešli dôkladným interným testovaním a budú čoskoro dostupné širokej verejnosti. Výhodou povolenia predbežných aktualizácií je možnosť prístupu k najnovším metódam detekcie a rôznym opravám. Treba však mať na pamäti, že predbežné aktualizácie nemusia byť vždy dostatočne stabilné a v žiadnom prípade by preto NEMALI byť používané na produkčných serveroch a pracovných staniciach, pri ktorých sa vyžaduje maximálna stabilita a dostupnosť.

Upozorniť pred sťahovaním aktualizácií – v prípade dostupnosti aktualizácie program zobrazí upozornenie, v ktorom môžete stiahnutie aktualizačných súborov potvrdiť alebo zamietnuť.

Upozorniť, ak veľkosť aktualizácie presiahne (kB) – ak veľkosť aktualizačného súboru presiahne zadanú hodnotu, program zobrazí potvrdzovacie dialógové okno. Ak je veľkosť aktualizačného súboru nastavená na 0 kB, program bude dialógové okno zobrazovať vždy.

Aktualizácie modulov

Povoliť častejšie aktualizácie detekčných signatúr – umožňuje kratší časový interval medzi aktualizáciami detekčného jadra. Vypnutie tohto nastavenia môže mať negatívny vplyv na účinnosť detekcie.

Aktualizácie produktu

Aktualizácie programových funkcií – automatické inštalovanie nových verzií produktu ESET Internet Security.

Možnosti pripojenia

Ak chcete na sťahovanie aktualizácií využívať proxy server, prečítajte si kapitolu Možnosti pripojenia.

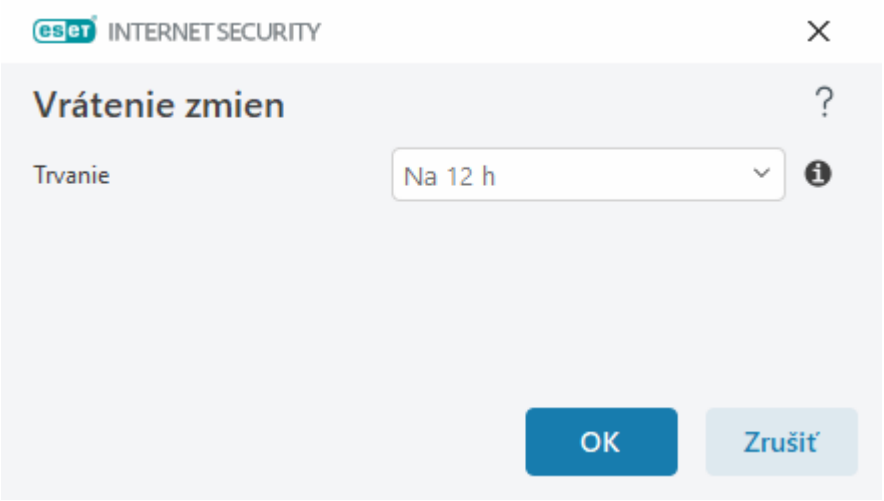
Vrátenie zmien aktualizácií

Ak máte podozrenie, že nová verzia detekčného jadra alebo programových modulov môže byť nestabilná alebo poškodená, môžete sa vrátiť na predchádzajúcu verziu a dočasne pozastaviť pravidelné aktualizácie. V tejto sekcii tiež môžete povoliť pravidelné aktualizácie, ktoré ste predtým odložili na neurčito.

ESET Internet Security vytvára záložné snímky programových modulov a detekčného jadra, ktoré môžu byť následne použité pri vrátení zmien na predchádzajúcu verziu (tzv. rollback). Pre vytváranie záložných snímok ponechajte možnosť **Vytvárať snímky modulov** označenú. Keď je vytváranie snímok modulov aktívne, prvá snímka sa vytvorí počas prvej aktualizácie. Ďalšia sa vytvorí po 48 hodinách. Pole **Počet záložných snímok** určuje počet snímok predošlých verzií modulov a detekčného jadra uložených na lokálnom disku počítača.

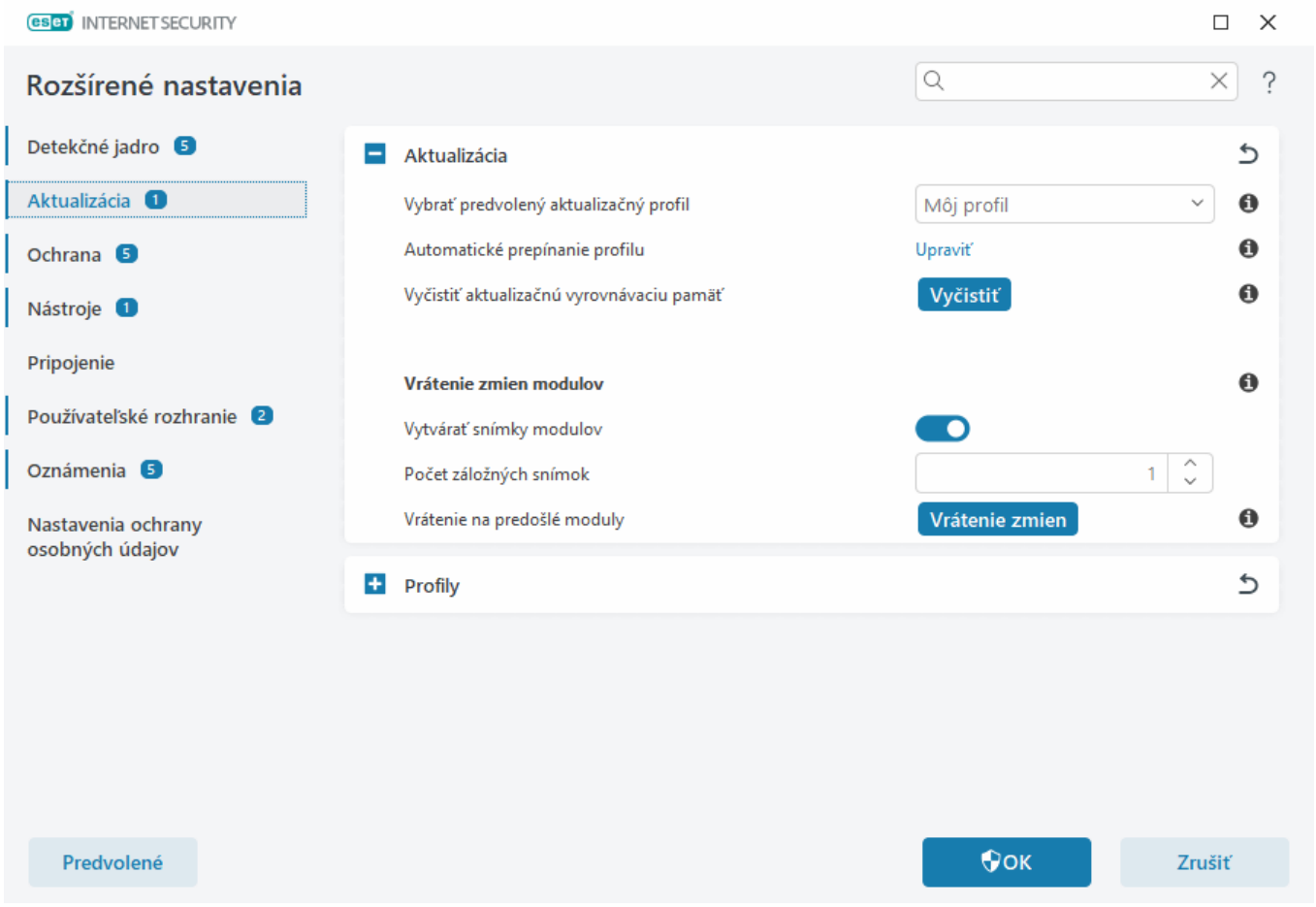
Po dosiahnutí maximálneho počtu vytvorených záložných snímok (napr. troch) dôjde každých 48 hodín k nahradeniu najstaršej záložnej snímky novou. ESET Internet Security pri vrátení zmien vždy vráti späť najstaršiu záložnú snímku aktualizácie programových modulov a detekčného jadra.

Ak kliknete na možnosť **Vrátenie zmien** v sekcii Rozšírené nastavenia > **Aktualizácia** > **Aktualizácia**, je potrebné vybrať časový interval z roletového menu **Trvanie**, ktorý predstavuje časové obdobie, počas ktorého budú pravidelné aktualizácie programových modulov a detekčného jadra pozastavené.



Ak si želáte pravidelné aktualizácie odložiť na neurčito, až pokým ich neskôr manuálne nepovolíte, vyberte možnosť **Do zrušenia**. ESET neodporúča výber tejto možnosti, pretože predstavuje potenciálne bezpečnostné riziko.

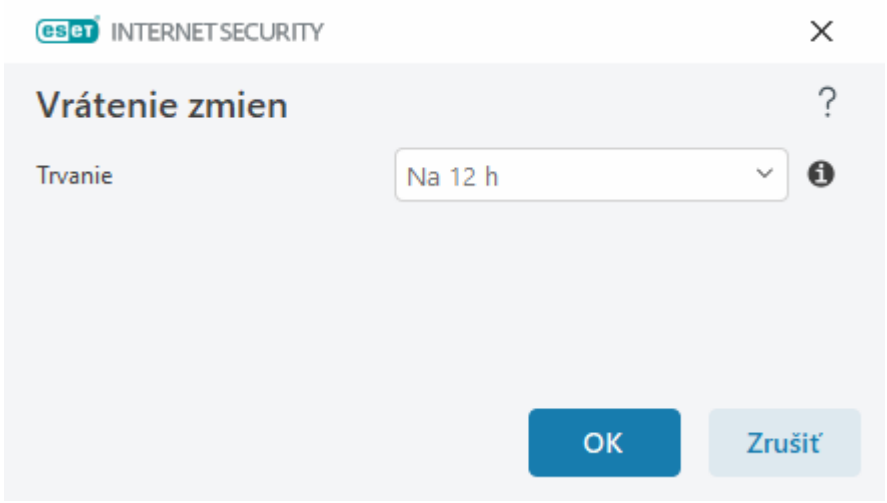
Po vykonaní vrátenia zmien sa tlačidlo **Vrátenie zmien** zmení na tlačidlo s názvom **Povoliť aktualizácie**. Bez manuálneho povolenia aktualizácií sa počas vami stanoveného časového intervalu nebudú sťahovať ani inštalovať žiadne aktualizácie. Detekčné jadro sa vráti späť na verziu, ktorá je uložená na disku počítača ako záložná snímka a je najstaršia.



Uveďme si príklad, v ktorom najaktuálnejšia verzia detekčného jadra má číslo 22700. Na pevnom disku počítača sú uložené snímky verzií 22698 a 22696. Všimnite si, že 22697 nie je k dispozícii, pretože počítač bol napríklad istú dobu vypnutý a počas tohto obdobia vznikla už novšia aktualizácia, ktorá bola stiahnutá. Ak bolo v poli **Počet záložných snímok** nastavené číslo 2, po kliknutí na tlačidlo **Vrátenie zmien** sa detekčné jadro (vrátane programových modulov) obnoví na verziu s číslom 22696. Tento proces môže chvíľu trvať. Vrátenie detekčného jadra na staršiu verziu sa dá overiť v hlavnom okne programu v časti Aktualizácia.

Vrátenie zmien – časový interval pozastavenia aktualizácií

Ak kliknete na možnosť **Vrátenie zmien** v sekcii Rozšírené nastavenia > **Aktualizácia** > **Aktualizácia**, je potrebné vybrať časový interval z roletového menu **Trvanie**, ktorý predstavuje časové obdobie, počas ktorého budú pravidelné aktualizácie programových modulov a detekčného jadra pozastavené.



Ak si želáte pravidelné aktualizácie odložiť na neurčito, až pokým ich neskôr manuálne nepovolíte, vyberte možnosť **Do zrušenia**. ESET neodporúča výber tejto možnosti, pretože predstavuje potenciálne bezpečnostné riziko.

Aktualizácie produktu

Sekcia **Aktualizácie produktu** umožňuje inštalovať nové aktualizácie funkcií.

Aktualizácie funkcií prinášajú do programu nové alebo upravujú už existujúce funkcie z predchádzajúcich verzií. Môžu prebiehať automaticky bez zásahu používateľa alebo s informovaním a výzvou na ich potvrdenie od používateľa. Po nainštalovaní aktualizácie programových funkcií môže byť potrebný reštart počítača.

Aktualizácie programových funkcií – ak je toto nastavenie zapnuté, aktualizácie funkcií budú prebiehať automaticky.

Možnosti pripojenia

Ak chcete získať prístup k možnostiam nastavenia proxy servera pre konkrétny aktualizačný profil, otvorte Rozšírené nastavenia > **Aktualizácia** > **Profily** > **Aktualizácie** > **Možnosti pripojenia**. Kliknite na roletové menu vedľa popisu **Režim proxy** a označte jednu z nasledujúcich možností:

- Nepoužívať proxy server
- Pripojenie prostredníctvom proxy servera
- Použiť globálne nastavenie proxy servera

Po označení možnosti **Použiť globálne nastavenie proxy servera** bude použitá konfigurácia proxy servera špecifikovaná v sekcii Rozšírené nastavenia > **Pripojenie** > **Proxy server**.

Po označení možnosti **Nepoužívať proxy server** používateľ explicitne definuje, že pri aktualizácii ESET Internet Security nemá byť použitý žiadny proxy server.

Možnosť **Pripojenie prostredníctvom proxy servera** označte v týchto prípadoch:

- Na aktualizáciu produktu ESET Internet Security sa používa iný proxy server ako ten, ktorý je zadefinovaný

v sekcii Rozšírené nastavenia > **Pripojenie**. Pri tejto konfigurácii by mali byť údaje nového proxy servera špecifikované v príslušných poliach. Je potrebné zadať adresu **Proxy servera**, komunikačný **Port** (predvolene 3128), prípadne tiež **Prihlasovacie meno** a **Heslo**.

- Proxy server používaný pri aktualizácii ESET Internet Security je iný ako globálne nastavený proxy server.

- Váš počítač je pripojený na internet cez proxy server. Nastavenia sú prevzaté z prehliadača Internet Explorer počas inštalácie programu, no ak dôjde po čase k zmene v nastaveniach proxy servera (napríklad v dôsledku zmeny sprostredkovateľa internetového pripojenia – ISP), bude potrebné skontrolovať nastavenia proxy v tejto sekcii. V opačnom prípade nebude automaticky prebiehať sťahovanie aktualizácií z aktualizačných serverov.

Pri štandardnej inštalácii je prednastavená možnosť **Použiť globálne nastavenie proxy servera**.

Použiť priame pripojenie, ak proxy nie je k dispozícii – ak bude proxy nedostupné, bezpečnostný produkt ESET sa automaticky pokúsi pripojiť k aktualizačným serverom bez použitia proxy.

Polia **Prihlasovacie meno** a **Heslo** sú v tejto sekcii špecifické pre proxy server. Vyplňte ich len v tom prípade, že pre prístup na proxy server sa vyžaduje zadanie prihlasovacieho mena a hesla. Tieto údaje preto nevypĺňajte, ak na prístup k internetu cez proxy server nie je potrebné heslo.

Ochrana

Vrstvy ochrany zabezpečujú kontrolu súborov, e-mailov a internetovej komunikácie a chránia tak systém pred nebezpečnými útokmi. Ak napríklad dôjde k zachyteniu objektu, ktorý je klasifikovaný ako malvér, začne sa proces nápravy. Detegovaný objekt sa eliminuje zablokovaním a následným vyliečením, odstránením alebo presunutím do karantény.

Podrobné možnosti sú k dispozícii v sekcii Rozšírené nastavenia > **Ochrana**.

Zmeny v nastaveniach ochrany odporúčame robiť len skúseným používateľom. Nesprávne nastavenia môžu znížiť úroveň ochrany.

V tejto kapitole nájdete nasledujúce témy:

- Reakcie na detekciu
- Nastavenie hlásení
- Nastavenie ochrany

Reakcie na detekciu

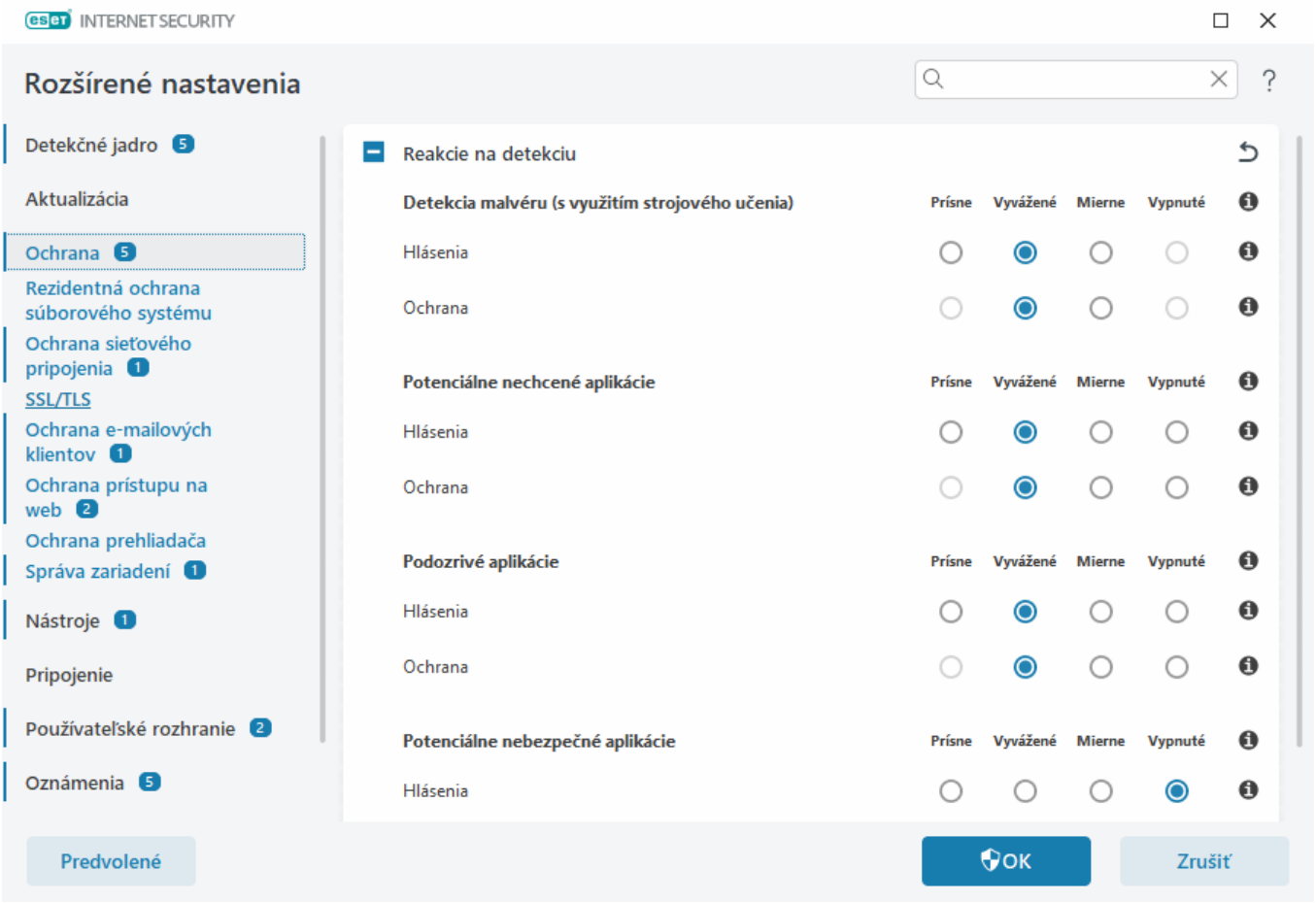
Reakcie na detekciu umožňujú konfigurovať úrovne hlásení a ochrany pre nasledujúce kategórie:

- **Detekcia malvéru (s využitím strojového učenia)** – počítačový vírus je škodlivý kód pripojený k existujúcim súborom na počítači. Termín „vírus“ sa však často používa nesprávne. Presnejším výrazom je „malvér“ (škodlivý softvér). Detekciu malvéru zabezpečuje modul detekčného jadra v kombinácii s komponentom strojového učenia. Prečítajte si viac o týchto typoch aplikácií v slovníku pojmov.

- **Potenciálne nechcené aplikácie** – grayware alebo tiež potenciálne nechcená aplikácia (PUA) je označenie pre širokú škálu softvéru, ktorý nie je jednoznačne škodlivý ako iné druhy malvéru, napríklad vírusy alebo trójske kone. Môže však na váš počítač nainštalovať ďalší nežiaduci softvér, zmeniť správanie zariadenia, vykonávať neočakávané operácie, prípadne akcie bez súhlasu používateľa. Prečítajte si viac o týchto typoch aplikácií v slovníku pojmov.

- **Podozrivé aplikácie** – predstavujú programy komprimované packermi alebo protektormi. Autori malvéru tieto typy nástrojov často zneužívajú na zmarenie detekcie.

- **Potenciálne nebezpečné aplikácie** – predstavujú v prevažnej miere komerčný a legitímny softvér, avšak v nesprávnych rukách môže dôjsť k jeho zneužitiu na nekalé účely. Medzi potenciálne nebezpečné aplikácie môžeme zaradiť nástroje vzdialeného prístupu, nástroje na prelomenie hesiel a keyloggery (programy zapisujúce každé stlačenie klávesu používateľom). Prečítajte si viac o týchto typoch aplikácií v slovníku pojmov.



Vylepšená ochrana

Pokročilé strojové učenie je teraz súčasťou ochrany, pričom funguje ako pokročilá vrstva vylepšujúca detekciu na základe strojového učenia. Viac o tomto type ochrany sa dočítate v slovníku pojmov.

Nastavenie hlásení

Ak dôjde k detekcii (napr. sa nájde hrozba, ktorá je klasifikovaná ako malvér), informácie sa zaznamenajú do protokolu Detekcie a zobrazia sa Oznámenia na ploche v prípade, že sú nakonfigurované v programe ESET Internet Security.

Úroveň hlásenia sa nastavuje zvlášť pre každú kategóriu (ďalej len „KATEGÓRIA“):

1.Detekcie malvéru

2.Potenciálne nechcené aplikácie

3.Potenciálne nebezpečné aplikácie

4.Podozrivé aplikácie

Pri hláseniach detegovaných objektov sa využíva detekčné jadro vrátane komponentu strojového učenia. V prípade hlásení pritom môžete nastaviť vyššiu úroveň (prah) než pri ochrane. Tieto nastavenia hlásení neovplyvnia blokovanie, liečenie ani odstraňovanie objektov.

Pred zmenou prahu (úrovne) hlásenia pre jednotlivé KATEGÓRIE si prečítajte nasledujúce informácie:

Úroveň nastavenia (zvolený prah)	Vysvetlenie
Prísne	Hlásenia danej KATEGÓRIE sú nakonfigurované na maximálnu citlivosť. Je preto hlásený väčší počet detekcií. **Prísne** nastavenie môže objekty nesprávne identifikovať ako objekt danej KATEGÓRIE.
Vyvážené	Hlásenia danej KATEGÓRIE sú nakonfigurované ako vyvážené. Toto nastavenie je optimalizované pre dosiahnutie vyváženého pomeru medzi výkonom a presnosťou detekcie a počtom nesprávne identifikovaných objektov.
Mierne	Hlásenia danej KATEGÓRIE sú nakonfigurované tak, aby sa minimalizovali nesprávne identifikované objekty pri súčasnom zachovaní dostatočnej úrovne ochrany. Objekty sú hlásené iba v prípade vysokej pravdepodobnosti a zhody so správaním charakteristickým pre danú KATEGÓRIU.
Vypnuté	Hlásenia danej KATEGÓRIE nie sú aktívne a detekcie tohto typu nie sú zachytávané, hlásené ani liečené. Toto nastavenie preto vyvolá vypnutie ochrany pred daným typom detekcie. Úroveň „Vypnuté“ nie je dostupná pre hlásenia malvéru a zároveň je to predvolená hodnota pre kategóriu potenciálne nebezpečných aplikácií.

Dostupnosť modulov ochrany programu ESET Internet Security

Nasledujúca tabuľka zobrazuje dostupnosť (povolené alebo zakázané) daného modulu ochrany pre zvolený prah v rámci KATEGÓRIE:

	Prísne	Vyvážené	Mierne	Vypnuté*
Modul pokročilého strojového učenia	✓ (prísny režim)	✓ (konzervatívny režim)	X	X
Modul detekčného jadra	✔	✔	✔	X
Iné moduly ochrany	✔	✔	✔	X

* Neodporúča sa.

Zistite verziu svojho produktu, verzie programových modulov a dátumy vydania

1. Kliknite na **Pomocník a podpora** > **O ESET Internet Security**.
2. Na obrazovke s názvom **O programe** sa v prvom riadku textu zobrazuje číslo verzie vášho bezpečnostného produktu ESET.
3. Kliknite na tlačidlo **Nainštalované súčasti**, ak si chcete zobraziť informácie o konkrétnych moduloch.

Dôležité poznámky

Pokiaľ ide o nastavenie vhodnej úrovne (prahu) hlásenia a ochrany pre vaše prostredie, tu je ešte niekoľko dôležitých poznámok:

- **Vyvážené** nastavenie sa odporúča pre väčšinu situácií.
- Čím vyšší prah hlásenia zvolíte, tým vyššia bude úspešnosť detekcie, ale zároveň sa zvýši aj možnosť výskytu nesprávne identifikovaných objektov.
- Vzhľadom na dynamiku hrozieb v reálnom prostredí nie je možné zaručiť 100 % úspešnosť detekcie a rovnako ani 0 % možnosť nesprávnych kategorizácií bezpečných objektov ako malvér.
- Udržujte program ESET Internet Security a jeho moduly v aktuálnom stave, aby ste tak dosiahli čo najlepší balans medzi výkonnosťou a presnosťou detekcie a počtom nesprávne identifikovaných objektov.

Nastavenie ochrany

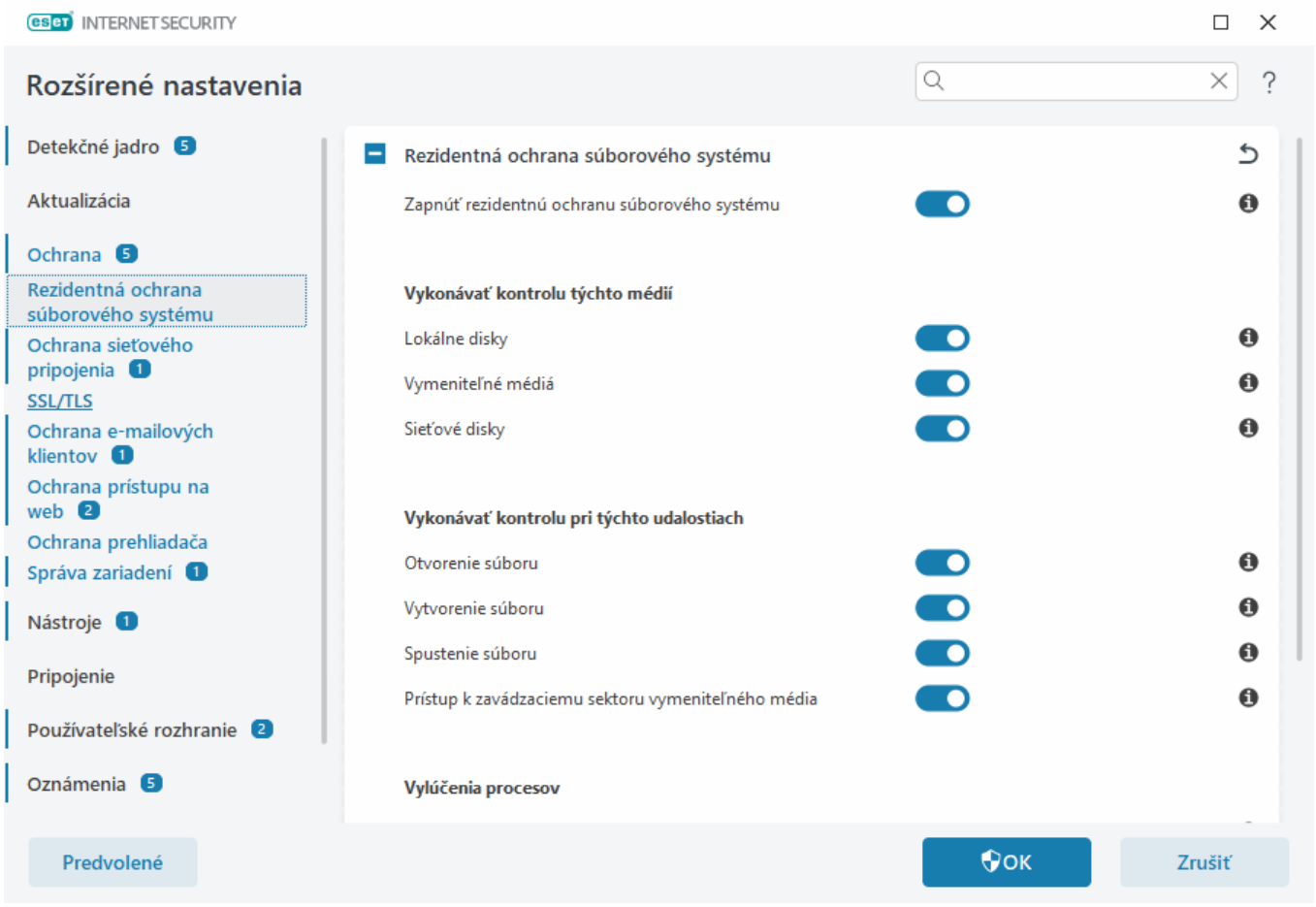
V prípade, že je zachytený objekt klasifikovaný ako KATEGÓRIA, program daný objekt zablokuje a následne ho vylieči, odstráni alebo presunie do karantény.

Pred zmenou prahu (úrovne) ochrany pre jednotlivé KATEGÓRIE si prečítajte nasledujúce informácie:

Úroveň nastavenia (zvolený prah)	Vysvetlenie
Prísne	Detekcie zachytené pri prísnej (alebo nižšej) úrovni nastavenia sú zablokované a automaticky dochádza k procesu nápravy (t. j. k liečeniu). Toto nastavenie sa odporúča, keď všetky koncové zariadenia prešli kontrolou pri prísnej úrovni nastavenia a nesprávne detegované objekty boli pridané do vylúčení detekcií.
Vyvážené	Detekcie zachytené pri vyváženej (alebo nižšej) úrovni nastavenia sú zablokované a automaticky dochádza k procesu nápravy (t. j. k liečeniu).
Mierne	Detekcie zachytené pri miernej úrovni nastavenia sú zablokované a automaticky dochádza k procesu nápravy (t. j. k liečeniu).
Vypnuté	Toto nastavenie je užitočné pre identifikáciu a vylúčenie nesprávne detegovaných objektov. Úroveň „Vypnuté“ nie je dostupná pre ochranu pred malvérom a zároveň je to predvolená hodnota pre kategóriu potenciálne nebezpečných aplikácií.

Rezidentná ochrana súborového systému

Rezidentná ochrana súborového systému kontroluje všetky súbory v systéme na prítomnosť škodlivého kódu pri ich otváraní, vytváraní a spúšťaní.



Na základe predvolených nastavení sa rezidentná ochrana súborového systému spustí pri štarte systému a následne poskytuje nepretržitú kontrolu. Neodporúčame vypínať rezidentnú ochranu zrušením výberu možnosti **Zapnúť rezidentnú ochranu súborového systému** v Rozšírených nastaveniach v sekcii **Ochrana** > **Rezidentná ochrana súborového systému** > **Rezidentná ochrana súborového systému**.

Vykonávať kontrolu týchto médií

Predvolene je nastavená kontrola všetkých typov médií:

- **Lokálne disky** – kontroluje všetky systémové a pevné disky (napr.: *C:*\, *D:*\).
- **Vymeniteľné médiá** – kontroluje CD/DVD, USB úložisko, pamäťové karty atď.
- **Sieťové disky** – kontroluje všetky namapované sieťové disky (napr.: *H:*\ ako *store04*) alebo sieťové disky s priamym prístupom (napr.: *store08*).

Odporúčame používať predvolené nastavenia kontroly všetkých médií a meniť ich iba v špecifických prípadoch, napríklad keď pri kontrole určitého média vzniká výrazné spomalenie prenosu dát.

Vykonávať kontrolu pri týchto udalostiach

Prednastavená je kontrola všetkých súborov pri ich otváraní, vytváraní alebo spúšťaní. Odporúčame vám ponechať tieto predvolené nastavenia bez zmeny, aby bola aj naďalej zabezpečená kontrola všetkého diania v počítači:

- **Otvorenie súboru** – kontroluje súbor pri jeho otvorení.

- **Vytvorenie súboru** – kontroluje novovytvorený alebo upravený súbor.
- **Spustenie súboru** – kontroluje súbor, keď dôjde k jeho spusteniu.
- **Prístup k zavádzaciemu sektoru vymeniteľného média** – ak k zariadeniu pripojíte vymeniteľné médium, ktoré obsahuje zavádzací sektor, prebehne okamžitá kontrola tohto zavádzacieho sektora. Táto možnosť neslúži na povolenie kontroly súborov uložených na vymeniteľných médiách. Nastavenie kontroly súborov na vymeniteľných médiách nájdete v časti **Vykonávať kontrolu týchto médií** > **Vymeniteľné médiá**. Pre správne fungovanie **prístupu k zavádzaciemu sektoru vymeniteľného média** nechajte v sekcii ThreatSense povolenú možnosť **Zavádzacie sektory/UEFI**.

Vylúčenia procesov

Prečítajte si kapitolu Vylúčenia procesov.

ThreatSense

Rezidentná ochrana súborového systému kontroluje všetky typy médií, pričom kontrola sa vykonáva pri rôznych udalostiach, napríklad pri prístupe k súboru. Pomocou detekčných metód technológie **ThreatSense** (bližšie informácie nájdete v časti ThreatSense) môže byť rezidentná ochrana súborového systému nastavená tak, aby pracovala s novovytvorenými súbormi inak ako v prípade už dlhšie existujúcich súborov. Napríklad pri novovytvorených súboroch je možné nastaviť hlbšiu úroveň kontroly.

Pre zabezpečenie minimálnych systémových nárokov pri používaní rezidentnej ochrany nedochádza k opakovanej kontrole tých súborov, ktoré už boli skontrolované (pokiaľ neboli zmenené). Hneď po každej novej aktualizácii detekčného jadra sú súbory opätovne skontrolované na prítomnosť infiltrácií. Toto správanie je kontrolované pomocou **Smart optimalizácie**. Pokiaľ **Smart optimalizáciu** vypnete, všetky súbory budú kontrolované vždy vtedy, keď sa k nim pristupuje. Ak chcete toto nastavenie zmeniť, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Rezidentná ochrana súborového systému**. Kliknite na **ThreatSense** > **Iné** a pomocou prepínača vedľa položky **Zapnúť Smart optimalizáciu** povoľte alebo zakážte túto funkciu.

Rezidentná ochrana súborového systému tiež umožňuje konfigurovať Doplňujúce parametre ThreatSense.

Vylúčenia procesov

Funkcia Vylúčenia procesov vám umožňuje vylúčiť procesy aplikácií z Rezidentnej ochrany súborového systému. Na zvýšenie rýchlosti zálohovania a vylepšenie integrity procesov a dostupnosti služieb sa počas zálohovania používajú niektoré techniky, ktoré sú v konflikte s antimalvérovou ochranou súborového systému. Jediným efektívnym riešením je deaktivácia antimalvérového softvéru. Vylúčením konkrétneho procesu (napr. procesu zálohovacieho riešenia) budú všetky jeho operácie so súbormi ignorované a považované za bezpečné, čím sa minimalizuje interferencia s procesom zálohovania. Pri vytváraní vylúčení odporúčame byť opatrný – zálohovací nástroj, ktorý bol vylúčený, môže pristupovať k infikovaným súborom bez toho, aby sa spustilo upozornenie, čo je dôvod, prečo sú rozšírené povolenia povolené iba v module rezidentnej ochrany.

> Tento typ vylúčení si nezamieňajte s príponami súborov vylúčených z kontroly, HIPS vylúčeniami, vylúčeniami detekcií a výkonnostnými vylúčeniami.

Vylúčenia procesov pomáhajú minimalizovať riziko potenciálnych konfliktov a zvýšiť výkon vylúčených aplikácií, čo má pozitívny vplyv na celkový výkon a stabilitu operačného systému. Vylúčenie procesu/aplikácie je vylúčenie príslušného spustiteľného súboru (*.exe*).

Spustiteľné súbory môžete pridať do zoznamu vylúčených procesov v sekcii Rozšírené nastavenia > **Ochrana** > **Rezidentná ochrana súborového systému** > **Rezidentná ochrana súborového systému** > **Vylúčenia procesov**.

Táto funkcia bola navrhnutá tak, aby vylúčila z kontroly zálohovacie nástroje. Vylúčenie procesu zálohovacieho nástroja z kontroly nielen zabezpečuje stabilitu systému, ale taktiež nemá negatívny vplyv na rýchlosť zálohy, keďže počas spustenia zálohy nedochádza k jej spomaľovaniu.

Kliknite na **Upraviť** pre otvorenie okna **Vylúčenia procesov**, v ktorom môžete pridať vylúčenie a vyhľadať spustiteľný súbor (napr. *Backup-tool.exe*), ktorý chcete vylúčiť z kontroly.
Hneď ako pridáte súbor *.exe* do vylúčení, aktivita príslušného procesu viac nebude monitorovaná programom ESET Internet Security a nebudú kontrolované žiadne operácie so súbormi, ktoré tento proces vykoná.

Ak spustiteľný súbor nevyberiete pomocou funkcie určenej na prehľadávanie, budete musieť k danému súboru manuálne zadať úplnú cestu. V opačnom prípade vylúčenie nebude fungovať správne a HIPS môže hlásiť chyby.

Existujúce vylúčené procesy môžete **upravovať** alebo ich **odstrániť** z vylúčení.

Ochrana prístupu na web neberie takéto vylúčenie do úvahy, preto v prípade, že vylúčite z kontroly spustiteľný súbor vášho webového prehliadača, sťahované súbory budú aj naďalej kontrolované. Vďaka tomu je stále možné zachytiť prípadné infiltrácie. Tento scenár slúži len ako príklad a neodporúčame vytvárať vylúčenia pre webové prehliadače.

Pridanie alebo úprava vylúčení procesov

Toto dialógové okno vám umožňuje **pridať** procesy, ktoré majú byť vylúčené z kontroly detekčným jadrom. Vylúčenia procesov pomáhajú minimalizovať riziko potenciálnych konfliktov a zvýšiť výkon vylúčených aplikácií, čo má pozitívny vplyv na celkový výkon a stabilitu operačného systému. Vylúčenie procesu/aplikácie je vylúčenie príslušného spustiteľného súboru (*.exe*).

Nastavte cestu k spustiteľnému súboru aplikácie, ktorú chcete vylúčiť z kontroly, kliknutím na ... (napr. *C:\Program Files\Firefox\Firefox.exe*). Nezadávajte názov aplikácie.
Hneď ako pridáte súbor *.exe* do vylúčení, aktivita príslušného procesu viac nebude monitorovaná programom ESET Internet Security a nebudú kontrolované žiadne operácie so súbormi, ktoré tento proces vykoná.

Ak spustiteľný súbor nevyberiete pomocou funkcie určenej na prehľadávanie, budete musieť k danému súboru manuálne zadať úplnú cestu. V opačnom prípade vylúčenie nebude fungovať správne a HIPS môže hlásiť chyby.

Existujúce vylúčené procesy môžete **upravovať** alebo ich **odstrániť** z vylúčení.

Kedy meniť nastavenia rezidentnej ochrany

Rezidentná ochrana je kľúčovým modulom zabezpečujúcim ochranu počítača. Preto pri zmenách nastavení treba byť obozretný. Nastavenia rezidentnej ochrany odporúčame meniť len v špecifických prípadoch.

Po nainštalovaní ESET Internet Security sú všetky nastavenia optimalizované na zabezpečenie najvyššej úrovne ochrany systému používateľa. Ak chcete obnoviť predvolené nastavenia, kliknite na ↩ vedľa možnosti Rozšírené

nastavenia > **Ochrana** > **Reakcie na detekciu**.

Kontrola rezidentnej ochrany

To, či je rezidentná ochrana funkčná a deteguje vírusy, je možné otestovať pomocou testovacieho súboru z *www.eicar.com*. Ide o neškodný testovací súbor, ktorý by každý funkčný antivírusový program mal byť schopný detegovať. Súbor bol vytvorený spoločnosťou EICAR (European Institute for Computer Antivirus Research) na otestovanie funkčnosti antivírusových programov.

Súbor je dostupný na stiahnutie na adrese http://www.eicar.org/download/eicar.com.
Keď túto URL adresu zadáte do prehliadača, mala by sa vám zobraziť správa o odstránení hrozby.

Čo robiť, ak nefunguje rezidentná ochrana

V tejto kapitole sú popísané problémové stavy, ktoré môžu nastať v prípade rezidentnej ochrany, a tiež ich odporúčané riešenie.

Rezidentná ochrana je vypnutá

Ak používateľ omylom vypne rezidentnú ochranu súborového systému, je potrebné ju znova aktivovať. V takomto prípade otvorte hlavné okno programu a kliknite na **Nastavenia** > **Ochrana počítača** > **Rezidentná ochrana súborového systému**.

Ak sa rezidentná ochrana automaticky nespúšťa pri štarte systému, pravdepodobne je deaktivovaná možnosť **Zapnúť rezidentnú ochranu súborového systému**. Aby ste sa uistili, že je táto možnosť zapnutá, otvorte Rozšírené nastavenia > **Ochrana** > **Rezidentná ochrana súborového systému**.

Rezidentná ochrana nedeteguje a nelieči infiltrácie

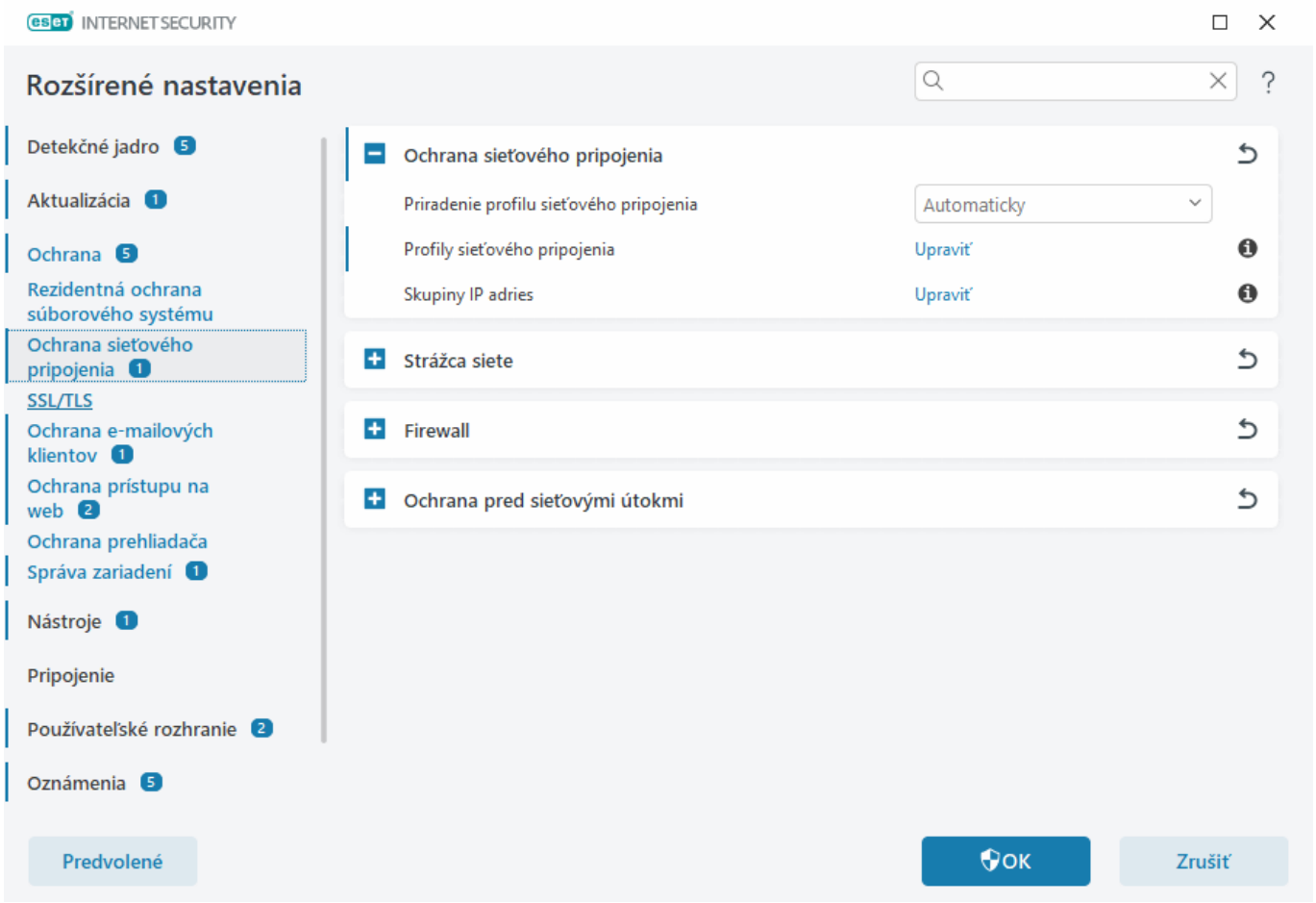
Uistite sa, že nemáte nainštalovaný antivírusový program od inej spoločnosti. Ak sú na počítači nainštalované dva antivírusové programy, medzi ich rezidentnými ochranami môže dochádzať ku konfliktu. Odporúčame preto odinštalovať akýkoľvek iný antivírusový program zo systému.

Rezidentná ochrana sa nespúšťa pri štarte

Ak sa rezidentná ochrana automaticky nespúšťa pri štarte systému (a možnosť **Zapnúť rezidentnú ochranu súborového systému** je aktivovaná), pravdepodobne dochádza ku konfliktu s iným programom. V takomto prípade odporúčame vytvoriť protokol ESET SysInspector a odoslať ho na analýzu technickej podpore spoločnosti ESET.

Ochrana sieťového pripojenia

Ochrana sieťového pripojenia umožňuje podrobnú konfiguráciu všetkých sieťových pripojení. Prostredníctvom nastavení môžete povoliť/blokovať prístup k svojmu počítaču z konkrétnych sietí, povoliť/zakázať prístup k sieťovým zariadeniam z počítača a podobne. ESET Internet Security má predvolene nastavené pravidlá firewallu a ochranu sieťových pripojení tak, aby zaisťovali maximálnu bezpečnosť. Špecifické prostredia si však môžu vyžadovať vlastnú konfiguráciu. Zmenu predvolených nastavení by mal vykonávať len skúsený používateľ.



Nasledujúce nastavenia môžete konfigurovať v sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** (kliknutím na odkazy nižšie si zobrazíte podrobný popis jednotlivých možností ochrany sieťového pripojenia):

Ochrana sieťového pripojenia

Profily sieťového pripojenia – profily umožňujú ovládať správanie firewallu v prípade konkrétnych sieťových pripojení.

Skupiny IP adries – môžete zadefinovať IP adresy, ktoré spolu tvoria logickú skupinu IP adries použiteľnú pri vytváraní pravidiel firewallu.

Strážca siete

Firewall

Ochrana pred sieťovými útokmi

Profily sieťového pripojenia

Profily sú účinným nástrojom na kontrolu správania funkcie Ochrana siete v programe ESET Internet Security pre konkrétne sieťové pripojenia. Pri vytváraní alebo úprave pravidla firewallu, IDS pravidla alebo pravidla ochrany pred útokmi hrubou silou môžete takéto pravidlo priradiť konkrétnemu profilu alebo ho aplikovať na všetky profily. Keď sa pre sieťové pripojenie aktivuje konkrétny profil, budú použité len globálne pravidlá (pravidlá bez priradeného profilu) a pravidlá, ktoré boli priradené priamo k danému profilu. Používateľ môže

vytvoriť viacero profilov s rôznymi priradenými pravidlami pre sieťové pripojenia, vďaka čomu môže jednoducho meniť správanie Firewallu.

Profily sieťového pripojenia a ich priradenie môžete konfigurovať v sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Ochrana sieťového pripojenia**.

Priradenie profilu sieťového pripojenia – umožňuje vám vybrať, či sa má novoobjaveným sieťovým pripojeniam automaticky priradiť prednastavený alebo vlastný profil na základe aktivátorov nakonfigurovaných v profiloch sieťového pripojenia (v takom prípade z roletového menu vyberte možnosť **Automaticky**), alebo či sa vám má pri každom zachytení nového sieťového pripojenia zobraziť výzva na nastavenie ochrany siete a manuálne priradenie profilu (v takom prípade z roletového menu vyberte možnosť **Spýtať sa**).

Konkrétny profil sieťového pripojenia môžete priradiť aj manuálne v hlavnom okne programu v sekcii **Nastavenia** > **Ochrana siete** > **Sieťové pripojenia**. Prejdite kurzorom myši na požadované sieťové pripojenie, kliknutím na ikonu menu > **Upraviť** otvorte okno Nastavenie ochrany siete a vyberte profil.

Profily sieťového pripojenia – kliknutím na tlačidlo **Upraviť** pridáte alebo upravíte profily sieťového pripojenia.

Nasledujúce profily sú preddefinované a nie je možné ich upraviť/odstrániť:

Súkromný – pre dôveryhodné siete (domácu alebo pracovnú sieť). Váš počítač a zdieľané súbory uložené na počítači budú viditeľné zo siete a systémové prostriedky budú dostupné pre ostatných používateľov v sieti (prístup k zdieľaným súborom a tlačiarňam, ako aj prichádzajúca RPC komunikácia budú povolené a služba zdieľania pracovnej plochy bude takisto dostupná). Toto nastavenie odporúčame použiť pri bezpečných lokálnych sieťach. Tento profil sa automaticky priradí k sieťovému pripojeniu, ak je v systéme Windows použitá konfigurácia domény alebo súkromnej siete.

Verejný – pre nedôveryhodné siete (verejné siete). Súbory a priečinky uložené vo vašom systéme nebudú zdieľané ani viditeľné pre ostatných používateľov v sieti a zdieľanie systémových prostriedkov bude deaktivované. Toto nastavenie odporúčame použiť pri pripojení k bezdrôtovým sieťam. Tento profil sa automaticky priradí ku každému sieťovému pripojeniu, ktoré nie je v systéme Windows nakonfigurované ako doména alebo súkromná sieť.

Keď sa pre sieťové pripojenie zapne iný profil, zobrazí sa oznámenie v pravom dolnom rohu obrazovky.

Pridanie alebo úprava profilov sieťového pripojenia

Profily sieťového pripojenia môžete pridať alebo upraviť v sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Ochrana sieťového pripojenia** > **Profily sieťového pripojenia** > **Upraviť**. Ak chcete profil upraviť, musíte ho vybrať zo zoznamu v okne **Profily sieťového pripojenia**.

Nasledujúce profily sú preddefinované a nie je možné ich upraviť/odstrániť:

Súkromný – pre dôveryhodné siete (domácu alebo pracovnú sieť). Váš počítač a zdieľané súbory uložené na počítači budú viditeľné zo siete a systémové prostriedky budú dostupné pre ostatných používateľov v sieti (prístup k zdieľaným súborom a tlačiarňam, ako aj prichádzajúca RPC komunikácia budú povolené a služba zdieľania pracovnej plochy bude takisto dostupná). Toto nastavenie odporúčame použiť pri bezpečných lokálnych sieťach. Tento profil sa automaticky priradí k sieťovému pripojeniu, ak je v systéme Windows použitá konfigurácia domény alebo súkromnej siete.

Verejný – pre nedôveryhodné siete (verejné siete). Súbory a priečinky uložené vo vašom systéme nebudú

zdieľané ani viditeľné pre ostatných používateľov v sieti a zdieľanie systémových prostriedkov bude deaktivované. Toto nastavenie odporúčame použiť pri pripojení k bezdrôtovým sieťam. Tento profil sa automaticky priradí ku každému sieťovému pripojeniu, ktoré nie je v systéme Windows nakonfigurované ako doména alebo súkromná sieť.

Navrch/Vyššie/Nižšie/Naspodok  – umožňuje nastaviť prioritu profilov sieťového pripojenia (profily sieťového pripojenia sa vyhodnocujú a používajú podľa nastavenej priority, pričom sa vždy použije prvý zodpovedajúci profil).

Pridanie alebo úprava profilu

Vlastný profil sieťového pripojenia umožňuje použiť pravidlá firewallu a definovať ďalšie nastavenia pre konkrétne sieťové pripojenia. V sekcii Aktivátory určíte, ku ktorým sieťovým pripojeniam bude vlastný profil priradený.

Ak chcete otvoriť editor profilov, v okne **Profily sieťového pripojenia**:

- Kliknite na **Pridať**.
- Vyberte jeden z existujúcich profilov a kliknite na **Upraviť**.
- Vyberte jeden z existujúcich profilov a kliknite na **Kopírovať**.

Názov – vami zadefinovaný názov profilu.

Popis – popis profilu na jeho jednoduchšiu identifikáciu.

Dodatočné dôveryhodné adresy – zadefinované adresy sa pridajú do dôveryhodnej zóny sieťového pripojenia, ku ktorému je tento profil priradený (bez ohľadu na typ ochrany siete).

Dôveryhodné pripojenie – váš počítač a zdieľané súbory uložené na počítači budú viditeľné zo siete a systémové prostriedky budú dostupné pre ostatných používateľov v sieti (prístup k zdieľaným súborom a tlačiarňam, ako aj prichádzajúca RPC komunikácia budú povolené a služba zdieľania pracovnej plochy bude takisto dostupná). Toto nastavenie odporúčame použiť pri vytváraní profilu pre zabezpečené pripojenie k lokálnej sieti. Všetky priamo pripojené podsiete sa tiež považujú za dôveryhodné. Napríklad ak má sieťový adaptér pre túto sieť IP adresu 192.168.1.5 a masku podsiete 255.255.255.0, podsieť 192.168.1.0/24 bude pridaná do dôveryhodnej zóny daného sieťového pripojenia. Ak má adaptér viac adries/podsietí, všetky budú dôveryhodné.

Upozorniť na slabé šifrovanie siete Wi-Fi – ESET Internet Security zobrazí oznámenie na ploche, ak sa pripojíte do nezabezpečenej alebo slabo zabezpečenej bezdrôtovej siete.

Aktivátory – používateľom nastavené podmienky, pri splnení ktorých sa sieťovému pripojeniu priradí príslušný profil sieťového pripojenia. Podrobné vysvetlenie nájdete v kapitole Aktivátory.

Aktivátory

Aktivátory predstavujú používateľom nastavené podmienky, pri splnení ktorých sa sieťovému pripojeniu priradí príslušný profil sieťového pripojenia. Ak má pripojená sieť rovnaké atribúty, aké sú definované v aktivátoroch v rámci profilu, daný profil sa aplikuje na pripojenú sieť. Profil sieťového pripojenia môže mať jeden alebo viacero aktivátorov. V prípade viacerých aktivátorov sa použije logický operátor OR (musí byť splnená aspoň jedna podmienka). Aktivátory môžete nastaviť v editore profilu sieťového pripojenia. Vytváranie vlastných profilov sieťového pripojenia sa odporúča len skúseným používateľom.

K dispozícii sú nasledujúce aktivátory (ak chcete zistiť podrobnosti vašej aktuálnej siete, pozrite si časť Sieťové pripojenia):

Adaptér

Typ adaptéra – profil sa aplikuje, ak je sieťové pripojenie nadviazané na vybranom type adaptéra.
Názov adaptéra – profil sa použije v prípade zhody s názvom sieťového adaptéra.
IP adresa adaptéra – profil sa použije v prípade zhody s IP adresou vášho sieťového adaptéra.

DNS

Prípona DNS – profil sa použije v prípade zhody s názvom domény.
IP adresa DNS – profil sa použije v prípade zhody s IP adresou DNS servera.

WINS

Profil sa použije v prípade zhody s IP adresou namapovanou cez službu Windows Internet Name Service (WINS).

DHCP

IP adresa DHCP – profil sa použije v prípade zhody s IP adresou DHCP servera.

Predvolená brána

IP adresa – profil sa použije v prípade zhody s IP adresou predvolenej brány.
MAC adresa – profil sa použije v prípade zhody s MAC adresou predvolenej brány.

Wi-Fi

SSID – profil sa použije v prípade zhody s identifikátorom SSID (názov siete Wi-Fi).
Názov profilu – profil sa použije v prípade zhody s názvom profilu Wi-Fi.
Typ zabezpečenia – profil sa použije v prípade, že sa typ zabezpečenia zhoduje s typom zvoleným v roletovom menu. Ak chcete vybrať viac ako jeden typ, vytvorte ďalší aktivátor.
Typ šifrovania – profil sa použije v prípade, že sa typ šifrovania zhoduje s typom zvoleným v roletovom menu. Ak chcete vybrať viac ako jeden typ, vytvorte ďalší aktivátor.
Zabezpečenie siete – profil sa použije v prípade, ak je sieť **otvorená/zabezpečená**.

Profil systému Windows

Profil sa použije v prípade, ak je sieť nakonfigurovaná v systéme Windows ako **doména/súkromná/verejná**.

Overenie

Sieťová autentifikácia vyhľadáva špecifický server na sieti a používa asymetrické šifrovanie (RSA) na autentifikáciu s týmto serverom. Názov siete, ktorá je overovaná, musí byť zhodný s názvom nastaveným v nastaveniach autentifikačného servera. Názov rozlišuje veľké a malé písmená. Názov servera môžete zadať ako IP adresu, názov DNS alebo NetBios.
Stiahnite si nástroj ESET Authentication Server.
Verejný kľúč môže byť vložený v nasledujúcich typoch:
• Verejný kľúč zašifrovaný vo formáte PEM (.pem); tento kľúč môžete vygenerovať pomocou nástroja ESET Authentication Server
• Šifrovaný verejný kľúč
• Verejný certifikát (.crt)
Kliknite na **Testovať** pre otestovanie nastavení. Ak bola autentifikácia úspešná, objaví sa oznámenie Overenie so serverom bolo úspešné. Ak nie je autentifikácia nastavená správne, môže sa objaviť jedno z nasledujúcich chybových hlásení:
Overenie so serverom nebolo úspešné. Neplatný alebo nezhodujúci sa podpis.
Podpis servera sa nezhoduje so zadaným verejným kľúčom.
Overenie so serverom nebolo úspešné. Názov siete sa nezhoduje.
Nastavený názov siete sa nezhoduje s názvom nastaveným na autentifikačnom serveri. Overte názvy a uistite sa, že sú zhodné.
Overenie so serverom nebolo úspešné. Neplatná alebo žiadna odpoveď zo servera.
Nie je prijatá odpoveď zo servera, server nie je spustený alebo je nedostupný. Neplatná odpoveď môže byť spôsobená iným HTTP serverom spusteným na nastavenej adrese.
Zadaný verejný kľúč je neplatný.
Uistite sa, že zadaný súbor verejného kľúča nie je poškodený.

Skupiny IP adries

Skupina IP adries je súbor IP adries, ktoré spolu tvoria jednu logickú skupinu IP adries. Skupiny sú užitočné, ak potrebujete použiť rovnakú skupinu IP adries vo viacerých pravidlách firewallu alebo pravidlách ochrany pred útokmi hrubou silou. ESET Internet Security obsahuje aj prednastavené skupiny IP adries, pre ktoré sa uplatňujú interné pravidlá. Príkladom takejto skupiny je napríklad **Dôveryhodná zóna**. Dôveryhodná zóna predstavuje skupinu sieťových adries, kde váš počítač a zdieľané súbory uložené na počítači budú viditeľné zo siete a systémové prostriedky budú dostupné pre ostatných používateľov v sieti.

Pridanie skupiny IP adries:

1. Otvorte Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Skupiny IP adries** > **Upraviť**.

2. Kliknite na tlačidlo **Pridať**, zadajte **Názov** a **Popis** zóny a do poľa **Vzdialená adresa počítača (IPv4, Ipv6, rozsah, maska)** zadajte vzdialenú IP adresu.

3. Kliknite na tlačidlo **OK**.

Ďalšie informácie nájdete v časti Úprava skupín IP adries.

Úprava skupín IP adries

Viac informácií o skupinách IP adries nájdete v kapitole Skupiny IP adries.

Stĺpce

Názov – názov skupiny vzdialených počítačov.

Popis – všeobecný popis skupiny.

IP adresy – vzdialené IP adresy, ktoré patria do konkrétnej skupiny IP adries.

Ovládacie prvky

Ak ste sa rozhodli **pridať** alebo **upraviť** skupinu IP adries, budú dostupné nasledujúce polia:

Názov – názov skupiny vzdialených počítačov.

Popis – všeobecný popis skupiny.

Vzdialená adresa počítača (IPv4, IPv6, rozsah, maska) – pridanie vzdialenej adresy, rozsahu adries alebo podsiete.

Odstrániť – odstránenie zóny zo zoznamu.

Prednastavené skupiny IP adries nie je možné odstrániť.

Príklady IP adries

Pridanie IPv4 adresy:
Samostatná adresa – zadanie IP adresy individuálneho počítača (napríklad *192.168.0.10*).
Rozsah adries – zadáva sa začiatočná a koncová IP adresa na stanovenie rozsahu IP adries skupiny počítačov (napr. *192.168.0.1-192.168.0.99*).
Podsieť – skupina počítačov patriacich do určitej podsiete. Zadáva sa IP adresa a maska podsiete. 255.255.255.0 je napríklad sieťová maska pre podsieť 192.168.1.0. Ak chcete vylúčiť celú podsieť, zadajte *192.168.1.0/24*.
Pridanie IPv6 adresy:
Samostatná adresa – zadanie IP adresy individuálneho počítača (napr. *2001:718:1c01:16:214:22ff:fec9:ca5*).
Podsieť – skupina počítačov patriacich do určitej podsiete. Zadáva sa IP adresa a maska podsiete (napr. *2002:c0a8:6301:1::1/64*).

Strážca siete

Strážca siete pomáha odhaliť bezpečnostné zraniteľnosti v rámci vašej dôveryhodnej (domácej alebo pracovnej) siete, ako napr. slabé heslo routera či otvorené porty. Poskytuje tiež zoznam pripojených zariadení, pričom zariadenia sú rozdelené do kategórií podľa typu (napr. tlačiarne, routery, mobilné zariadenia atď.). Vďaka tomu budete mať prehľad o tom, aké zariadenia sú pripojené k vašej sieti (napr. herná konzola, zariadenia IoT alebo iné domáce smart zariadenia). Strážcu siete môžete konfigurovať v sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Strážca siete**.

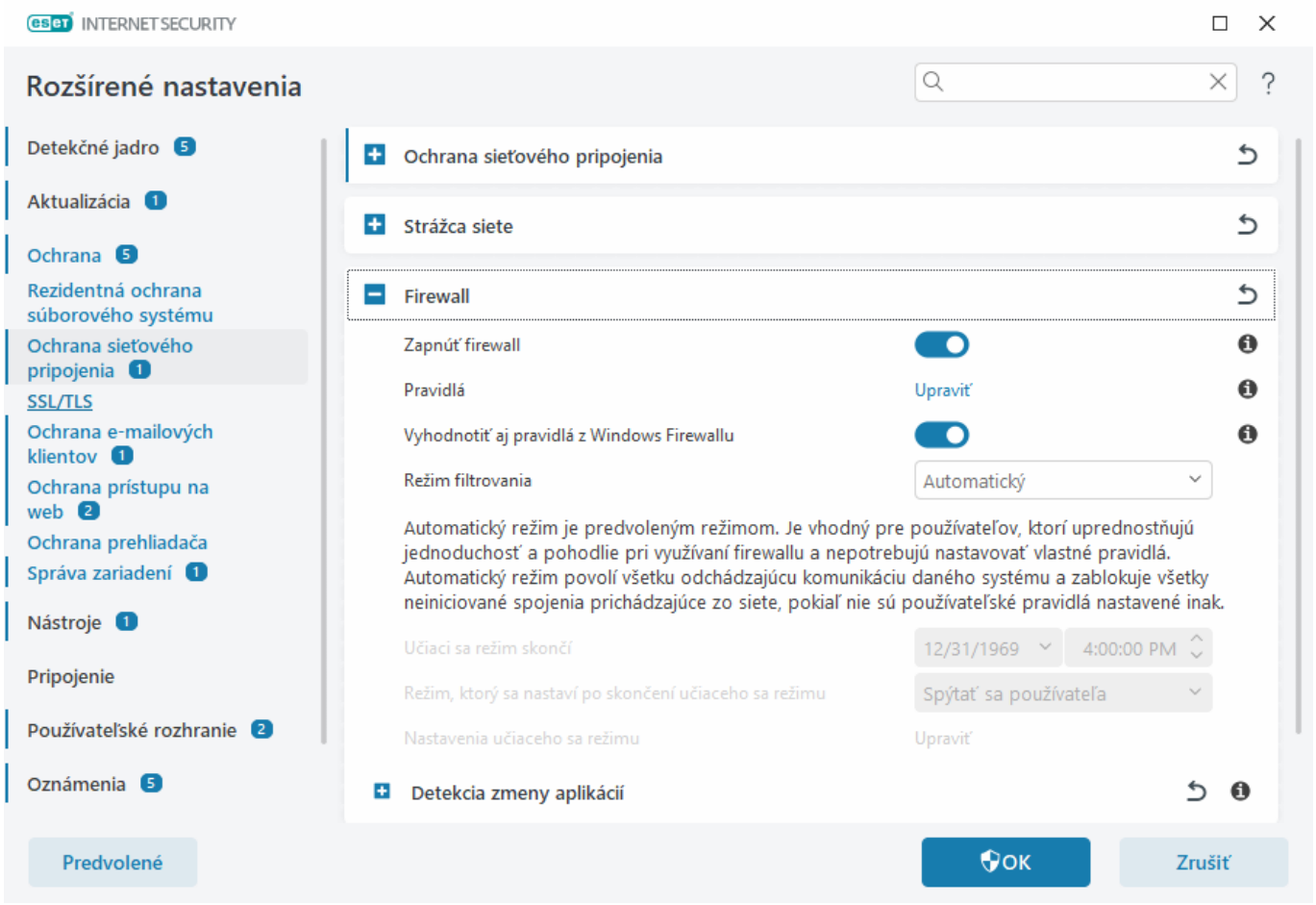
Zapnúť Strážcu siete – funkcia Strážca siete vám pomáha odhaliť bezpečnostné zraniteľnosti v sieti, napríklad slabé heslo routera či otvorené porty. Poskytuje aj zoznam pripojených zariadení, ktoré sú rozdelené do kategórií podľa typu.

Upozorniť na novoobjavené sieťové zariadenia – upozorní vás v prípade, že vo vašej sieti bolo zistené nové zariadenie.

Firewall

Firewall kontroluje všetku prichádzajúcu a odchádzajúcu sieťovú komunikáciu v počítači na základe interných a používateľom definovaných pravidiel. Jednotlivé sieťové pripojenia povoľuje alebo blokuje. Firewall chráni pred útokmi zo vzdialených zariadení a umožňuje blokovanie potenciálne nebezpečných služieb.

Ak chcete konfigurovať Firewall, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Firewall**.



Firewall

Zapnúť firewall

Na zaistenie maximálnej ochrany vášho systému vám odporúčame ponechať túto možnosť povolenú. Pri zapnutom Firewalle sa sieťová komunikácia kontroluje v oboch smeroch.

Pravidlá

Nastavenie pravidiel umožňuje prezeranie a úpravu všetkých pravidiel firewallu, ktorými sa riadi komunikácia jednotlivých aplikácií v rámci dôveryhodných pripojení a internetu.

Môžete vytvoriť IDS pravidlo pri Botnet útoku na váš počítač. Pravidlo je možné upravovať v sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Ochrana pred sieťovými útokmi** > **IDS pravidlá** po kliknutí na **Upraviť**.

Vyhodnotiť aj pravidlá z Windows Firewallu

Pri automatickom režime filtrovania bude povolená aj prichádzajúca komunikácia, ktorá je povolená pravidlami Windows Firewallu, pokiaľ nie je blokovaná existujúcimi pravidlami ESET.

Režim filtrovania

Správanie firewallu sa mení podľa zvoleného režimu filtrovania. Režimy filtrovania tiež určujú, do akej miery bude potrebná interakcia používateľa.

Firewall programu ESET Internet Security môže pracovať v štyroch režimoch filtrovania:

Režim filtrovania	Popis
Automatický režim	Ide o predvolený režim. Je vhodný pre používateľov, ktorí preferujú pohodlné používanie firewallu bez potreby vytvárania pravidiel. Vlastné používateľské pravidlá môžu byť vytvorené aj v **automatickom režime**, no nie sú povinné. Povoľuje všetku odchádzajúcu komunikáciu z daného systému a blokuje väčšinu novej prichádzajúcej komunikácie (okrem komunikácie z dôveryhodnej zóny, ktorá je nastavená v časti IDS a pokročilé možnosti/Povolené služby) a prichádzajúcej komunikácie odpovedajúcej na nedávnu odchádzajúcu komunikáciu.
Interaktívny režim	Umožňuje nastaviť si firewall na mieru podľa vašich požiadaviek. V prípade zistenia akejkoľvek komunikácie, na ktorú nie je možné aplikovať žiadne existujúce pravidlo, je používateľovi zobrazené informačné okno o zachytení neznámeho spojenia. Následne je možné túto komunikáciu povoliť alebo zamietnuť, pričom toto rozhodnutie môže byť uložené ako nové pravidlo firewallu. V prípade vytvorenia pravidla bude každá komunikácia tohto typu v budúcnosti povolená alebo zablokovaná podľa daného pravidla.
Režim politík	Blokuje každé spojenie, pre ktoré neexistuje povoľujúce pravidlo. Skúsený používateľ teda môže nastaviť pravidlá firewallu tak, aby boli povolené len želané a bezpečné spojenia. Firewall bude blokovať všetku ostatnú neznámu komunikáciu.
Učiaci sa režim	Automaticky vytvára a ukladá pravidlá. Tento režim je vhodný na prvotné nastavenie firewallu, no nemal by zostávať aktívny na dlhšie časové obdobie. Vytvorenie pravidiel prebehne bez interakcie s používateľom, keďže ESET Internet Security ukladá pravidlá na základe prednastavených parametrov. Tento režim odporúčame používať len dovtedy, kým sa nevytvoria všetky pravidlá pre bežnú komunikáciu. Vyhnete sa tak bezpečnostným rizikám.

Učiaci sa režim skončí – nastavte dátum a čas, kedy sa má tento režim automaticky skončiť. Učiaci sa režim môžete kedykoľvek vypnúť aj manuálne.

Režim, ktorý sa nastaví po skončení učiaceho sa režimu – táto možnosť určuje, ktorý režim filtrovania bude v rámci Firewallu použitý po skončení učiaceho sa režimu. Viac informácií o režimoch filtrovania nájdete v tabuľke vyššie. Možnosť **Spýtať sa používateľa** vyžaduje oprávnenia správcu, aby bolo možné vykonať zmenu režimu filtrovania.

Nastavenia učiaceho sa režimu – po kliknutí na tlačidlo **Upraviť** môžete konfigurovať parametre ukladania pravidiel vytváraných počas učiaceho sa režimu.

Detekcia zmeny aplikácií

Funkcia Detekcia zmeny aplikácií zobrazí upozornenie v momente, keď sa zmenená aplikácia (pre ktorú je vytvorené pravidlo firewallu) pokúsi nadviazať sieťové spojenie.

Učiaci sa režim

Učiaci sa režim automaticky vytvorí a uloží pre každú komunikáciu zodpovedajúce pravidlo. Vytvorenie pravidiel prebehne bez interakcie s používateľom, keďže ESET Internet Security ukladá pravidlá na základe prednastavených parametrov.

Používanie tohto režimu môže vystaviť váš systém riziku a odporúča sa len v prípade potreby prvotného nastavenia firewallu.

Ak chcete aktivovať Učiaci sa režim a súvisiace možnosti, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Firewall** > **Firewall** > **Režim filtrovania** a z roletového menu vyberte možnosť **Učiaci sa**. Po kliknutí na tlačidlo **Upraviť** vedľa položky **Nastavenia učiaceho sa režimu** môžete konfigurovať nasledujúce možnosti:

V učiacom sa režime firewall nefiltruje komunikáciu. Všetka odchádzajúca a prichádzajúca komunikácia je povolená. Váš počítač v tomto režime nie je plne chránený pomocou firewallu.

Prichádzajúca komunikácia z dôveryhodnej zóny – príkladom prichádzajúcej komunikácie z dôveryhodnej zóny je, keď sa vzdialené zariadenie z dôveryhodnej zóny pokúša komunikovať s lokálnou aplikáciou bežiacou na vašom počítači.

Odchádzajúca komunikácia do dôveryhodnej zóny – lokálna aplikácia sa pokúša nadviazať spojenie s iným zariadením v rámci lokálnej siete alebo inej siete v dôveryhodnej zóne.

Prichádzajúca internetová komunikácia – vzdialené zariadenie sa pokúša komunikovať s aplikáciou bežiacou na počítači.

Odchádzajúca internetová komunikácia – lokálna aplikácia sa pokúša nadviazať spojenie s iným zariadením.

V každej sekcii môžete definovať parametre, ktoré sa pridajú do vytváraných pravidiel:

Pridať lokálny port – číslo lokálneho portu sieťového spojenia. Pre odchádzajúcu komunikáciu sa generujú náhodné čísla. Preto je vhodné tento parameter definovať len pri kontrole prichádzajúcich spojení.

Pridať aplikáciu – názov lokálnej aplikácie. Túto možnosť odporúčame použiť vtedy, ak chcete do pravidla zahrnúť kompletnú komunikáciu špecifikovanej aplikácie. Napríklad môžete povoliť komunikáciu iba pre webový prehliadač, e-mailového klienta atď.

Pridať vzdialený port – číslo vzdialeného portu sieťovej komunikácie. Napríklad môžete povoliť/zakázať konkrétnu službu so štandardným číslom portu (napr. HTTP – 80, POP3 – 110 a pod.).

Pridať vzdialenú IP adresu/dôveryhodnú zónu – vzdialená IP adresa alebo celá zóna adries môže byť použitá ako parameter pre nové pravidlá, ktoré sa aplikujú na všetky sieťové spojenia medzi lokálnym systémom a vzdialenou adresou/zónou. Túto možnosť je vhodné použiť v prípade, že chcete definovať akcie pre konkrétne zariadenie alebo skupinu zariadení v sieti.

Maximálny počet pravidiel pre jednu aplikáciu – pokiaľ aplikácia komunikuje viacerými smermi (z rôznych portov, na rôzne IP adresy a pod.), Firewall v učiacom sa režime pre ňu vytvára zodpovedajúci počet pravidiel. Pomocou tejto možnosti je možné limitovať počet pravidiel, ktoré možno vytvoriť pre jednu aplikáciu.

Pravidlá firewallu

Pravidlá firewallu predstavujú zoznam podmienok, podľa ktorých sú testované všetky sieťové pripojenia, pričom na splnenie týchto podmienok sa viažu definované akcie. Pomocou pravidiel firewallu je teda možné definovať, aká akcia sa má vykonať s pripojením spĺňajúcim podmienky daného pravidla.

Pravidlá sa vyhodnocujú zhora nadol a ich priorita je uvedená v prvom stĺpci. To znamená, že pri každom testovanom sieťovom spojení bude uplatnená akcia prvého pravidla, ktorého podmienky boli splnené.

Z pohľadu smeru komunikácie je možné sieťové spojenia rozdeliť na prichádzajúce a odchádzajúce. Prichádzajúce spojenie je inicializované na vzdialenej strane, keď sa vzdialené zariadenie snaží nadviazať spojenie s lokálnym systémom (lokálnou stranou). V prípade odchádzajúceho spojenia je situácia opačná, teda lokálna strana nadväzuje spojenie so vzdialeným zariadením.

V prípade zachytenia neznámej komunikácie je potrebné zvážiť, či ju povoliť alebo zamietnuť. Nevyžiadané, nezabezpečené alebo úplne neznáme spojenia predstavujú pre systém bezpečnostné riziko. Pri takejto komunikácii je vhodné venovať pozornosť hlavne vzdialenému zariadeniu a aplikácii, ktoré sa pokúšajú nadviazať spojenie s vaším počítačom. Mnohé infiltrácie sa snažia získať a odoslať súkromné dáta alebo sťahujú iné škodlivé aplikácie na používateľské pracovné stanice. Práve takéto spojenia je možné pomocou firewallu odhaliť a zablokovať.

Pravidlá firewallu môžete zobraziť a upraviť v sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Firewall** > **Pravidlá** > **Upraviť**.

Ak máte veľa pravidiel firewallu, môžete použiť filter na zobrazenie len určitých pravidiel. Ak chcete filtrovať pravidlá firewallu, kliknite na možnosť **Ďalšie filtre** nad zoznamom pravidiel firewallu. Pravidlá môžete filtrovať podľa týchto kritérií:

- Pôvod
- Smer
- Akcia
- Dostupnosť

Štandardne sú predvolené pravidlá firewallu skryté. Ak chcete zobraziť všetky preddefinované pravidlá, deaktivujte prepínač vedľa položky **Skryť vstavané (predvolené) pravidlá**. Tieto pravidlá môžete deaktivovať, ale nemôžete ich zmazať.

Kliknutím na ikonu vyhľadávania v pravom hornom rohu vyhľadáte pravidlo.

Stĺpce

Priorita – pravidlá sa vyhodnocujú zhora nadol a ich priorita je uvedená v prvom stĺpci.

Zapnuté – zobrazuje, či je pravidlo aktívne alebo neaktívne; začiarknutím príslušného políčka je možné pravidlo

aktivovať.

Aplikácia – aplikácia, pre ktorú bude pravidlo platiť.

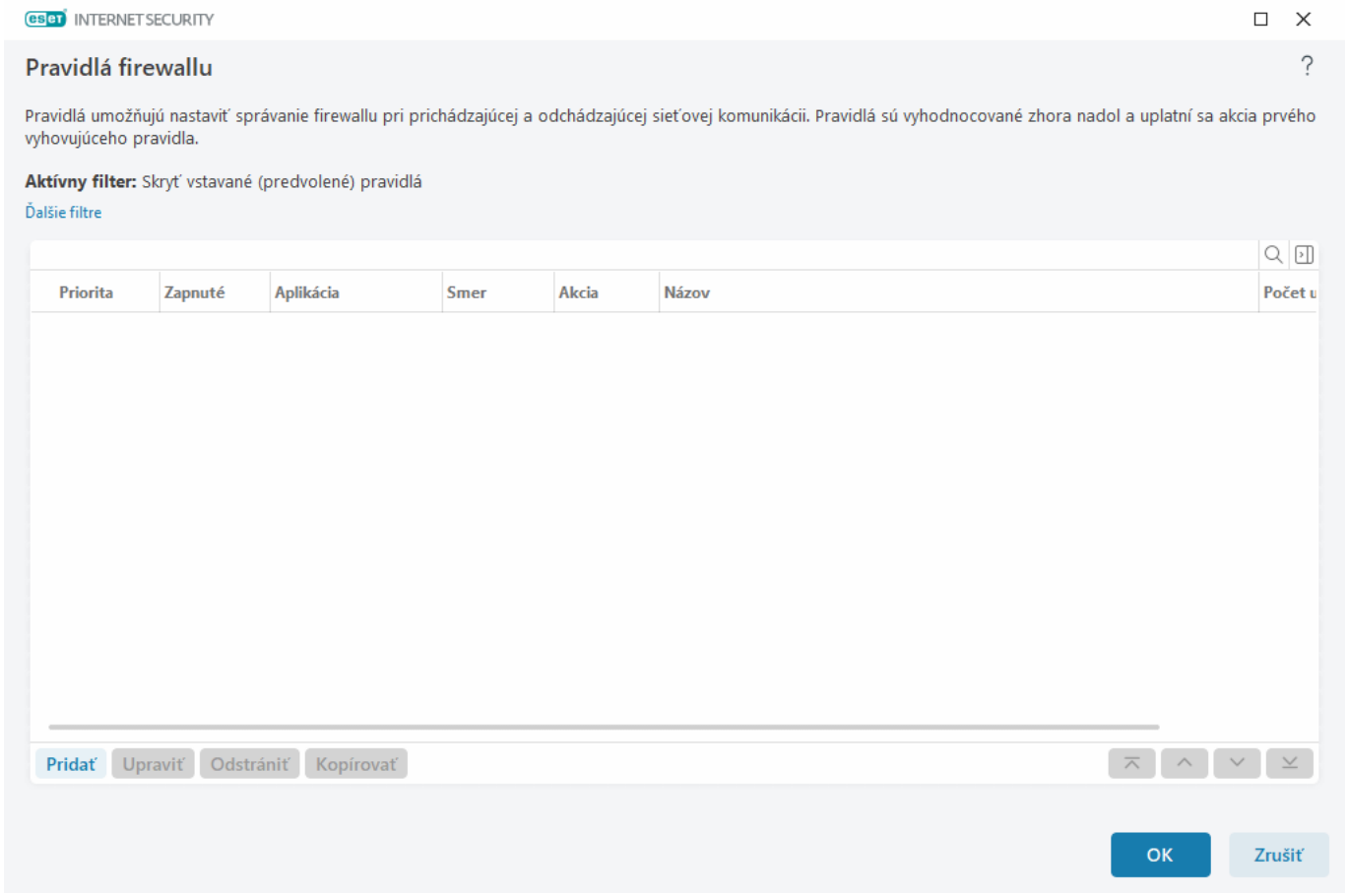
Smer – zobrazuje smer komunikácie (dnu/von/oba).

Akcia – zobrazuje stav komunikácie po uplatnení pravidla (povolené/zakázané/pýtať sa).

Názov – názov pravidla. Ikona ESET predstavuje predvolené pravidlo.

Počet uplatnení – celkový počet uplatnení pravidla.

Kliknutím na ikonu rozbalenia zobrazíte podrobnosti o pravidle.



Ovládacie prvky

Pridať – pridanie nového pravidla.

Upraviť – úprava existujúceho pravidla.

Odstrániť – odstránenie existujúceho pravidla.

Kopírovať – vytvorenie kópie vybraného pravidla.

Navrch/Vyššie/Nižšie/Naspodok – šípky, ktoré vám umožňujú meniť prioritu pravidiel v zozname (pravidlá sa uplatňujú zhora nadol).

Pridanie alebo úprava pravidiel firewallu

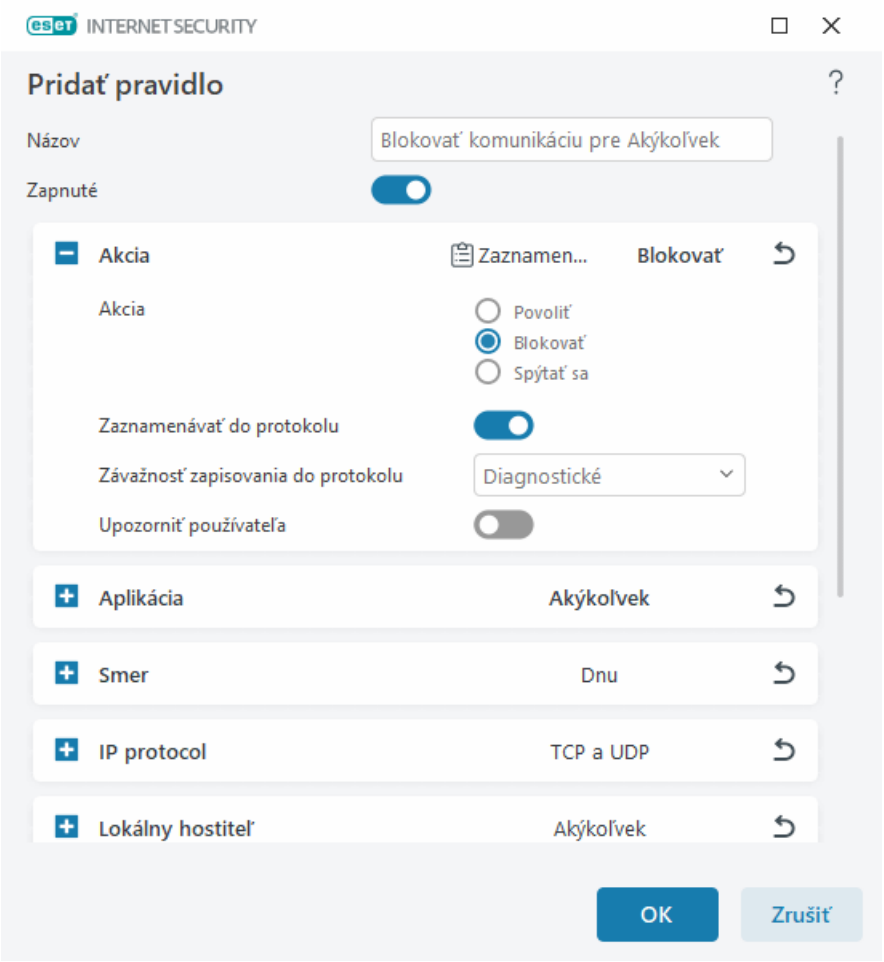
Pravidlá firewallu predstavujú podmienky, podľa ktorých sú testované všetky sieťové pripojenia, pričom na splnenie týchto podmienok sa viažu definované akcie. Pridanie alebo úprava pravidiel firewallu môžu byť potrebné v prípade zmeny sieťových nastavení (napríklad pri zmene sieťovej adresy vzdialenej strany alebo čísla portu) s cieľom zabezpečiť správne fungovanie aplikácie, ktorú ovplyvňuje pravidlo. Skúsený používateľ by si mal vytvoriť vlastné pravidlá firewallu.

Ilustrované inštrukcie

Berte, prosím, na vedomie, že nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:

- Povolenie alebo zakázanie konkrétneho portu vo firewalle ESET
- Ako vytvorím pravidlo firewallu z protokolov v programe ESET Internet Security?

Ak chcete pridať alebo upraviť pravidlo firewallu, otvorte Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Firewall** > **Pravidlá** > **Upraviť**. V okne Pravidlá firewallu kliknite na **Pridať** alebo **Upraviť**.



Názov – zadajte názov pravidla.

Zapnuté – kliknutím na prepínač sa pravidlo aktivuje.

Pridanie akcií a podmienok pre pravidlo firewallu:

Akcia

Akcia – vyberte, či chcete **povoliť/zakázať** komunikáciu, ktorá zodpovedá podmienkam definovaným v tomto pravidle, alebo či chcete, aby sa ESET Internet Security **spýtal** pri každom nadviazaní komunikácie.
Zaznamenávať do protokolu – ak sa pravidlo použije, zaznamená sa do protokolu.
Závažnosť zapisovania do protokolu – vyberte závažnosť zapisovania do protokolu pre toto pravidlo.
Upozorniť používateľa – zobrazí oznámenie v prípade, že sa pravidlo použije.

Aplikácia

Zadajte aplikáciu, na ktorú sa bude toto pravidlo uplatňovať.
Cesta k aplikácii – kliknite na **...** a prejdite na aplikáciu alebo zadajte úplnú cestu k aplikácii (napr. C:\Program Files\Firefox\Firefox.exe). Nezadávajte len názov aplikácie.
Podpis aplikácie – pravidlo môžete uplatniť na aplikácie na základe ich podpisu (názvu vydavateľa).
V roletovom menu vyberte, či chcete pravidlo uplatniť na aplikácie s **akýmkoľvek platným podpisom** alebo na aplikácie s **podpisom konkrétneho podpisovateľa**. Ak vyberiete aplikácie s **podpisom konkrétneho podpisovateľa**, musíte ho definovať v poli **Meno podpisovateľa**.
Aplikácia z Microsoft Store – v roletovom menu vyberte aplikáciu nainštalovanú z obchodu Microsoft Store.
Služba – namiesto aplikácie môžete vybrať systémovú službu. Rozbaľte roletové menu a vyberte službu.
Použiť na podradené procesy – niektoré aplikácie môžu spúšťať viac procesov, hoci vy vidíte len jedno okno aplikácie. Kliknutím na prepínač aktivujete pravidlo pre každý proces v zadanej aplikácii.

Smer

Vyberte **Smer** komunikácie pre toto pravidlo:
- **Oba** – prichádzajúca aj odchádzajúca komunikácia
- **Dnu** – len prichádzajúca komunikácia
- **Von** – len odchádzajúca komunikácia

Protokol IP

Ak chcete, aby sa toto pravidlo vzťahovalo len na konkrétny protokol, vyberte ho z roletového menu **Protokol**.

Lokálny hostiteľ

Lokálne adresy, rozsah adries alebo podsieť, na ktorú sa toto pravidlo vzťahuje. Ak nie je zadaná žiadna adresa, pravidlo sa bude uplatňovať na všetku komunikáciu s lokálnymi hostiteľmi. IP adresy, rozsahy adries alebo podsiete môžete pridať priamo do textového poľa **IP adresa** alebo vybrať z existujúcich skupín IP adries kliknutím na tlačidlo **Upraviť** vedľa možnosti **Skupiny IP adries**.

Lokálny port

Čísla lokálnych **portov**. Ak nie sú zadané žiadne čísla, pravidlo sa bude uplatňovať na akýkoľvek port. Zadajte čísla portov alebo ich rozsah.

Vzdialený hostiteľ

Vzdialená adresa, rozsah adries alebo podsieť, na ktorú sa toto pravidlo vzťahuje. Ak nie je zadaná žiadna adresa, pravidlo sa bude uplatňovať na všetku komunikáciu so vzdialenými hostiteľmi. IP adresy, rozsahy adries alebo podsiete môžete pridať priamo do textového poľa **IP adresa** alebo vybrať z existujúcich skupín IP adries kliknutím na tlačidlo **Upraviť** vedľa možnosti **Skupiny IP adries**.

Vzdialený port

Čísla **portov** komunikácie so vzdialenou stranou. Ak nie sú zadané žiadne čísla, pravidlo sa bude uplatňovať na akýkoľvek port. Zadajte čísla portov alebo ich rozsah.

Profil

Pravidlo firewallu možno uplatniť v prípade konkrétnych profilov sieťových pripojení.
Akýkoľvek – pravidlo sa uplatní v prípade akéhokoľvek sieťového pripojenia bez ohľadu na použitý profil.
Vybraný – pravidlo sa uplatní v prípade konkrétneho sieťového pripojenia na základe vybraného profilu. Začiarknite políčka vedľa profilov, ktoré chcete vybrať.

V tomto príklade si vytvoríme nové pravidlo, ktoré povolí webovému prehliadaču Firefox pristupovať k webovým stránkam na internete/lokálnej sieti:
1.V sekcii **Akcia** vyberte možnosť **Akcia** > **Povoliť**.
2.V sekcii **Aplikácia** zadajte **Cestu k aplikácii** webového prehliadača (napr. C:\Program Files\Firefox\Firefox.exe). Nezadávajte len názov aplikácie.
3.V sekcii **Smer** vyberte **Smer** > **Von**.
4.V sekcii **Protokol IP** vyberte z roletového menu **Protokol** možnosť **TCP a UDP**.
5.V sekcii **Vzdialený port** pridajte čísla **portov**: *80,443* na umožnenie štandardného prehliadania.

Detekcia zmeny aplikácií

Funkcia detekcie zmien aplikácií umožňuje zobraziť upozornenie na zmenu aplikácie (pre ktorú je vytvorené pravidlo firewallu) v momente, keď sa zmenená aplikácia pokúsi nadviazať sieťové spojenie. Zmena aplikácie znamená dočasné alebo trvalé nahradenie pôvodného spustiteľného súboru aplikácie iným súborom (chráni pred zneužitím pravidiel firewallu).

Táto funkcia nie je určená na detekciu zmien všetkých aplikácií. Cieľom tejto funkcie je zabrániť zneužitiu existujúcich pravidiel firewallu, preto sú monitorované len aplikácie, pre ktoré existujú pravidlá.

Ak chcete upraviť nastavenia pre **detekciu zmeny aplikácií**, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Firewall** > **Detekcia zmeny aplikácií**.

Sledovať zmenu aplikácií – program bude sledovať, či nedošlo k zmene aplikácií (či sa aplikácia aktualizovala, infikovala alebo inak zmenila). Firewall zobrazí upozornenie na zmenu aplikácie v momente, keď sa zmenená aplikácia pokúsi nadviazať sieťové spojenie.

Povoliť zmenu podpísaných (dôveryhodných) aplikácií – používateľ nebude informovaný o zmene aplikácie v prípade, že daná aplikácia má rovnaký digitálny podpis pred aj po zistenej zmene.

Zoznam aplikácií vylúčených z detekcie – v tomto zozname je možné pridávať alebo odoberať aplikácie, pre ktoré sú povolené zmeny. V prípade zmeny týchto aplikácií používateľ nedostane žiadne upozornenie.

Zoznam aplikácií vylúčených z detekcie

Firewall v programe ESET Internet Security umožňuje monitorovať stav aplikácií a odhaliť, ak sa ich škodlivý kód pokúsi modifikovať (pozri kapitolu Detekcia zmeny aplikácií).

Z rôznych dôvodov sa môže vyskytnúť stav, keď je pri špecifickej aplikácii táto funkcionalita nežiaduca a je potrebné danú aplikáciu z kontroly firewallom vylúčiť.

Pridať – zobrazí sa okno, v ktorom môžete vybrať aplikáciu, ktorú chcete pridať do zoznamu aplikácií vylúčených z detekcie zmien. Aplikáciu môžete vybrať zo zoznamu aplikácií, ktoré sa spúšťajú v systéme a pre ktoré vo Firewalle existuje pravidlo, prípadne môžete cestu k aplikácii zadať manuálne.

Upraviť – zobrazí sa okno, v ktorom môžete upraviť umiestenie aplikácie, ktorá je na zozname aplikácií vylúčených z detekcie zmien. Inú aplikáciu môžete vybrať zo zoznamu aplikácií, ktoré sa spúšťajú v systéme a pre ktoré vo firewalle existuje pravidlo, prípadne môžete umiestnenie aplikácie zmeniť manuálne.

Odstrániť – umožňuje odobrať položky zo zoznamu aplikácií vylúčených z detekcie zmien.

Ochrana pred sieťovými útokmi (IDS)

Ochrana pred sieťovými útokmi (IDS) zlepšuje detekciu zneužití známych zraniteľností. Viac informácií o ochrane pred sieťovými útokmi sa dočítate v slovníku pojmov. Ak chcete nakonfigurovať ochranu pred sieťovými útokmi, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Ochrana pred sieťovými útokmi**.

Zapnúť ochranu pred sieťovými útokmi (IDS) – analyzuje obsah sieťovej komunikácie a chráni pred sieťovými útokmi. Akákoľvek komunikácia, ktorá je považovaná za nebezpečnú, bude zablokovaná.

Zapnúť ochranu pred botnetmi – deteguje a blokuje komunikáciu s riadiacimi C&C servermi rozpoznávaním charakteristík, ktoré naznačujú, že počítač je infikovaný a bot sa pokúša komunikovať. Viac o ochrane pred botnetmi sa dočítate v slovníku pojmov.

IDS pravidlá – v tejto časti môžete nastaviť pokročilé možnosti filtrovania a detekcie rôznych typov zraniteľností a útokov, ktoré môžu byť namierené na váš počítač.

> **Ilustrované inštrukcie**
> Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
> - Ako vylúčiť IP adresu z IDS v programe ESET Internet Security

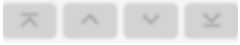
Všetky dôležité udalosti zaznamenané ochranou siete sú ukladané do protokolu. Pre viac informácií si pozrite kapitolu Protokol ochrany siete.

IDS pravidlá

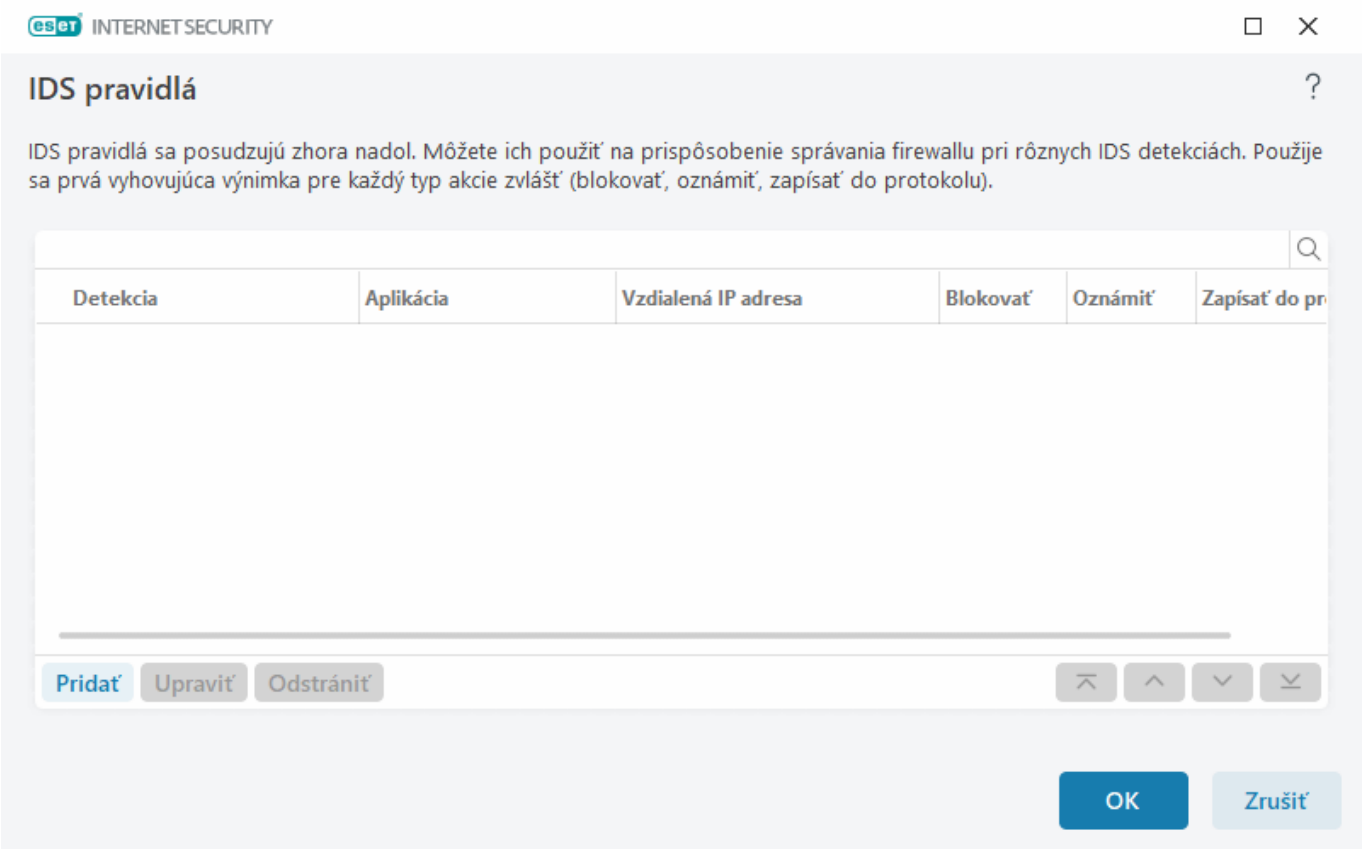
V niektorých situáciách môže systém na detekciu narušenia (IDS) zaznamenať komunikáciu medzi routermi alebo inými internými sieťovými zariadeniami ako potenciálny útok. Môžete napríklad pridať známu bezpečnú adresu do Adries vylúčených z aktívnej ochrany IDS, a tak obísť IDS.

> **Ilustrované inštrukcie**
> Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
> - Ako vylúčiť IP adresu z IDS v programe ESET Internet Security

Spravovanie IDS pravidiel

- **Pridať** – vytvorenie nového IDS pravidla.
- **Upraviť** – zmena existujúceho IDS pravidla.
- **Odstrániť** – odstránenie označeného IDS pravidla zo zoznamu.
-  **Navrch/Vyššie/Nižšie/Naspodok** – zmeňte prioritu položiek v zozname (pravidlá sú

vyhodnocované zhora nadol).



Editor pravidiel

Detekcia – typ detekcie.

Názov hrozby – pre niektoré z dostupných detekcií môžete zadať názov hrozby.

Aplikácia – nastavte cestu k vylúčenej aplikácii kliknutím na ... (napríklad *C:\Program Files\Firefox\Firefox.exe*). Nezadávajte názov aplikácie.

Vzdialená IP adresa – zoznam vzdialených IPv4 alebo IPv6 adries/rozsahov/podsietí. Viaceré adresy musia byť oddelené čiarkou.

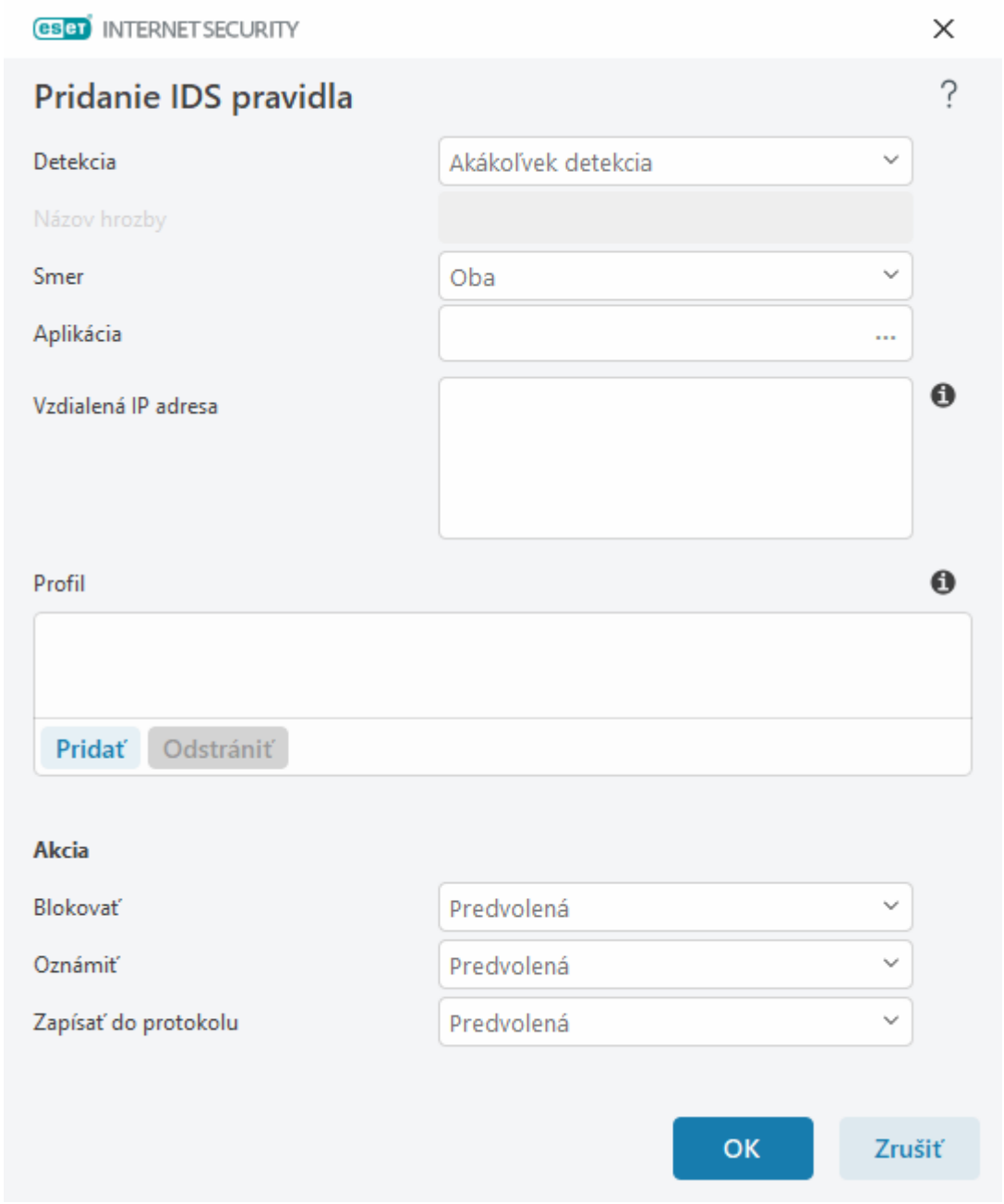
Profil – môžete vybrať profil sieťového pripojenia, na ktorý sa bude pravidlo vzťahovať.

Akcia

Blokovať – každý systémový proces má vlastné predvolené správanie a priradenú akciu (blokovať alebo povoliť). Pre zmenu predvoleného správania produktu ESET Internet Security vyberte z roletového menu možnosť áno alebo nie.

Oznámiť – ak chcete zapnúť zobrazovanie oznámení na ploche, označte možnosť Áno. Ak nechcete, aby sa zobrazovali oznámenia na ploche, označte možnosť Nie. Dostupné hodnoty sú Predvolená/Áno/Nie.

Zapísať do protokolu – ak chcete zaznamenávať udalosti do protokolu, označte možnosť **Áno**. Ak nechcete zaznamenávať udalosti do protokolu produktu, označte možnosť **Nie**. Dostupné hodnoty sú **Predvolená**/**Áno**/**Nie**.



Ak chcete, aby sa pri každom výskyte konkrétnej udalosti zobrazilo oznámenie a bol vytvorený protokol:
1.Kliknite na **Pridať** a pridajte nové IDS pravidlo.
2.Z roletového menu **Detekcia** vyberte konkrétny typ detekcie.
3.Po kliknutí na **...** zvoľte cestu k aplikácii, pre ktorú chcete toto oznámenie použiť.
4.V roletovom menu **Blokovať** ponechajte možnosť **Predvolená**. Takto bude vykonaná akcia, ktorá je predvolená produktom ESET Internet Security.
5.V roletovom menu **Oznámiť** a **Zapísať do protokolu** vyberte možnosť **Áno**.
6.Kliknite na **OK**, aby sa oznámenie uložilo.

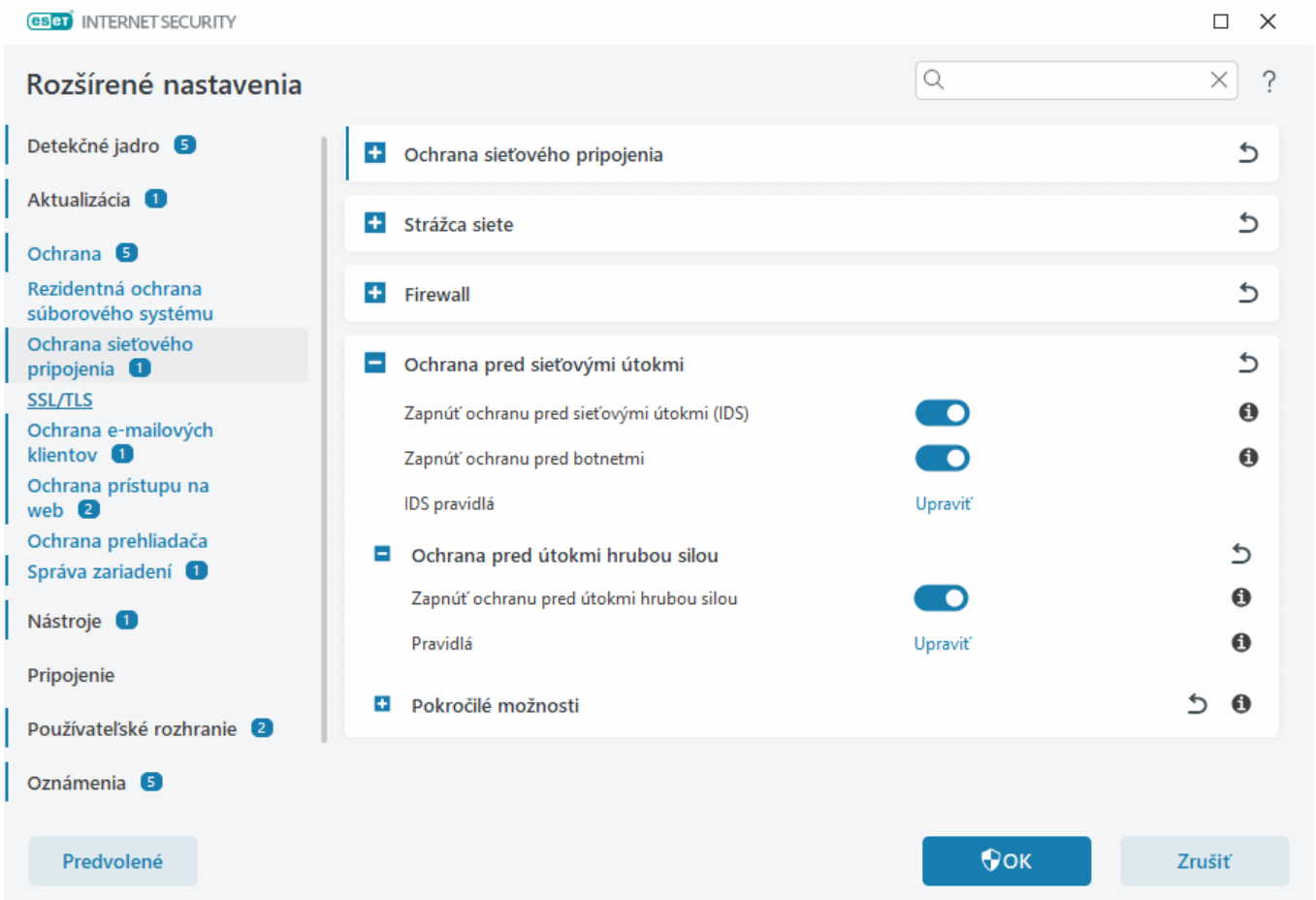
Ak chcete, aby sa prestali opakovane zobrazovať oznámenia pre konkrétny typ **Detekcie**, ktorú nepovažujete za hrozbu:
1.Kliknite na **Pridať** a pridajte nové IDS pravidlo.
2.Z roletového menu **Detekcia** vyberte konkrétny typ detekcie, napr. **Relácia SMB bez bezpečnostných rozšírení** alebo **Útok skenovaním portov TCP**.
3.V prípade prichádzajúcej komunikácie vyberte z roletového menu Smer možnosť **Dnu**.
4.V roletovom menu **Oznámiť** vyberte možnosť **Nie**.
5.V roletovom menu **Zapísať do protokolu** vyberte možnosť **Áno**.
6.Pole **Aplikácia** nechajte prázdne.
7.Ak komunikácia neprichádza z konkrétnej IP adresy, pole **Vzdialená IP adresa** nechajte prázdne.
8.Kliknite na **OK**, aby sa oznámenie uložilo.

Ochrana pred útokmi hrubou silou

Ochrana pred útokmi hrubou silou blokuje pokusy o uhádnutie hesiel pre služby SMB a RDP. Útok hrubou silou je metóda systematického testovania možných kombinácií písmen, číslic a symbolov s cieľom prelomiť heslo. Ak chcete nakonfigurovať ochranu pred útokmi hrubou silou, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Ochrana pred sieťovými útokmi** > **Ochrana pred útokmi hrubou silou**.

Zapnúť ochranu pred útokmi hrubou silou – ESET Internet Security kontroluje obsah sieťovej komunikácie a blokuje pokusy o uhádnutie hesiel.

Pravidlá – umožňujú vytvárať, upravovať a zobrazovať pravidlá pre prichádzajúce a odchádzajúce sieťové pripojenia. Viac informácií nájdete v kapitole Pravidlá.



Pravidlá

V okne s pravidlami ochrany pred útokmi hrubou silou môžete vytvárať, upravovať a zobrazovať pravidlá pre prichádzajúce a odchádzajúce sieťové pripojenia. Prednastavené pravidlá nie je možné upraviť ani odstrániť.

Správa pravidiel ochrany pred útokmi hrubou silou

Pridať – pridanie nového pravidla.

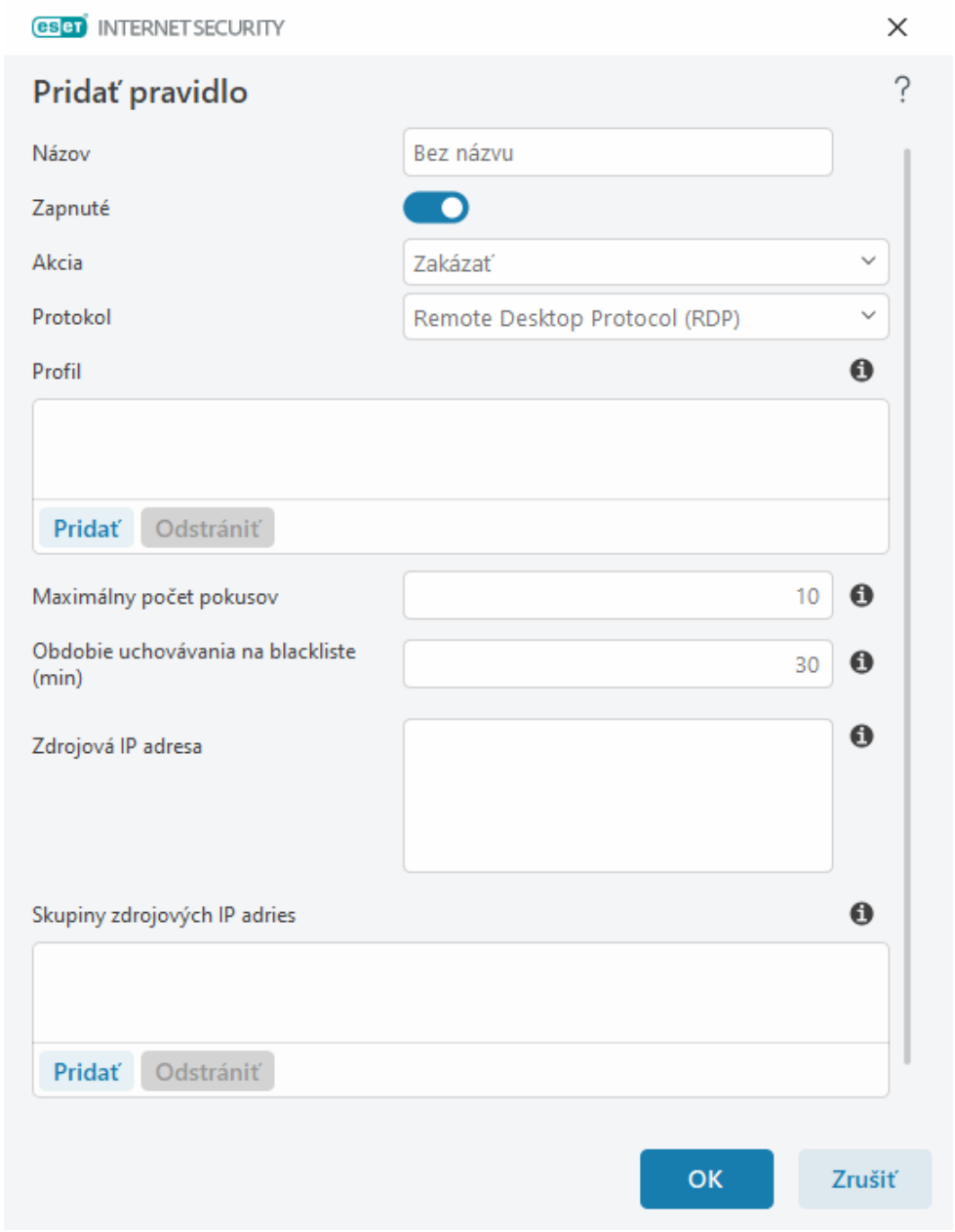
Upraviť – úprava existujúceho pravidla.

Odstrániť – odstránenie existujúceho pravidla zo zoznamu pravidiel.

 **Navrch/Vyššie/Nižšie/Naspodok** – šípky, ktoré vám jednoducho umožňujú meniť prioritu pravidiel v zozname.

> V záujme maximálnej ochrany sa blokovacie pravidlo s najnižšou hodnotou nastavenou pre **Maximálny počet pokusov** použije aj vtedy, keď je v zozname pravidiel nižšie v poradí a podmienkam detekcie vyhovuje viacero pravidiel blokovania.

Editor pravidiel



Názov – názov pravidla.

Zapnuté – deaktivujte túto možnosť, ak pravidlo nechcete používať, no želáte si ho ponechať v zozname.

Akcia – zvoľte, či sa má pri splnení pravidlom definovaných podmienok spojenie **Zakázať** alebo **Povoliť**.

Protokol – komunikačný protokol, pre ktorý má pravidlo platiť.

Profil – pre konkrétne profily možno nastaviť a použiť vlastné pravidlá.

Maximálny počet pokusov – maximálny povolený počet pokusov o opakovanie útoku, pokým IP adresa nebude zablokovaná a pridaná na blacklist.

Obdobie uchovávania na blackliste (min) – nastaví čas odstránenia IP adresy z blacklistu.

Zdrojová IP adresa – zoznam IP adries, rozsahov alebo podsietí. Viaceré adresy musia byť oddelené čiarkou.

Skupiny zdrojových IP adries – IP adresy, ktoré ste už zadefinovali v skupinách IP adries.

Pokročilé možnosti

V sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana sieťového pripojenia** > **Ochrana pred sieťovými útokmi** > **Pokročilé možnosti** môžete zapnúť alebo vypnúť detekciu rôznych typov útokov a zneužití, ktoré predstavujú nebezpečenstvo pre váš počítač.

V určitých prípadoch sa nezobrazí výstražné oznámenie o zablokovanej komunikácii. Postup zobrazenia všetkých blokovaných komunikácií nájdete v kapitole Vytváranie protokolov a pravidiel alebo výnimiek z protokolu.

Dostupnosť konkrétnych možností v tomto okne môže závisieť od typu alebo verzie vášho bezpečnostného produktu ESET a modulu firewallu, ako aj verzie vášho operačného systému.

Detekcia útokov

Detekcia útokov monitoruje sieťovú komunikáciu zariadenia a zachytáva škodlivú aktivitu.

- **Protokol SMB** – detekcia a blokovanie rôznych bezpečnostných problémov v SMB protokole.
- **Protokol RPC** – deteguje a blokuje rôzne zraniteľnosti (CVE) v protokole RPC, ktorý bol navrhnutý pre Distributed Computing Environment (DCE).
- **Protokol RDP** – deteguje a blokuje rôzne zraniteľnosti (CVE) v protokole RDP (pozri popis vyššie v tejto kapitole).
- **Detekcia útoku ARP Poisoning** – detekcia útokov typu ARP poisoning, ktoré zapríčiňujú útoky typu „man-in-the-middle“ a detekcia tzv. sniffingu na sieťovom prepínači. Protokol ARP (Address Resolution Protocol) je sieťovými aplikáciami alebo zariadeniami využívaný na zistenie Ethernet adresy.
- **Detekcia útoku skenovaním portov TCP/UDP** – zabraňuje útokom softvéru, ktorý sa pokúša nájsť otvorené porty hostiteľského zariadenia posielaním požiadaviek na určitý rozsah adries portov za účelom nájdenia aktívneho portu, ktorý je možné zneužiť na napadnutie systému. Viac o tomto type útoku sa môžete dočítať v slovníku pojmov.
- **Blokovať nebezpečnú adresu po detekcii útoku** – ak je zistený útok z určitej IP adresy, pridá sa na blacklist a všetka komunikácia z nej bude na určitý čas blokovaná. Prostredníctvom nastavenia **Obdobie uchovávania na blackliste** môžete určiť, ako dlho bude adresa po zachytení útoku blokovaná.
- **Upozorniť na detekciu útoku** – pri zachytení útoku program zobrazí upozornenie v pravom dolnom rohu obrazovky v oblasti oznámení systému Windows.
- **Zobraziť upozornenie pri pokusoch o zneužitie bezpečnostných dier** – program zobrazí upozornenie, ak bude zachytený útok na bezpečnostné diery alebo pokus o preniknutie do systému týmto spôsobom.

Kontrola paketov

Analýza paketov, ktorá filtruje dáta prenášané v sieti.

- **Povoliť prichádzajúce spojenie k správcovským zdieľaným položkám cez SMB protokol** – správcovské zdieľané položky (admin shares) sú predvolené zdieľané položky na sieti, ktoré zdieľajú oddiely pevného disku (*C$*, *D$* atď.) spolu so systémovým priečinkom (*ADMIN$*). Zakázanie prístupu k správcovským zdieľaným

položkám výrazne znižuje bezpečnostné riziká. Napríklad červ Conficker vykonáva slovníkové (dictionary) útoky v snahe získať prístup k týmto položkám.

- **Zakázať staré (nepodporované) SMB dialekty** – zakáže SMB reláciu so starým dialektom SMB, ktorý nepodporuje IDS. Najnovšie operačné systémy Windows podporujú staré dialekty SMB kvôli spätnej kompatibilite so staršími operačnými systémami, ako napríklad Windows 95. Útočník môže použiť starší dialekt SMB s úmyslom vyhnúť sa kontrole paketov. Zakážte staré SMB dialekty, ak váš počítač nepotrebuje zdieľať súbory so staršími verziami operačného systému Windows.

- **Zakázať zabezpečenie SMB bez bezpečnostných rozšírení** – bezpečnostné rozšírenia môžu byť použité počas nadväzovania SMB relácie pre zaistenie bezpečnejšieho mechanizmu autentifikácie ako v prípade LAN Manager Challenge/Response (LM). Schéma LM je považovaná za slabú a neodporúča sa ju používať.

- **Zakázať otvorenie spustiteľného súboru na serveroch mimo dôveryhodnej zóny cez SMB protokol** – zabraňuje komunikácii v prípade, že sa používateľ snaží otvoriť spustiteľný súbor (.exe, .dll) zo zdieľaného priečinku na serveri, ktorý nie je v dôveryhodnej zóne Firewallu. Kopírovanie spustiteľných súborov z dôveryhodných zdrojov je v poriadku. Táto funkcionalita by však mala obmedziť nebezpečenstvo otvorenia spustiteľného súboru zo škodlivých serverov.

- **Zakázať NTLM overenie cez SMB protokol pri pripojení na server v/mimo dôveryhodnej zóny** – protokoly používajúce autentifikačnú schému NTLM (obe verzie) sú ohrozené útokmi, ktorých cieľom je preposielanie prihlasovacích údajov (v prípade SMB protokolu známe ako SMB Relay útoky). Zakázaním autentifikácie NTLM so servermi mimo dôveryhodnej zóny sa zníži riziko preposlania prihlasovacích údajov škodlivým serverom mimo dôveryhodnej zóny. Tiež môžete zakázať aj autentifikáciu NTLM so servermi v dôveryhodnej zóne.

- **Povoliť komunikáciu so službou Security Account Manager (Správca zabezpečenia kont)** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-SAMR].

- **Povoliť komunikáciu so službou Local Security Authority (Lokálna autorita zabezpečenia)** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-LSAD] a [MS-LSAT].

- **Povoliť komunikáciu so službou Remote Registry (Vzdialená databáza Registry)** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-RRP].

- **Povoliť komunikáciu so službou Service Control Manager (Správca riadenia služieb)** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-SCMR].

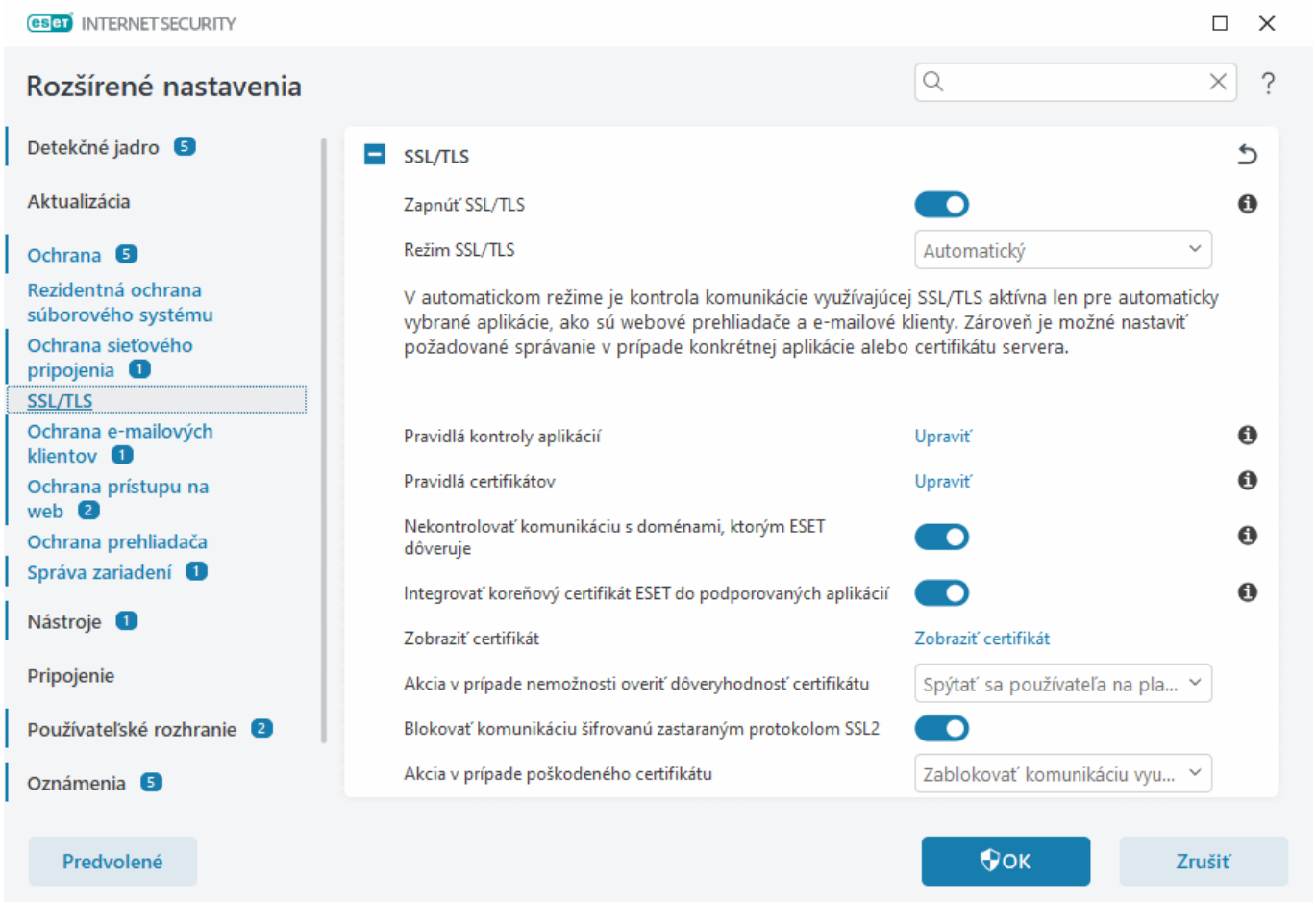
- **Povoliť komunikáciu so službou Server** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-SRVS].

- **Povoliť komunikáciu s ostatnými službami** – ostatné MSRPC služby. MSRPC je implementáciou DCE RPC mechanizmu v systéme Microsoft Windows. MSRPC môže na prenos (ncacn_np) používať pomenované kanály v rámci SMB protokolu. Služby MSRPC poskytujú rozhranie na vzdialenú správu systémov Windows. V systéme MSRPC bolo objavených mnoho zraniteľných miest (tieto zraniteľnosti zneužíva napr. červ Conficker, červ Sasser atď.). Zakázaním komunikácie so službami MSRPC, ktoré nepotrebujete, predídete mnohým bezpečnostným rizikám (ako napríklad vzdialené spúšťanie kódu alebo zlyhávanie služieb kvôli útoku).

SSL/TLS

ESET Internet Security dokáže zachytávať komunikačné hrozby, ktoré využívajú protokol SSL. Dostupné sú rôzne režimy filtrovania podľa toho, či certifikát využívaný danou komunikáciou chránenou protokolom SSL je

dôveryhodný, neznámy alebo je v zozname certifikátov, ktoré sú vylúčené z kontroly komunikácie chránenej protokolom SSL. Ak chcete upraviť nastavenia SSL/TLS, otvorte Rozšírené nastavenia > **Ochrana** > **SSL/TLS**.



Zapnúť SSL/TLS – ak je toto nastavenie vypnuté, ESET Internet Security nebude kontrolovať komunikáciu prenášanú cez protokol SSL/TLS.

K dispozícii sú nasledujúce **režimy SSL/TLS**:

Režim filtrovania	Popis
Automatický	Predvolený režim, v ktorom sa kontrolujú len automaticky vybrané aplikácie, ako sú webové prehliadače a e-mailové klienty. Zároveň je možné manuálne nastaviť požadované správanie v prípade konkrétnych aplikácií.
Interaktívny	Pri prístupe k novej webovej stránke chránenej protokolom SSL (s neznámym certifikátom) sa zobrazí okno s možnosťou výberu akcie. Tento režim vám umožňuje vytvoriť zoznam certifikátov/aplikácií využívajúcich SSL, ktoré budú z kontroly vylúčené.
Podľa politík	Vyberte tento režim, ak chcete kontrolovať všetku komunikáciu chránenú protokolom SSL okrem komunikácie chránenej certifikátmi vylúčenými z kontroly. Pri nadviazaní novej komunikácie využívajúcej zatiaľ neznámy certifikát, ktorý je dôveryhodne podpísaný, nebude používateľ upozornený a komunikácia sa bude automaticky filtrovať. Ak používateľ pristupuje na server používajúci nedôveryhodný certifikát, pričom bol tento používateľom označený ako dôveryhodný (zaradený do zoznamu dôveryhodných certifikátov), komunikácia so serverom bude povolená a prenášaný obsah bude filtrovaný.

Pravidlá kontroly aplikácií – umožňuje prispôsobiť správanie programu ESET Internet Security pre konkrétne aplikácie.

Pravidlá certifikátov – umožňuje prispôsobiť správanie programu ESET Internet Security pre konkrétne SSL certifikáty.

Nekontrolovať komunikáciu s doménami, ktorým ESET dôveruje – ak je táto možnosť zapnutá, komunikácia s dôveryhodnými doménami bude vylúčená z kontroly. Dôveryhodnosť domény sa určuje na základe vstavaného whitelistu spravovaného spoločnosťou ESET.

Integrovať koreňový certifikát ESET do podporovaných aplikácií – pre správne fungovanie SSL komunikácie v danom prehliadači/e-mailovom kliente je nevyhnutné, aby do jeho zoznamu známych koreňových certifikátov (vydavateľov) bol pridaný aj certifikát spoločnosti ESET. Povolením tejto možnosti ESET Internet Security zabezpečí automatické pridanie certifikátu ESET SSL Filter CA do známych prehliadačov (napríklad Opera). Do prehliadačov, ktoré používajú ukladací priestor systémových certifikátov, bude certifikát pridaný automaticky. Napríklad Firefox je automaticky nakonfigurovaný tak, aby dôveroval koreňovým autoritám v úložisku systémových certifikátov.

V prípade nepodporovaných prehliadačov môžete certifikát exportovať kliknutím na **Zobraziť certifikát** > **Podrobnosti** > **Kopírovať do súboru** a následne manuálne importovať do prehliadača.

Akcia v prípade nemožnosti overiť dôveryhodnosť certifikátu – v niektorých prípadoch sa dôveryhodnosť certifikátu webovej stránky nedá overiť pomocou úložiska koreňových certifikátov vydaných dôveryhodnými certifikačnými autoritami (TRCA). Môže ísť napríklad o certifikát s uplynutou platnosťou, nedôveryhodný certifikát, certifikát neplatný pre konkrétnu doménu alebo podpis, ktorý je možné overiť, ale certifikát ním nie je správne podpísaný. Legitímne webové stránky vždy používajú dôveryhodné certifikáty. Ak stránka takýto certifikát nemá, môže to znamenať, že útočník dešifruje vašu komunikáciu alebo má stránka technické problémy.

Ak je označená možnosť **Spýtať sa používateľa na platnosť certifikátu** (predvolené nastavenie), budete v prípade nadviazania šifrovanej komunikácie vyzvaný na výber akcie, ktorá sa má vykonať. Zobrazí sa okno, kde je možné označiť daný certifikát ako dôveryhodný alebo ho vylúčiť z kontroly dôveryhodnosti. V prípade, že certifikát nie je v zozname TRCA, okno je červené. V opačnom prípade je okno zelené.

Ak zvolíte možnosť **Zablokovať komunikáciu využívajúcu daný certifikát**, komunikácia s webovou stránkou využívajúcou nedôveryhodný certifikát sa vždy zablokuje.

Blokovať komunikáciu šifrovanú zastaraným protokolom SSL2 – komunikácia využívajúca staršiu verziu protokolu SSL sa bude automaticky blokovať.

Akcia v prípade poškodeného certifikátu – poškodený certifikát znamená, že certifikát používa formát, ktorý program ESET Internet Security nevie rozpoznať, alebo už bol prijatý v poškodenom stave (napríklad bol prepísaný náhodnými údajmi). V tomto prípade odporúčame ponechať označenú možnosť **Zablokovať komunikáciu využívajúcu daný certifikát**. Ak je zvolená možnosť **Spýtať sa používateľa na platnosť certifikátu**, pri nadviazaní šifrovanej komunikácie bude používateľ vyzvaný na výber akcie.

Ilustrované príklady

Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:

- Oznámenia týkajúce sa certifikátov v produktoch ESET určených pre domácnosti (Windows)
- Pri návšteve webovej stránky sa zobrazilo upozornenie na nedôveryhodný certifikát

Pravidlá kontroly aplikácií

Pravidlá kontroly aplikácií môžete použiť na prispôsobenie správania programu ESET Internet Security pre konkrétne aplikácie, ako aj na zapamätanie akcií zvolených počas **Interaktívneho režimu** nastaveného v sekcii

Režim SSL/TLS. Zoznam pravidiel si môžete zobraziť a upravovať v sekcii Rozšírené nastavenia > **Ochrana** > **SSL/TLS** > **Pravidlá kontroly aplikácií** po kliknutí na tlačidlo **Upraviť**.

Okno **Pravidlá kontroly aplikácií** obsahuje:

Stĺpce

Aplikácia – vyberte spustiteľný súbor zo stromovej štruktúry, kliknutím na **...** alebo cestu k súboru aplikácie zadajte manuálne.

Akcia kontroly – vyberte možnosť **Kontrolovať** alebo **Ignorovať** ako akciu kontroly pre komunikáciu. K dispozícii je aj možnosť **Automaticky**, ktorá spustí kontrolu v automatickom režime a zobrazí výzvu na výber akcie v interaktívnom režime. Ak vyberiete možnosť **Spýtať sa**, pri každej komunikácii sa zobrazí okno s výberom akcie.

Ovládacie prvky

Pridať – pridajte filtrovanú aplikáciu.

Upraviť – označte aplikáciu, ktorú chcete konfigurovať, a kliknite na **Upraviť**.

Odstrániť – označte aplikáciu, ktorú chcete odstrániť, a kliknite na **Odstrániť**.

Import/Export – importujte aplikácie zo súboru alebo si do súboru uložte aktuálny zoznam aplikácií.

OK/Zrušiť – kliknite na **OK** pre uloženie zmien v nastavení alebo na **Zrušiť**, ak chcete okno zatvoriť bez uloženia vykonaných zmien.

Pravidlá certifikátov

Pravidlá certifikátov môžete použiť na prispôsobenie správania programu ESET Internet Security pre konkrétne SSL certifikáty, ako aj na zapamätanie akcií zvolených počas **Interaktívneho režimu** nastaveného v sekcii **Režim SSL/TLS**. Zoznam pravidiel si môžete zobraziť a upravovať v sekcii Rozšírené nastavenia > **Ochrana** > **SSL/TLS** > **Pravidlá certifikátov** po kliknutí na tlačidlo **Upraviť**.

Okno **Pravidlá certifikátov** obsahuje:

Stĺpce

Názov – názov certifikátu.

Vydavateľ certifikátu – meno autora certifikátu.

Predmet certifikátu – identifikuje entitu asociovanú s verejným kľúčom uloženým v poli predmet verejného kľúča.

Prístup – zvoľte **Povoliť** alebo **Blokovať** ako **Akciu prístupu** na povolenie alebo blokovanie komunikácie zabezpečenej certifikátom bez ohľadu na jeho dôveryhodnosť. Vyberte možnosť **Automaticky** na povolenie dôveryhodných certifikátov a pýtanie sa na nedôveryhodné certifikáty. Ak vyberiete možnosť **Spýtať sa**, pri každej komunikácii sa zobrazí okno s výberom akcie.

Kontrolovať – vyberte **Kontrolovať** alebo **Ignorovať** ako **Akciu kontroly** podľa toho, či chcete kontrolovať alebo

ignorovať komunikáciu zabezpečenú týmto certifikátom. K dispozícii je aj možnosť **Automaticky**, ktorá spustí kontrolu v automatickom režime a zobrazí výzvu na výber akcie v interaktívnom režime. Ak vyberiete možnosť **Spýtať sa**, pri každej komunikácii sa zobrazí okno s výberom akcie.

Ovládacie prvky

Pridať – pridanie certifikátu a nastavenie akcie prístupu a kontroly daného certifikátu.

Upraviť – označte certifikát, ktorý chcete konfigurovať, a kliknite na **Upraviť**.

Odstrániť – označte certifikát a kliknite na **Odstrániť** pre jeho odstránenie.

OK/Zrušiť – kliknite na **OK** pre uloženie zmien v nastavení alebo na **Zrušiť**, ak chcete okno zatvoriť bez uloženia vykonaných zmien.

Šifrovaná sieťová komunikácia

Ak je počítač nastavený na kontrolu SSL/TLS, v nasledujúcich dvoch situáciách sa zobrazí dialógové okno s výzvou vybrať si želanú akciu:

Prvá situácia nastáva, ak stránka používa neoveriteľný alebo neplatný certifikát a program ESET Internet Security je v takýchto prípadoch nastavený pýtať sa používateľa (predvolene len pri neoveriteľných certifikátoch). Zobrazí sa dialógové okno s možnosťami **Blokovať** alebo **Povoliť** spojenie. Certifikát je považovaný za nedôveryhodný, ak sa nenachádza v úložisku koreňových certifikátov vydaných dôveryhodnými certifikačnými autoritami (Trusted Root Certification Authorities store – TRCA).

Druhá situácia nastáva, ak je **Režim SSL/TLS** nastavený na **Interaktívny režim**. V takomto prípade sa používateľovi zobrazí dialógové okno pre každú webovú stránku s možnosťami **Kontrolovať** alebo **Ignorovať** danú sieťovú komunikáciu. Niektoré aplikácie kontrolujú, či ich SSL komunikácia nie je zmenená alebo sledovaná inou aplikáciou, v takomto prípade musí ESET Internet Security **ignorovať** komunikáciu týchto aplikácií, aby nedošlo k obmedzeniu ich funkčnosti.

> **Ilustrované príklady**
> Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
> - Oznámenia týkajúce sa certifikátov v produktoch ESET určených pre domácnosti (Windows)
> - Pri návšteve webovej stránky sa zobrazilo upozornenie na nedôveryhodný certifikát

V oboch hore uvedených prípadoch môže používateľ označiť, aby si program zapamätal zvolenú akciu. Zapamätané akcie sú uložené v pravidlách certifikátov.

Ochrana e□mailových klientov

Ak chcete upraviť konfiguráciu ochrany e□mailových klientov, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana e□mailových klientov** a vyberte si z nasledujúcich možností:

- Ochrana prenosu e-mailov
- Ochrana e□mailových schránok

- Správa zoznamov adries
- ThreatSense

Ochrana prenosu e-mailov

IMAP(S) a POP3(S) sú najrozšírenejšie protokoly slúžiace na príjem e□mailovej komunikácie prostredníctvom e□mailového klienta. IMAP (Internet Message Access Protocol) je internetový protokol na načítavanie e□mailov. V porovnaní s protokolom POP3 má niekoľko výhod, napríklad umožňuje viacerým klientom naraz pripojiť sa k tej istej e-mailovej schránke a zachovávať informácie o stave správy (napríklad, či správa bola prečítaná, odstránená alebo či na ňu bolo odpovedané). Modul zabezpečujúci kontrolu sa zavádza pri štarte operačného systému a počas celej doby je zavedený v pamäti.

ESET Internet Security zabezpečuje ochranu týchto protokolov nezávisle od používaného e□mailového klienta a bez potreby zmeny jeho konfigurácie. Predvolene je všetka komunikácia prostredníctvom protokolov POP3 a IMAP kontrolovaná, bez ohľadu na predvolené čísla portov POP3/IMAP.
Protokol MAPI nie je kontrolovaný. Komunikáciu s Microsoft Exchange Serverom je však možné kontrolovať prostredníctvom modulu integrácie v e□mailových klientoch, ako je Microsoft Outlook.

> ESET Internet Security podporuje aj kontrolu komunikácie cez protokoly IMAPS (585, 993) a POP3S (995). Pri tejto komunikácii sú prenášané údaje medzi serverom a klientom zašifrované. ESET Internet Security kontroluje komunikáciu využívajúcu protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Šifrovaná komunikácia je predvolene kontrolovaná. Nastavenia skenera zobrazíte otvorením položky Rozšírené nastavenia > **Ochrana** > SSL/TLS.

Ak chcete nakonfigurovať ochranu prenosu e□mailov, prejdite do sekcie Rozšírené nastavenie > **Ochrana** > **Ochrana e□mailových klientov** > **Ochrana prenosu e□mailov**.

Zapnúť ochranu prenosu e□mailov – ak je táto možnosť povolená, ESET Internet Security bude kontrolovať prenos e□mailov.

Kliknutím na prepínacie tlačidlo vedľa nasledujúcich možností môžete zvoliť, ktoré protokoly na prenos e□mailov sa majú kontrolovať (v predvolenom nastavení sú vybrané všetky protokoly):

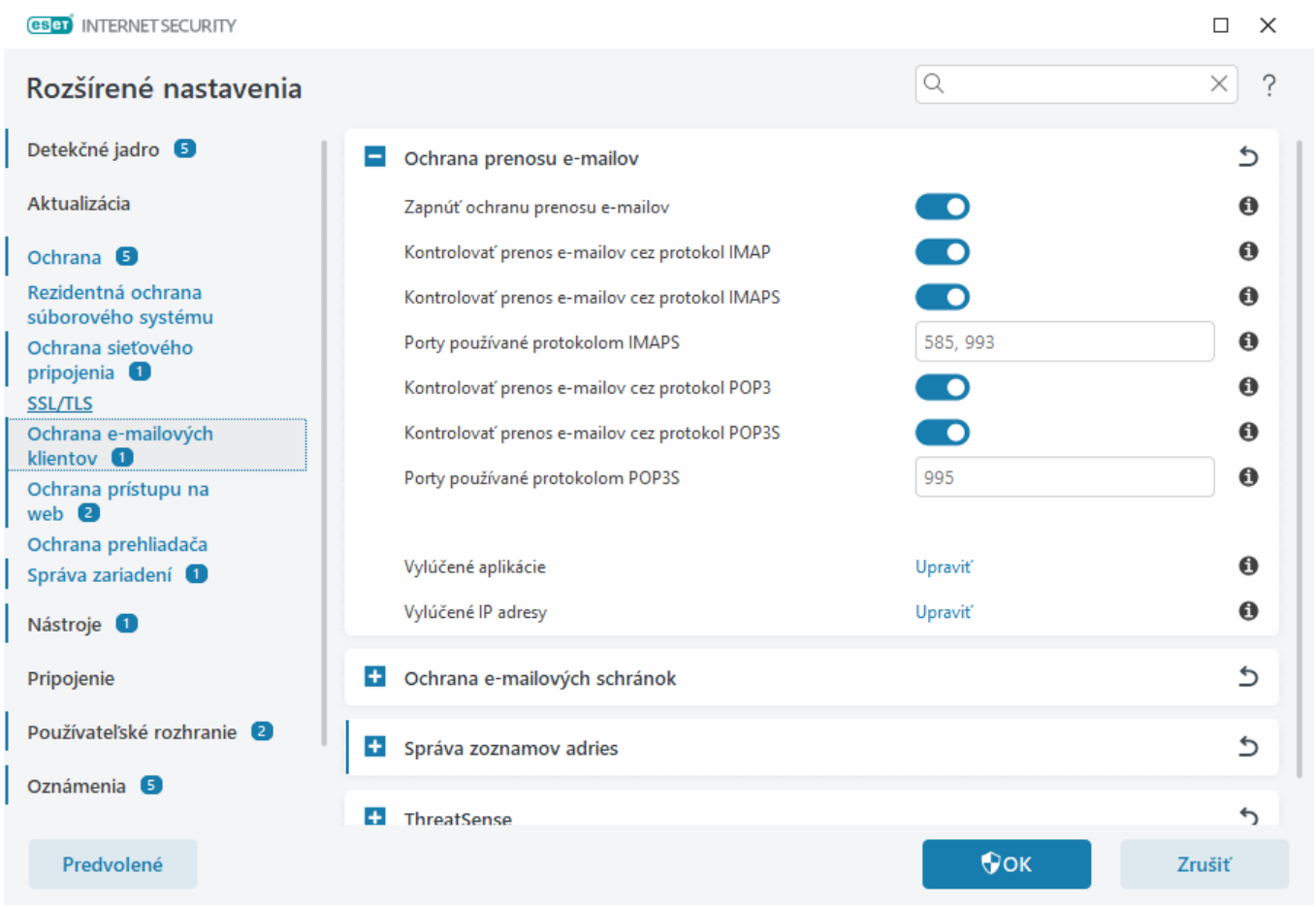
- **Kontrolovať prenos e□mailov cez protokol IMAP**
- **Kontrolovať prenos e□mailov cez protokol IMAPS**
- **Kontrolovať prenos e□mailov cez protokol POP3**
- **Kontrolovať prenos e□mailov cez protokol POP3S**

V predvolenom nastavení bude ESET Internet Security kontrolovať komunikáciu prenášanú cez protokoly IMAPS a POP3S na štandardných portoch. Ak chcete pridať vlastné porty pre protokoly IMAPS a POP3S, pridajte ich do textového poľa **Porty používané protokolom IMAPS** alebo **Porty používané protokolom POP3S**. Čísla portov sa oddeľujú čiarkou.

Vylúčené aplikácie – umožňuje vylúčiť konkrétne aplikácie z kontroly v rámci Ochrany prenosu e□mailov. Takéto vylúčenie môže byť užitočné v prípade, keď ochrana prístupu na web spôsobuje problémy s kompatibilitou.

Vylúčené IP adresy – umožňuje vylúčiť konkrétne vzdialené adresy z kontroly v rámci Ochrany prenosu e□mailov. Takéto vylúčenie môže byť užitočné v prípade, keď ochrana prístupu na web spôsobuje problémy

s kompatibilitou.



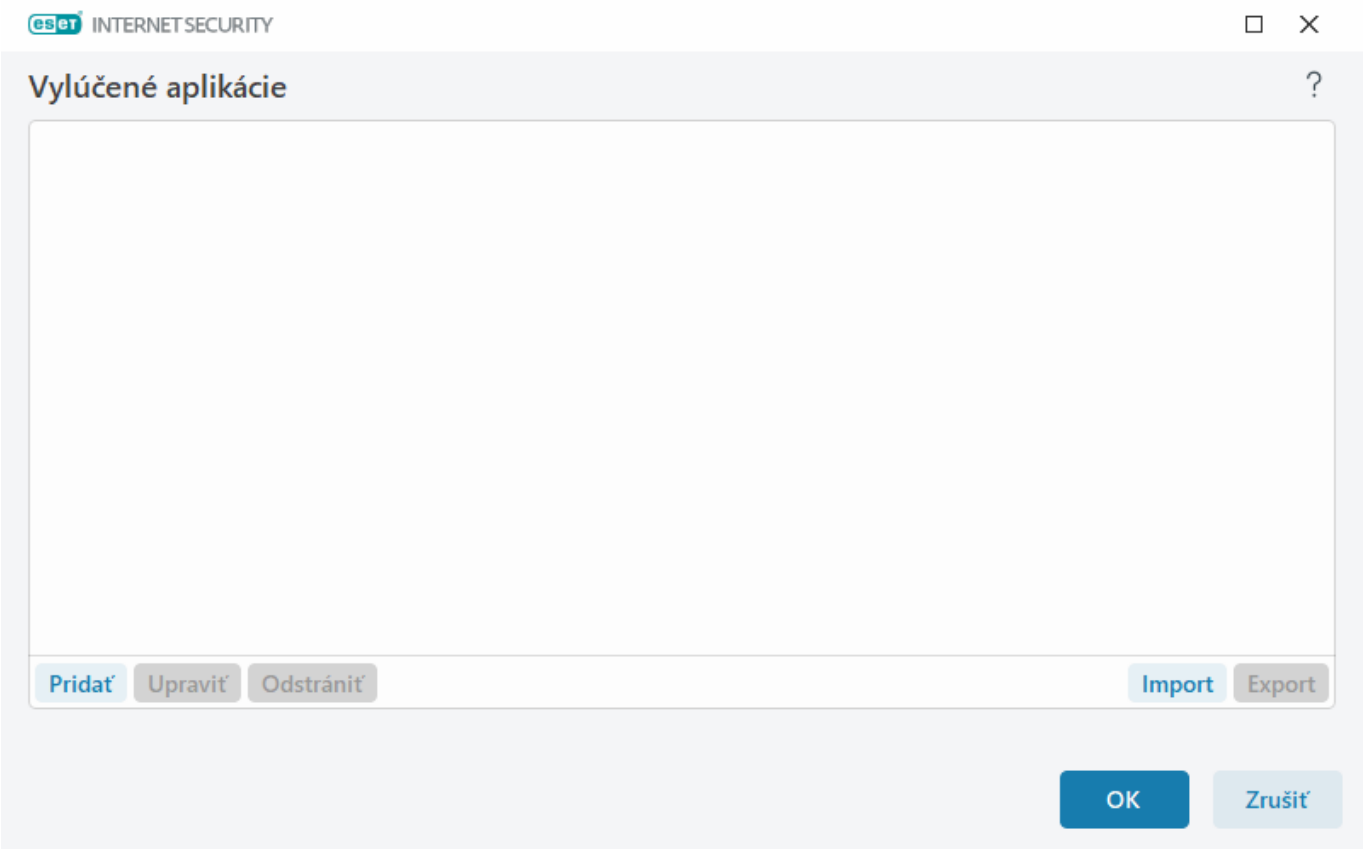
Vylúčené aplikácie

Ak nechcete kontrolovať komunikáciu pre konkrétne aplikácie, pridajte ich do zoznamu vylúčení. HTTP(S)/POP3(S)/IMAP(S) komunikácia označených aplikácií nebude kontrolovaná na prítomnosť škodlivého kódu. Vylúčenie aplikácie z kontroly odporúčame iba v nevyhnutných prípadoch, napríklad ak aplikácia v dôsledku kontroly jej komunikácie nepracuje správne.

Spustené aplikácie a služby sa zobrazia automaticky po kliknutí na tlačidlo **Pridať**. Kliknite na **...** a vyhľadajte aplikáciu, pre ktorú chcete pridať vylúčenie.

Upraviť – umožňuje upravovať zvolené položky v zozname.

Odstrániť – umožňuje odstrániť zvolené položky zo zoznamu.



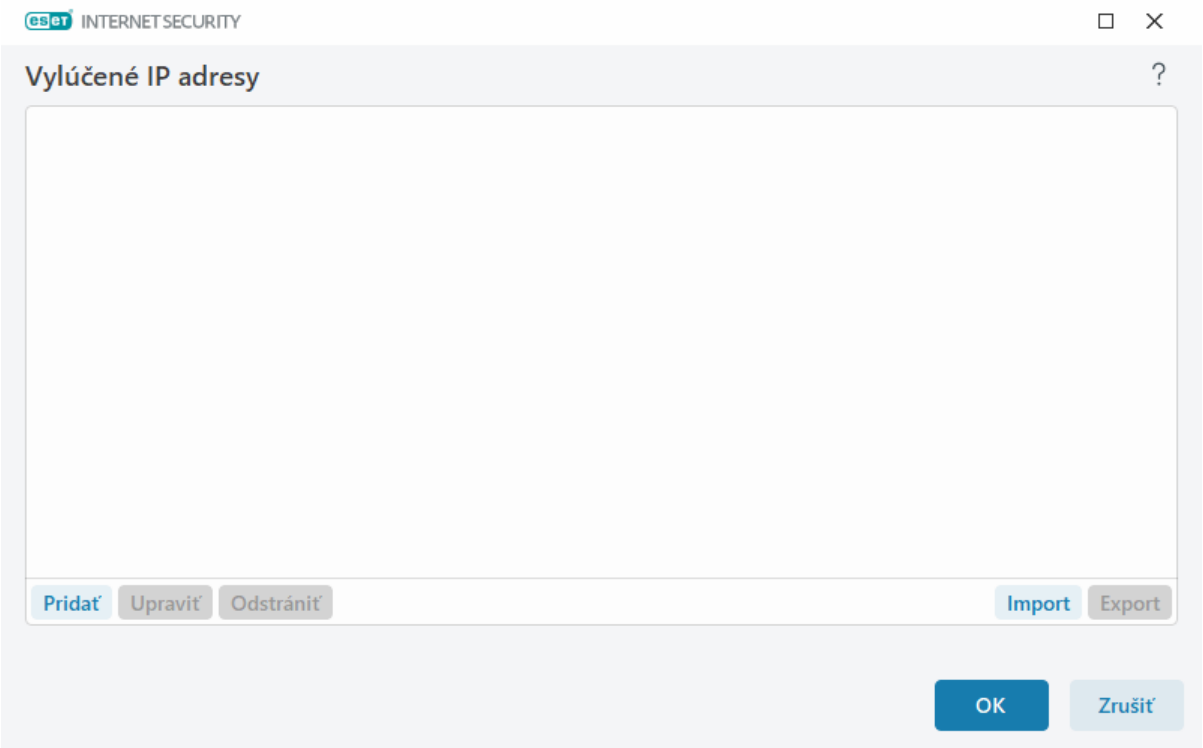
Vylúčené IP adresy

IP adresy uvedené v zozname budú vylúčené z kontroly. Obojstranná HTTP(S)/POP3(S)/IMAP(S) komunikácia označených aplikácií nebude kontrolovaná na prítomnosť škodlivého kódu. Odporúčame používať túto možnosť iba v prípade dôveryhodných IP adries.

Kliknite na **Pridať**, ak chcete vylúčiť vzdialenú IP adresu, rozsah adries alebo podsieť.

Kliknite na **Upraviť**, ak chcete zmeniť vybranú IP adresu.

Kliknite na **Odstrániť**, ak chcete odstrániť označené položky zo zoznamu.



Príklady IP adries

Pridanie IPv4 adresy:

Samostatná adresa – zadanie IP adresy individuálneho počítača (napríklad *192.168.0.10*).

Rozsah adries – zadáva sa začiatočná a koncová IP adresa na stanovenie rozsahu IP adries skupiny počítačov (napr. *192.168.0.1-192.168.0.99*).

Podsieť – skupina počítačov patriacich do určitej podsiete. Zadáva sa IP adresa a maska podsiete. 255.255.255.0 je napríklad sieťová maska pre podsieť 192.168.1.0. Ak chcete vylúčiť celú podsieť, zadajte *192.168.1.0/24*.

Pridanie IPv6 adresy:

Samostatná adresa – zadanie IP adresy individuálneho počítača (napr. *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podsieť – skupina počítačov patriacich do určitej podsiete. Zadáva sa IP adresa a maska podsiete (napr. *2002:c0a8:6301:1::1/64*).

Ochrana e□mailových schránok

Integrácia programu ESET Internet Security s vašou e□mailovou schránkou zlepšuje aktívnu ochranu pred škodlivým kódom v e□mailových správach.

Ak chcete nakonfigurovať ochranu e□mailových schránok, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana e□mailových klientov** > **Ochrana e□mailových schránok**.

Zapnúť e□mailovú ochranu prostredníctvom pluginov klienta – ak je táto možnosť deaktivovaná, ochrana prostredníctvom pluginov e□mailového klienta je vypnutá.

Vyberte, aké e□maily sa majú kontrolovať:

- **Prijaté e-maily**
- **Odoslané e-maily**

- **Prečítané e-maily**
- **Zmenené e-maily**

Odporúčame ponechať možnosť **Zapnúť e□mailovú ochranu prostredníctvom pluginov klienta** aktívnu. V prípade, že integrácia nie je povolená alebo funkčná, bude e□mailová komunikácia stále zabezpečená prostredníctvom Ochrany prenosu e□mailov (IMAP/IMAPS a POP3/POP3S).

Kontrola na prítomnosť spamu

V súčasnosti sa medzi najväčšie problémy e□mailovej komunikácie radí nevyžiadaná pošta – spam. Spam tvorí až 30 % všetkej e□mailovej komunikácie. Antispamová ochrana e□mailových klientov vás pred ním zabezpečí. Zahŕňa kombináciu viacerých bezpečnostných princípov zaisťujúcich špičkové filtrovanie nevyžiadanej pošty. Kľúčovou metódou detekcie spamu je rozpoznať nevyžiadané e□maily prostredníctvom preddefinovaných dôveryhodných (whitelist) a spamových (blacklist) adries.

Hlavným princípom je zachytávanie spamu na základe vlastností e□mailových správ. Prijatá správa je preverená podľa základných pravidiel (vzorky správ, štatistická heuristika, rozpoznávacie algoritmy a ďalšie jedinečné metódy) a podľa výsledku sa určí, či ide o spam, alebo nie.

Zapnúť antispamovú ochranu e□mailových klientov – ak je táto možnosť povolená, prijaté správy sa budú kontrolovať na prítomnosť spamu.

Používať pokročilú kontrolu spamu – pravidelne sa budú sťahovať dodatočné antispamové dáta, čím sa zlepšia schopnosti a výsledky antispamovej kontroly.

Zapisovať hodnotenie antispamovej ochrany do protokolu – antispamové jadro ESET Internet Security priraďuje každej skontrolovanej správe skóre. Správa bude zaznamenaná v protokole antispamovej ochrany (hlavné okno programu > **Nástroje** > **Protokoly** > **Antispamová ochrana e□mailových klientov**).

- **Žiadne** – hodnotenie antispamovej kontroly nebude do protokolu zaznamenané.
- **Preklasifikované a označené ako SPAM** – zvoľte túto možnosť, ak si želáte zapisovať do protokolu spamové hodnotenie pre správy označené ako SPAM.
- **Všetko** – všetky správy budú mať zaznamenané spamové hodnotenie.

Po kliknutí na správu v priečinku nevyžiadanej pošty môžete vybrať možnosť **Preklasifikovať vybrané správy ako NIE SPAM** a správa bude presunutá do priečinka prijatých správ. Po kliknutí na správu v priečinku prijatých správ môžete vybrať možnosť **Preklasifikovať správy ako SPAM** a správa bude presunutá do priečinka nevyžiadanej pošty. Môžete označiť viacero správ a vykonať akciu pre všetky správy naraz.

Optimalizovať spracovanie príloh – ak je optimalizácia vypnutá, všetky prílohy sa budú kontrolovať okamžite. Môže dôjsť k spomaleniu výkonu e□mailového klienta.

Integrácie – umožňuje integrovať ochranu e□mailových schránok do vášho e□mailového klienta. Ďalšie informácie nájdete v kapitole Integrácie.

Reakcia – umožňuje prispôsobiť spracúvanie nevyžiadaných správ (spamu). Viac informácií nájdete v kapitole Reakcia.

Integrácie

Integrácia programu ESET Internet Security s vaším e□mailovým klientom zlepšuje aktívnu ochranu pred škodlivým kódom v e□mailových správach. V prípade, že je daný e□mailový klient podporovaný, môžete povoliť jeho integráciu v programe ESET Internet Security. Pri integrácii dochádza k vloženiu panela nástrojov ESET Internet Security priamo do e□mailového klienta, čo prispieva k účinnejšej kontrole e□mailových správ. Ak chcete upraviť nastavenia integrácie, otvorte Rozšírené nastavenia > **Ochrana** > **Ochrana e□mailových klientov** > **Ochrana e□mailových schránok** > **Integrácia**.

Povoliť integráciu s Microsoft Outlook – Microsoft Outlook je v súčasnosti jediný podporovaný e□mailový klient. E□mailová ochrana funguje prostredníctvom pluginu. Hlavnou výhodou je nezávislosť od použitého protokolu. V prípade šifrovanej komunikácie program takto od e-mailového klienta dostáva na kontrolu už dešifrované správy. Kompletný zoznam podporovaných verzií programu Microsoft Outlook nájdete v článku Databázy znalostí spoločnosti ESET.

Pokročilé spracovanie e□mailovými klientmi – spracúvanie ďalších udalostí Outlook Messaging API (MAPI): objekt upravený (`fnevObjectModified`) a objekt vytvorený (`fnevObjectCreated`). Vypnite túto možnosť, ak ste zaznamenali spomalenie systému pri práci s e□mailovým klientom.

Panel nástrojov programu Microsoft Outlook

Ochrana programu Microsoft Outlook funguje prostredníctvom pluginu. Po nainštalovaní produktu ESET Internet Security sa do programu Microsoft Outlook pridá panel nástrojov pozostávajúci z možností antivírusovej ochrany a antispamovej ochrany e-mailových klientov:

Spam – vybrané správy označí ako spam. Po označení sa pošle „odtlačok“ správy na centrálny server s databázou charakteristík nevyžiadanej pošty. V prípade, že rovnaký „odtlačok“ pošle väčší počet ľudí, bude sa takáto správa v budúcnosti vyhodnocovať ako spam.

Nie spam – vybrané správy označí ako „nie spam“.

Spamová adresa (blokované, zoznam spamových adries) – pridá adresu odosielateľa vybraných správ do zoznamu adries ako blokovanú. Správy z týchto adries budú automaticky označované ako spam.

> ⚠ Vyhýbajte sa spoofingu – pri odosielaní nevyžiadanej pošty sa využíva tzv. spoofing, keď sa skutočný odosielateľ maskuje za inú e-mailovú adresu.

Dôveryhodná adresa (povolené, zoznam dôveryhodných adries) – pridá adresu odosielateľa vybraných správ do zoznamu adries ako povolenú. Správy z povolených adries nebudú nikdy automaticky označované ako spam.

ESET Internet Security – dvojitým kliknutím na ikonu otvoríte hlavné okno programu ESET Internet Security.

Opätovná kontrola správ – umožní vám manuálne spustiť kontrolu e-mailových správ. Môžete vybrať správy, ktoré majú byť skontrolované, a môžete tiež aktivovať opätovné prekontrolovanie prijatých e□mailov. Pre viac informácií si prečítajte kapitolu Ochrana e□mailových schránok.

Nastavenie skenera – zobrazí možnosti nastavenia Ochrany e□mailových schránok.

Nastavenia antispamu – zobrazí možnosti nastavenia Ochrany e□mailových schránok.

Zoznamy adries – otvorí okno Správa zoznamov adries, ktoré vám umožní prístup k zoznamom vylúčených, dôveryhodných a spamových adries.

Potvrdzovacie dialógové okno

Dialógové okno s možnosťou potvrdenia alebo zamietnutia zvolenej akcie slúži na overenie, či chce používateľ akciu skutočne vykonať. Môžete tak predísť akciám, ktoré ste nastavili nedopatrením.

Zároveň máte možnosť zobrazovanie potvrdzovacích správ úplne vypnúť.

Opätovná kontrola správ

Integrovaný ovládací panel produktu ESET Internet Security v e-mailovom kliente umožňuje používateľom nastaviť rôzne druhy kontroly e-mailových správ. Prostredníctvom možnosti **Opätovná kontrola správ** je možné zvoliť dva režimy kontroly:

Všetky správy v aktuálnom priečinku – budú kontrolované všetky správy v priečinku, ktorý je aktuálne zobrazený.

Iba vybrané správy – kontrole budú podliehať len správy, ktoré používateľ priamo označil.

Položka **Kontrolovať aj správy, ktoré už boli prekontrolované** zabezpečí, aby sa do kontroly zahrnuli aj správy, ktoré už boli v minulosti prekontrolované.

Reakcia

Na základe výsledkov kontroly správ môže ESET Internet Security presunúť skontrolované správy alebo pridať vlastný text do predmetu správy. Tieto nastavenia môžete nakonfigurovať v sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana e□mailových klientov** > **Ochrana e□mailových schránok** > **Reakcia**.

Antispamová ochrana e□mailových klientov v programe ESET Internet Security vám umožňuje nakonfigurovať tieto parametre správ:

Pridávať text do predmetu e-mailu – umožňuje pridať vlastný text do predmetu e-mailovej správy klasifikovanej ako spam. Predvolený **text** je „[SPAM]“.

Presúvať do spamového priečinka – ak je táto možnosť zapnutá, spamové správy budú presunuté do predvoleného priečinka pre nevyžiadanú poštu a správy preklasifikované ako „nie spam“ budú presunuté do priečinka prijatých správ. Keď na e-mailovú správu kliknete pravým tlačidlom myši a z kontextového menu označíte možnosť ESET Internet Security, zobrazia sa vám dostupné možnosti pre danú správu.

Presúvať do vlastného priečinka – ak je táto možnosť zapnutá, spamové správy sa presunú do priečinka špecifikovaného nižšie.

Priečinok – priečinok, do ktorého bude program presúvať správy, v ktorých boli zachytené infiltrácie.

ESET Internet Security sa predvolene pokúsi infikovanú správu vyliečiť. Ak sa to nepodarí, môžete vybrať **akciu, ktorá sa má vykonať, ak nie je možné liečenie**:

• **Žiadna akcia** – ak je táto možnosť povolená, program nájde e□mailové správy s infikovanými prílohami, no nevykoná s nimi žiadnu akciu.

• **Odstrániť email** – program upozorní používateľa na infikované prílohy a odstráni celú e-mailovú správu.

• **Presunúť e-mail do priečinka vymazaných správ** – program bude automaticky presúvať infikované správy do priečinka Vymazané správy.

• **Presunúť e-mail do priečinka** (predvolená akcia) – program bude automaticky presúvať infikované správy do zadaného priečinka.

Priečinok – priečinok, do ktorého bude program presúvať e□mailové správy, v ktorých boli zachytené infiltrácie.

Spamové správy označovať ako prečítané – umožní automatické označovanie spamových správ ako prečítané. Pomôže vám to sústrediť sa na legitímne neprečítané správy.

Preklasifikované správy označovať ako neprečítané – správy pôvodne označené ako spam, no neskôr prehodnotené a označené ako legitímne, sa zobrazia ako neprečítané správy.

Program umožňuje pridávať do skontrolovaných e□mailov oznámenie s informáciami o výsledku kontroly. Používateľ môže zvoliť, či chce **Pridávať poznámku do prijatých a prečítaných e□mailov** alebo tiež **Pridávať poznámku do odosielaných e□mailov**. Na tieto poznámky o výsledku kontroly sa nemožno úplne spoliehať, nakoľko nemusia byť doplnené do problematických HTML správ a taktiež môžu byť sfalšované malvérom. Pridávanie textových poznámok možno nastaviť zvlášť pre prijaté a prečítané e□maily a zvlášť pre odosielané e□maily, prípadne pre všetky e□maily. K dispozícii sú nasledujúce možnosti:

• **Nikdy** – do správ nebudú pridávané žiadne poznámky s informáciou o výsledku kontroly.

• **Pri zachytení detekcie** – program bude pridávať poznámky len do infikovaných správ (predvolené nastavenie).

• **Do všetkých skontrolovaných e□mailov** – program bude pridávať poznámky do všetkých skontrolovaných e□mailov.

Upraviť predmet prijatých a čítaných e□mailov/Upraviť predmet odosielaných e□mailov – zapnutím tejto možnosti pridáte do správy vlastný text špecifikovaný nižšie.

Text pridaný do predmetu e□mailu – túto šablónu upravte v prípade, ak chcete zmeniť formát predpony predmetu infikovaného e□mailu. Táto funkcia nahradí predmet správy „Ahoj“ nasledujúcim formátom: „[detekcia %DETECTIONNAME%] Ahoj“. Premenná %DETECTIONNAME% predstavuje detekciu.

Správa zoznamov adries

Antispamová ochrana e-mailových klientov programu ESET Internet Security umožňuje nastaviť rôzne parametre pre prácu so zoznamami adries. Ak chcete nakonfigurovať zoznamy adries, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana e□mailových klientov** > **Správa zoznamov adries**.

Povoliť používateľský zoznam adries – zapnite túto možnosť, ak chcete aktivovať zoznam adries používateľa.

Používateľský zoznam adries – zoznam e□mailových adries, kde môžete pridávať, upravovať alebo mazať adresy a definovať pravidlá antispamu. Pravidlá v tomto zozname sa budú vzťahovať na aktuálneho používateľa.

Povoliť globálny zoznam adries – zapnite túto možnosť, ak chcete aktivovať používanie globálneho zoznamu adries, ktorý je spoločný pre všetkých používateľov zariadenia.

Globálny zoznam adries – zoznam e□mailových adries, kde môžete pridávať, upravovať alebo mazať adresy a definovať pravidlá antispamu. Pravidlá v tomto zozname sa budú vzťahovať na všetkých používateľov.

Automatické povolenie a pridávanie adries do používateľského zoznamu

Považovať adresy zo zoznamu kontaktov za dôveryhodné – adresy z vášho zoznamu kontaktov budú považované za dôveryhodné aj bez ich pridania do používateľského zoznamu adries.

Pridávať adresy príjemcov z odosielaných správ – adresy príjemcov z odosielaných správ budú pridané do používateľského zoznamu adries ako povolené.

Pridávať adresy odosielateľov zo správ preklasifikovaných ako NIE SPAM – adresy odosielateľov správ, ktoré boli preklasifikované ako NIE SPAM, budú pridané do používateľského zoznamu adries ako povolené.

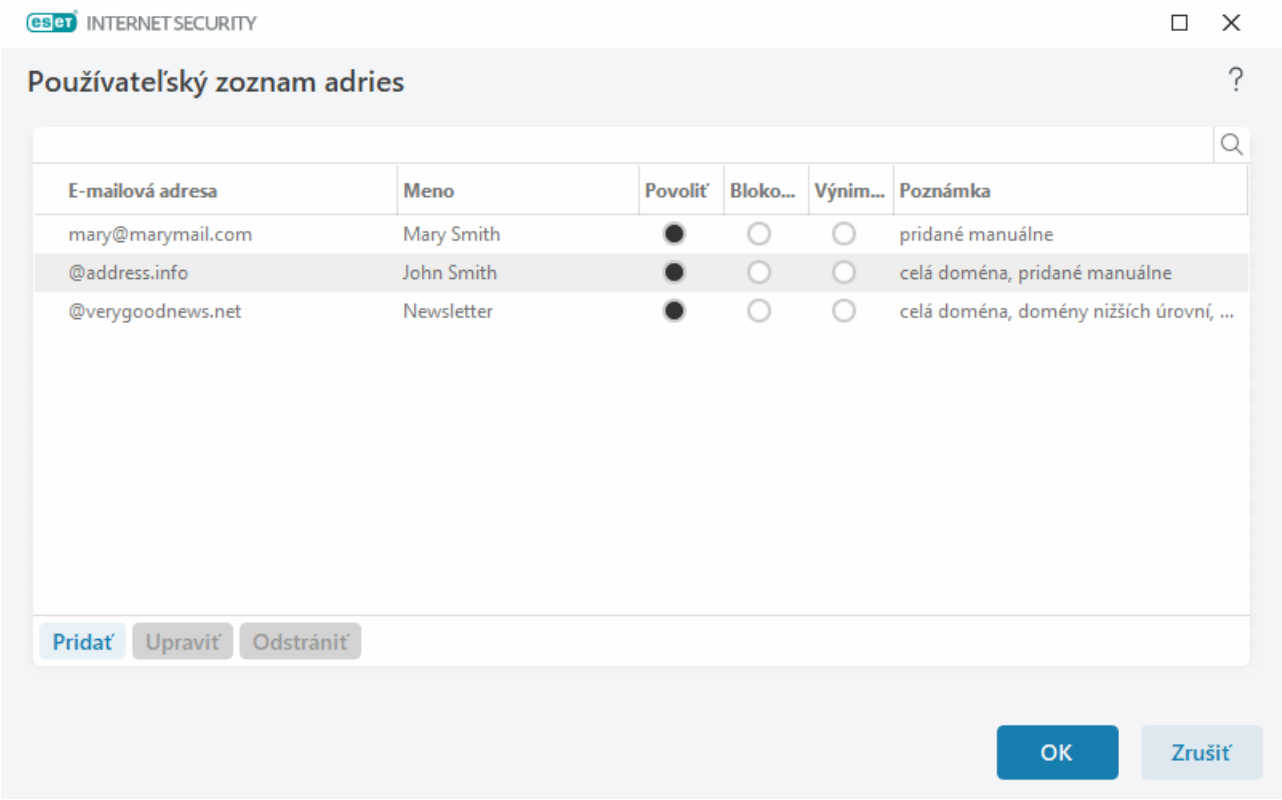
Automatické pridávanie adries do používateľského zoznamu v podobe výnimiek

Pridávať adresy z vlastných účtov – e□mailové adresy z existujúcich účtov e□mailového klienta budú pridané do používateľského zoznamu adries ako výnimka.

Zoznamy adries

Na zabezpečenie ochrany pred nevyžiadanými e□mailmi vám ESET Internet Security umožňuje triediť e□mailové adresy do zoznamov adries.

Ak chcete upravovať zoznamy adries, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana e□mailových klientov** > **Správa zoznamov adries** a kliknite na možnosť **Upraviť** vedľa popisu **Používateľský zoznam adries** alebo **Globálny zoznam adries**.



Stĺpce

E-mailová adresa – adresa, na ktorú sa bude pravidlo vzťahovať. Zástupné znaky nie sú podporované.

Názov – vlastný názov pravidla.

Povoliť/Blokovať/Výnimka – prepínače umožňujú nastaviť, aká akcia sa má vykonať pre danú e□mailovú adresu (kliknutím na prepínač vo vybranom stĺpci viete rýchlo zmeniť akciu):

- **Povoliť** – e□mailové adresy, ktoré považujete za bezpečné a z ktorých chcete prijímať e□maily.
- **Blokovať** – e□mailové adresy, ktoré považujete za nebezpečné/spamové a z ktorých nechcete dostávať e□maily.
- **Výnimka** – e□mailové adresy, ktoré môžu byť falošné a použité na rozposielanie spamu a ktoré majú byť vždy kontrolované na prítomnosť spamu.

Poznámka – informácia o tom, ako bolo pravidlo vytvorené a či sa vzťahuje na celú doménu/domény nižších úrovní.

Spravovanie adries

- **Pridať** – umožňuje pridať pravidlo pre novú adresu.
- **Upraviť** – umožňuje upraviť existujúce pravidlo.
- **Odstrániť** – umožňuje odstrániť pravidlo zo zoznamu adries.

Pridanie/úprava adresy

Toto okno umožňuje pridať alebo upraviť adresu v Správe zoznamov adries a nastaviť želanú akciu:

E-mailová adresa – adresa, na ktorú sa bude pravidlo vzťahovať.

Názov – vlastný názov pravidla.

Akcia – akcia, ktorá sa má vykonať, ak sa e□mailová adresa daného kontaktu zhoduje s adresou uvedenou v poli **E□mailová adresa**:

- **Povoliť** – e□mailové adresy, ktoré považujete za bezpečné a z ktorých chcete prijímať e□maily.
- **Blokovať** – e□mailové adresy, ktoré považujete za nebezpečné/spamové a z ktorých nechcete dostávať e□maily.
- **Výnimka** – e□mailové adresy, ktoré môžu byť falošné a použité na rozposielanie spamu a ktoré majú byť vždy kontrolované na prítomnosť spamu.

Celá doména – pri zvolení tejto možnosti sa bude pravidlo uplatňovať na celú doménu (teda nielen na konkrétnu adresu zadanú v poli **E□mailová adresa**, ale napríklad na všetky adresy s doménou *adresa.sk*).

Domény nižších úrovní – ak sa e□mailová adresa skladá aj z domén nižších úrovní, je možné označením tejto voľby uplatniť pravidlo aj na takéto adresy (všetky subdomény domény, napr. *adresa.sk* je doména a *moja.adresa.sk* je subdoména).

Výsledok spracovania adries

Pri pridávaní nových adries alebo zmene akcie pre e□mailovú adresu program ESET Internet Security zobrazí správa s upozornením. Obsah v okne upozornenia sa mení v závislosti od akcie, ktorú sa pokúšate vykonať.

Po označení možnosti **Nezobrazovať viac túto správu** sa pri ďalšom pokuse akcia vykoná automaticky bez zobrazenia tejto správy.

ThreatSense

ThreatSense je názov technológie, ktorú tvorí súbor komplexných metód detekcie infiltrácií. Táto technológia je proaktívna, takže poskytuje ochranu aj počas prvých hodín šírenia novej hrozby. K odhaleniu hrozieb využíva kombináciu niekoľkých metód (analýza kódu, emulácia kódu, generické signatúry, generické a vírusové definície), čím efektívne spája ich výhody. Detekčné jadro je schopné kontrolovať niekoľko dátových tokov paralelne, a tak maximalizovať rýchlosť a účinnosť detekcie. Technológia ThreatSense dokáže úspešne eliminovať aj rootkity.

Nastavenia ThreatSense vám umožňujú špecifikovať viacero parametrov kontroly:

- typy súborov a prípony, ktoré sa majú kontrolovať,
- kombinácie rôznych metód detekcie,
- úrovne liečenia atď.

Pre zobrazenie okna s nastaveniami kliknite na **ThreatSense** v Rozšírených nastaveniach príslušných modulov využívajúcich technológiu ThreatSense (pozrite nižšie). Odlišné bezpečnostné scenáre si vyžadujú rôzne nastavenia. Technológia ThreatSense je osobitne nastaviteľná pre tieto moduly:

- Rezidentná ochrana súborového systému
- Kontrola v nečinnosti
- Kontrola pri štarte
- Ochrana dokumentov
- Ochrana e□mailových klientov
- Ochrana prístupu na web
- Kontrola počítača

Parametre ThreatSense sú pre každý modul odlišné. Zmeny v nastavení týchto parametroch môžu výrazne ovplyvniť celkový výkon systému. Príkladom môže byť povolenie pokročilej heuristiky v rámci modulu rezidentnej ochrany súborového systému a voľba vždy kontrolovať runtime archívy, čo môže viesť k spomaleniu systému (pri predvolenom nastavení sú pri týchto metódach kontrolované iba novovytvorené súbory). Preto odporúčame ponechať pôvodné nastavenia ThreatSense pre všetky moduly ochrany okrem Kontroly počítača.

Objekty na kontrolu

Táto sekcia umožňuje nastaviť, ktoré komponenty počítača a súborového systému budú testované na prítomnosť infiltrácií.

Operačná pamäť – slúži na kontrolu prítomnosti hrozieb, ktoré môžu byť zavedené v operačnej pamäti počítača.

Zavádzacie sektory/UEFI – kontroluje zavádzacie sektory na prítomnosť malvéru v hlavnom zavádzacom zázname. Viac o UEFI sa dočítate v slovníku pojmov.

E-mailové súbory – program podporuje nasledujúce prípony súborov: DBX (Outlook Express) a EML.

Archívy – program podporuje nasledujúce prípony: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE a mnoho ďalších.

Samorozbaľovacie archívy – archívy, ktoré nepotrebujú pre svoje rozbalenie iné programy. Ide o SFX (self-extracting) archívy.

Runtime archívy – runtime archívy sa na rozdiel od štandardných archívov po spustení rozbalia v pamäti počítača. Okrem štandardných statických archívov (UPX, yoda, ASPack, FSG atď.) dokáže program rozpoznať vďaka emulácii kódu aj veľa iných typov archívov.

Možnosti kontroly

V tejto sekcii môžete nastaviť, ktoré metódy detekcie sa použijú pri kontrole systému na prítomnosť infiltrácií. K dispozícii sú nasledujúce možnosti:

Heuristika – heuristika je algoritmus, ktorý analyzuje (škodlivú) aktivitu programov. Výhodou heuristiky je schopnosť odhaliť aj taký škodlivý softvér, ktorý v dobe poslednej aktualizácie modulu detekčného jadra

programu ešte neexistoval alebo nebol pokrytý. Nevýhodou je (veľmi malá) pravdepodobnosť „falošného poplachu“.

Pokročilá heuristika/DNA vzorky – pokročilá heuristika je jedinečný algoritmus vyvinutý spoločnosťou ESET, ktorý je optimalizovaný pre odhaľovanie počítačových červov a trójskych koní písaných vo vyšších programovacích jazykoch. Použitie pokročilej heuristiky značne zvyšuje možnosti rozpoznávania vírusov a malvéru. Vzorky umožňujú spoľahlivo odhaliť a identifikovať nové vírusy. Vďaka pravidelnej aktualizácii sú nové vzorky k dispozícii zvyčajne už do niekoľkých hodín od objavenia hrozby. Nevýhodou je, že táto metóda odhaľuje iba vírusy na základe známych vzoriek, prípadne ich čiastočne pozmenené verzie.

Liečenie

Nastavenia liečenia určujú správanie programu ESET Internet Security pri čistení infikovaných súborov. Sú dostupné 4 úrovne liečenia:

ThreatSense poskytuje nasledujúce úrovne nápravy (t. j. liečenia) v prípade detegovaných objektov:

Liečenie v ESET Internet Security

Úroveň liečenia	Popis
Vždy vyriešiť detekciu	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých zriedkavých prípadoch (napríklad pri systémových súboroch), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení.
Vyriešiť detekciu a ak to nie je možné, ponechať ju	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých prípadoch (napríklad pri systémových súboroch alebo archívoch s infikovanými aj neškodnými súbormi), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení.
Vyriešiť detekciu a ak to nie je možné, spýtať sa	Program sa pokúsi o liečenie detegovaného objektu. V niektorých prípadoch, keď nie je možné vykonať žiadnu akciu, sa koncovému používateľovi zobrazí interaktívne upozornenie, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Toto nastavenie sa odporúča vo väčšine prípadov.
Vždy sa spýtať koncového používateľa	Koncovému používateľovi sa pri liečení objektov zobrazí interaktívne okno, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Táto úroveň liečenia je určená pre pokročilých používateľov, ktorí vedia, ako postupovať pri detekciách.

Vylúčenia

Prípona je časť názvu súboru, spravidla oddelená bodkou. Prípona určuje typ a obsah súboru. V tejto časti nastavení ThreatSense zvolíte, ktoré typy súborov budú kontrolované.

Ostatné

V rámci konfigurácie parametrov ThreatSense pre Manuálnu kontrolu počítača sú v sekcii **Iné** k dispozícii aj nasledujúce možnosti:

Kontrolovať alternatívne dátové prúdy (ADS) – alternatívne dátové prúdy používané systémom NTFS sú asociácie k súborom a adresárom, ktoré sú pre bežné spôsoby kontroly neviditeľné. Veľký počet vírusov ich preto využíva na svoje maskovanie a ukrytie sa pred prípadným odhalením.

Kontroly na pozadí vykonávať s nízkou prioritou – každá kontrola počítača využíva isté množstvo systémových prostriedkov. Ak práve pracujete s programami náročnými na výkon počítača, presunutím kontroly na pozadie jej môžete priradiť nižšiu prioritu a získať tým viac systémových prostriedkov pre svoje aplikácie.

Zapisovať všetky objekty do protokolu – protokol kontroly zobrazí všetky skontrolované súbory v samorozbaľovacích archívoch, a to aj súbory, ktoré neboli infikované (môže tak dochádzať ku generovaniu veľkého množstva dát a viesť k veľkému súboru protokolu kontroly).

Zapnúť Smart optimalizáciu – pri zapnutej Smart optimalizácii sa použijú optimálne nastavenia na zabezpečenie najefektívnejšej úrovne kontroly pri zachovaní najvyššej možnej rýchlosti kontroly. Moduly ochrany pri kontrole dômyselne využívajú rozdielne metódy kontroly pre rôzne typy súborov. Ak je Smart optimalizácia vypnutá, pri kontrole sú použité len používateľské nastavenia jadra ThreatSense pre konkrétne moduly.

Zachovať čas posledného prístupu k súborom – pri kontrole súboru nebude zmenený čas prístupu, ale bude ponechaný pôvodný (vhodné pri používaní zálohovacích systémov).

Obmedzenia

V sekcii Obmedzenia môžete nastaviť maximálnu veľkosť kontrolovaných objektov a maximálnu hĺbku kontroly v archívoch.

Nastavenie objektov

Maximálna veľkosť objektu – definuje maximálnu veľkosť skenovaného objektu. Daný modul antivírusu bude kontrolovať len objekty s menšou veľkosťou, ako je definovaná hodnota. Tieto hodnoty odporúčame meniť len pokročilým používateľom, ktorí chcú veľké objekty z určitého dôvodu vylúčiť z kontroly. Predvolená hodnota: neobmedzené.

Maximálny čas kontroly objektu (v sekundách) – definuje maximálny povolený čas na kontrolu súborov v objekte kontajnera (napr. archívy RAR/ZIP alebo e□mail s viacerými prílohami). Toto nastavenie sa netýka samostatných súborov. Ak používateľ zadefinuje určitú hodnotu, po prekročení uvedeného času sa prebiehajúca kontrola skončí bez ohľadu na to, či bol skontrolovaný každý súbor v objekte kontajnera.
V prípade archívu s veľkými súbormi sa kontrola zastaví až po extrahovaní súboru z archívu (napríklad keď používateľ zadefinuje premennú 3 sekundy, ale extrakcia súboru trvá 5 sekúnd). Po uplynutí tohto času sa zostávajúce súbory v archíve nebudú kontrolovať.
Na obmedzenie času kontroly (aj v prípade väčších archívov) použite možnosť **Maximálna veľkosť objektu** a **Maximálna veľkosť súboru v archíve** (neodporúča sa z dôvodu možných bezpečnostných rizík).
Predvolená hodnota: neobmedzené.

Nastavenie kontroly archívov

Úroveň vnorenia archívov – špecifikuje maximálny počet vnorených archívov, do ktorého bude prebiehať antivírusová kontrola. Predvolená hodnota: 10.

Maximálna veľkosť súboru v archíve – špecifikuje maximálnu veľkosť rozbalených súborov v archíve, ktoré sa majú kontrolovať. Maximálna hodnota je **3 GB**.

Neodporúčame meniť predvolené hodnoty, za normálnych okolností nie je žiadny dôvod na ich zmenu.

Ochrana prístupu na web

Ochrana prístupu na web umožňuje konfigurovať pokročilé nastavenia modulu Ochrana internetu. V časti Rozšírené nastavenia > **Ochrana** > **Ochrana prístupu na web** > **Ochrana prístupu na web** sú k dispozícii tieto možnosti:

Zapnúť ochranu prístupu na web – ak je táto možnosť vypnutá, ochrana prístupu na web a antiphishingová ochrana nebudú fungovať.

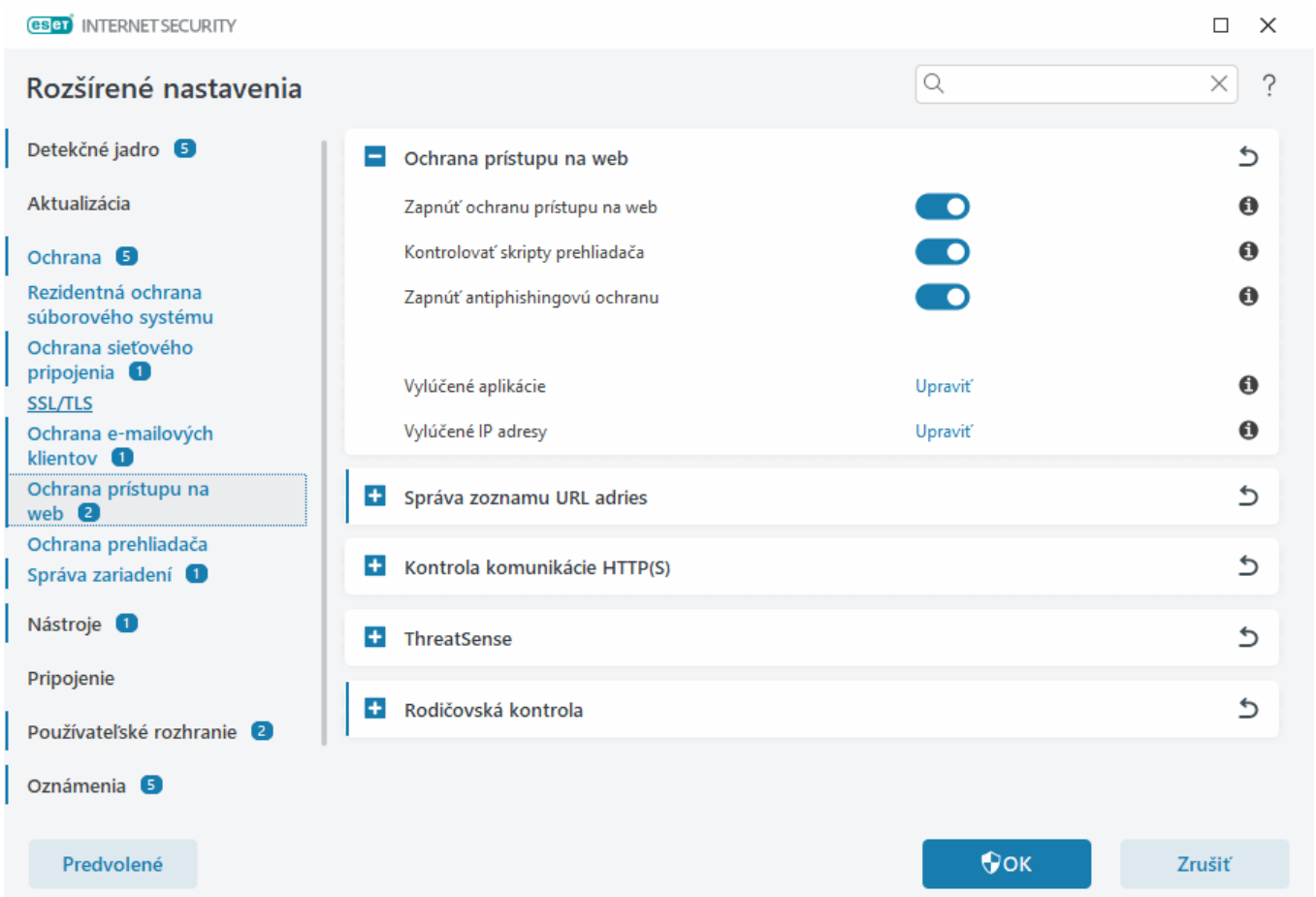
> Dôrazne odporúčame ponechať Ochranu prístupu na web zapnutú a predvolene nevylučovať žiadne aplikácie ani IP adresy.

Kontrolovať skripty prehliadača – ak je táto funkcia zapnutá, detekčné jadro kontroluje všetky programy využívajúce JavaScript, ktoré sú spúšťané webovými prehliadačmi.

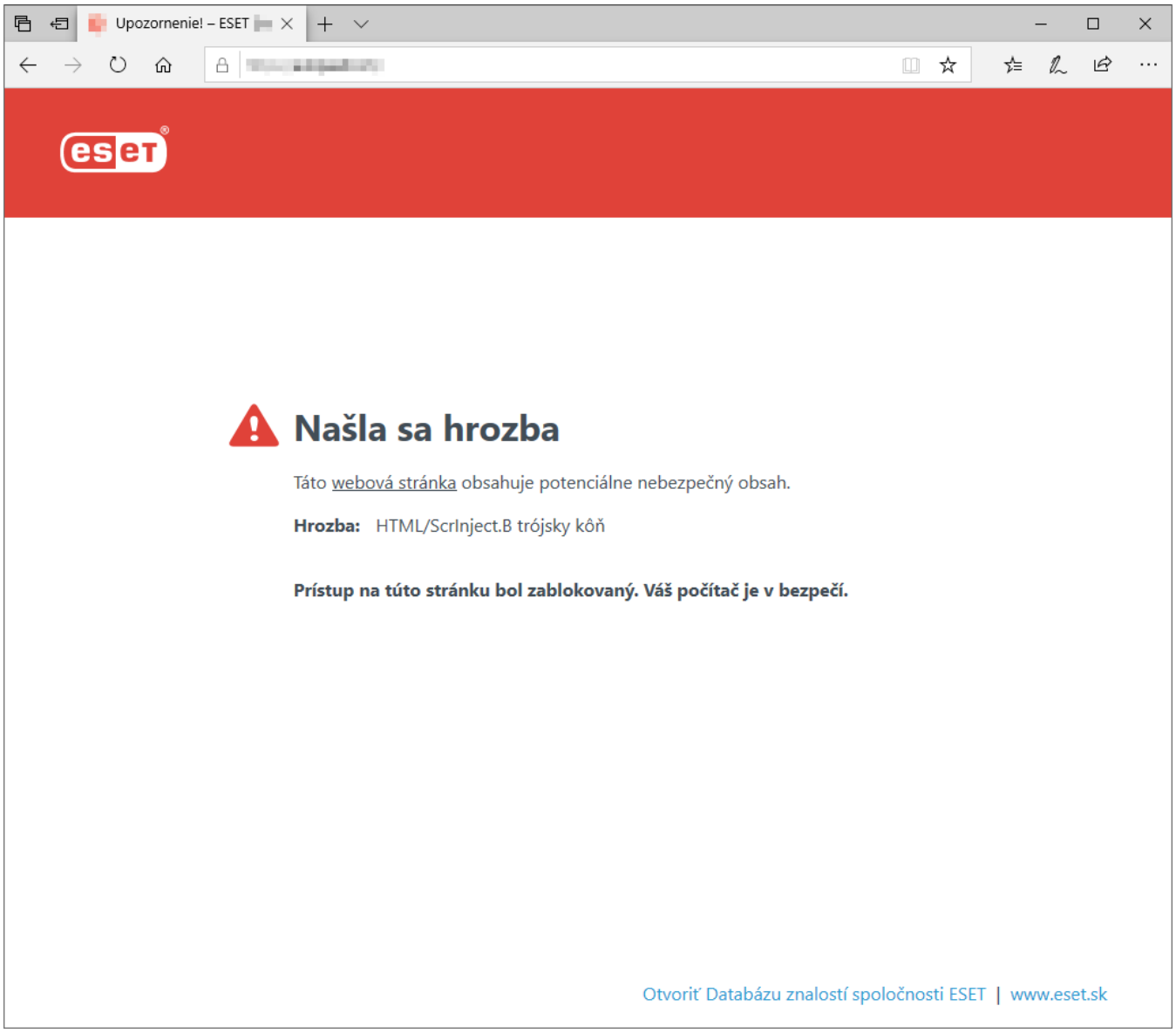
Zapnúť antiphishingovú ochranu – ak je táto funkcia zapnutá, phishingové webové stránky budú blokované. Pre viac informácií si prečítajte kapitolu Antiphishingová ochrana.

Vylúčené aplikácie – umožňuje vylúčiť konkrétne aplikácie z kontroly v rámci Ochrany prístupu na web. Takéto vylúčenie môže byť užitočné v prípade, keď ochrana prístupu na web spôsobuje problémy s kompatibilitou.

Vylúčené IP adresy – umožňuje vylúčiť konkrétne vzdialené adresy z kontroly v rámci Ochrany prístupu na web. Takéto vylúčenie môže byť užitočné v prípade, keď ochrana prístupu na web spôsobuje problémy s kompatibilitou.



Ak dôjde k zablokovaniu webovej stránky, Ochrana prístupu na web zobrazí vo vašom prehliadači nasledujúcu správu:



Ilustrované inštrukcie

Berte, prosím, na vedomie, že nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:

- Ako vylúčiť bezpečnú webovú stránku z blokovania modulom Ochrany prístupu na web?
- Ako zablokovať webovú stránku prostredníctvom ESET Internet Security?

Vylúčené aplikácie

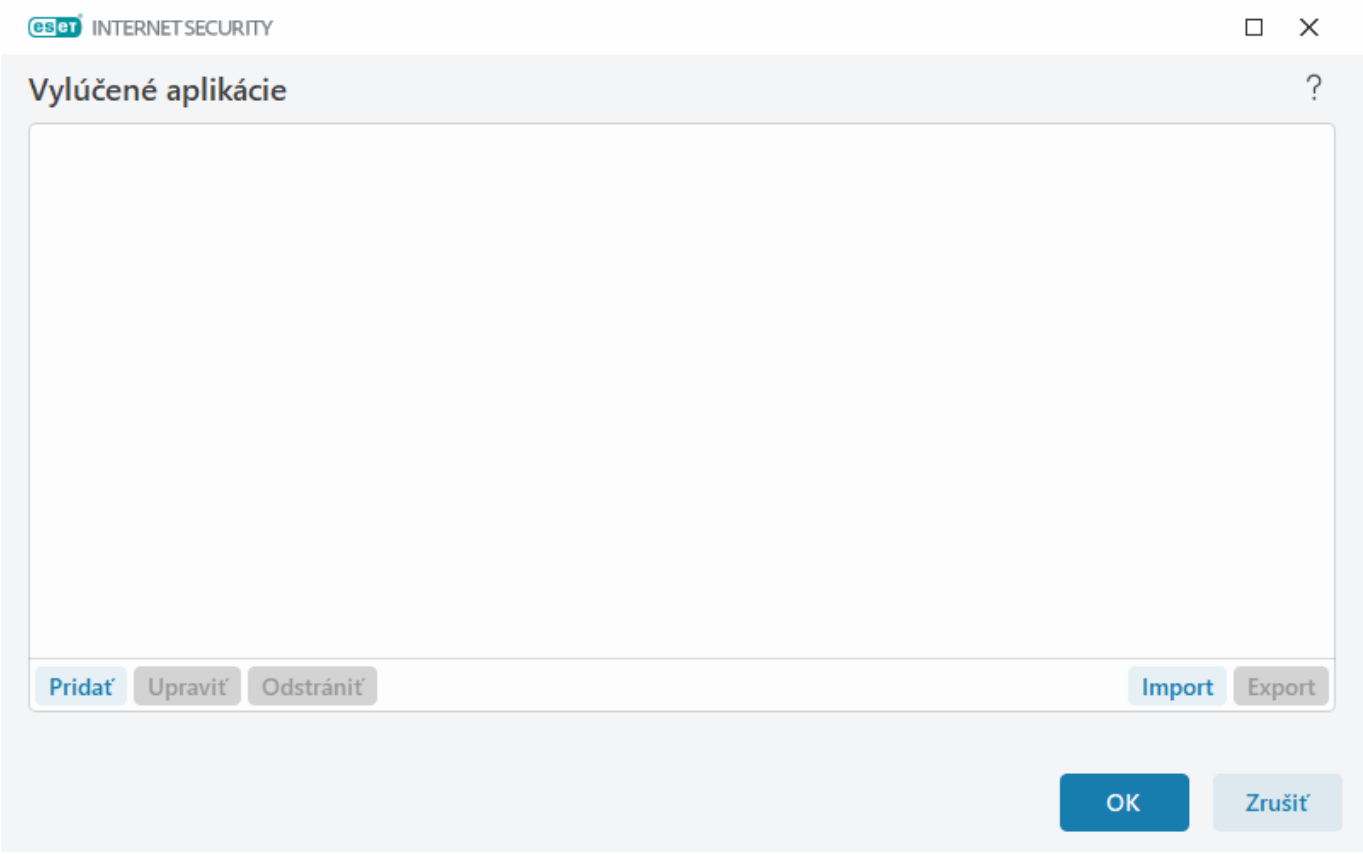
Ak nechcete kontrolovať komunikáciu pre konkrétne aplikácie, pridajte ich do zoznamu vylúčení. HTTP(S)/POP3(S)/IMAP(S) komunikácia označených aplikácií nebude kontrolovaná na prítomnosť škodlivého kódu. Vylúčenie aplikácie z kontroly odporúčame iba v nevyhnutných prípadoch, napríklad ak aplikácia v dôsledku kontroly jej komunikácie nepracuje správne.

Spustené aplikácie a služby sa zobrazia automaticky po kliknutí na tlačidlo **Pridať**. Kliknite na **...** a vyhľadajte

aplikáciu, pre ktorú chcete pridať vylúčenie.

Upraviť – umožňuje upravovať zvolené položky v zozname.

Odstrániť – umožňuje odstrániť zvolené položky zo zoznamu.



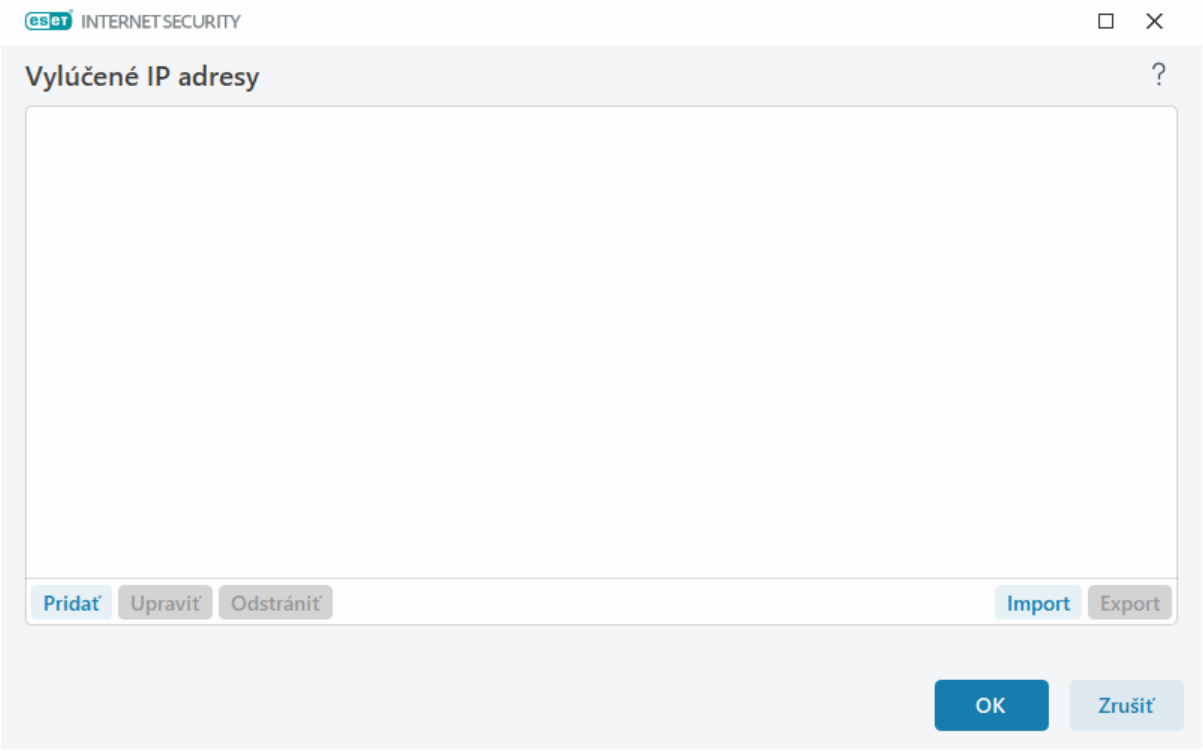
Vylúčené IP adresy

IP adresy uvedené v zozname budú vylúčené z kontroly. Obojstranná HTTP(S)/POP3(S)/IMAP(S) komunikácia označených aplikácií nebude kontrolovaná na prítomnosť škodlivého kódu. Odporúčame používať túto možnosť iba v prípade dôveryhodných IP adries.

Kliknite na **Pridať**, ak chcete vylúčiť vzdialenú IP adresu, rozsah adries alebo podsieť.

Kliknite na **Upraviť**, ak chcete zmeniť vybranú IP adresu.

Kliknite na **Odstrániť**, ak chcete odstrániť označené položky zo zoznamu.



Príklady IP adries

Pridanie IPv4 adresy:

Samostatná adresa – zadanie IP adresy individuálneho počítača (napríklad *192.168.0.10*).

Rozsah adries – zadáva sa začiatočná a koncová IP adresa na stanovenie rozsahu IP adries skupiny počítačov (napr. *192.168.0.1-192.168.0.99*).

Podsieť – skupina počítačov patriacich do určitej podsiete. Zadáva sa IP adresa a maska podsiete. 255.255.255.0 je napríklad sieťová maska pre podsieť 192.168.1.0. Ak chcete vylúčiť celú podsieť, zadajte *192.168.1.0/24*.

Pridanie IPv6 adresy:

Samostatná adresa – zadanie IP adresy individuálneho počítača (napr. *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podsieť – skupina počítačov patriacich do určitej podsiete. Zadáva sa IP adresa a maska podsiete (napr. *2002:c0a8:6301:1::1/64*).

Správa zoznamu URL adries

Správa zoznamu URL adries v sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana prístupu na web** vám umožňuje určiť, ktoré HTTP adresy sa majú blokovať, povoliť alebo vylúčiť z kontroly obsahu.

Ak chcete okrem HTTP adries filtrovať aj HTTPS adresy, musíte mať zapnuté nastavenie SSL/TLS. V opačnom prípade budú pridané len domény HTTPS stránok, ktoré ste navštívili, a celé URL adresy nebudú pridané.

Webové stránky na **zozname blokovaných adries** nebudú prístupné, na rozdiel od stránok na **zozname povolených adries**. Webové stránky na **zozname adries vylúčených z kontroly obsahu** nebudú pri prístupe kontrolované na prítomnosť škodlivého kódu.

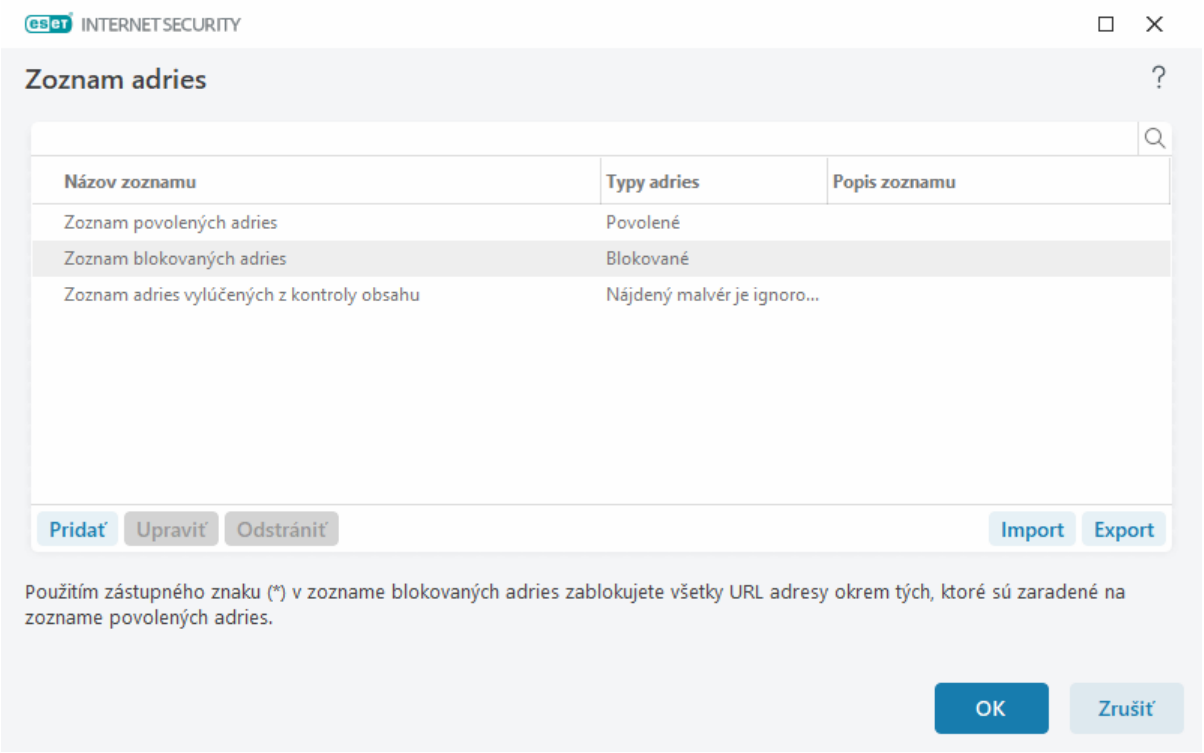
Ak chcete zablokovať všetky HTTP adresy okrem adries zaradených na **Zozname povolených adries**, pridajte znak hviezdičky (*) do **Zoznamu blokovaných adries**.

Je možné používať špeciálne znaky * (hviezdička) a ? (otáznik). Hviezdička nahrádza ľubovoľný reťazec znakov a otáznik nahrádza ľubovoľný znak. Pri zadávaní vylúčených URL adries dávajte pozor, pretože zoznam by mal

obsahovať len dôveryhodné a bezpečné adresy. Rovnako je potrebné dbať na opatrnosť pri používaní špeciálnych znakov (* a ?) v tomto zozname. Viac informácií o tom, ako bezpečne pomocou masky zadefinovať celú doménu vrátane všetkých subdomén, nájdete v kapitole Pridanie HTTP adresy/masky domény. Pre aktivovanie zoznamu kliknite na možnosť **Zoznam je aktívny**. Ak chcete byť upozornený na zadanie adresy zo zoznamu, zvoľte možnosť **Upozorniť pri použití adresy zo zoznamu**.

Dôveryhodné adresy podľa whitelistu ESET

Ak je v sekcii SSL/TLS zapnutá možnosť **Nekontrolovať komunikáciu s doménami, ktorým ESET dôveruje**, domény na whiteliste spravovanom spoločnosťou ESET nebudú ovplyvnené konfiguráciou správy zoznamu URL adries.



Ovládacie prvky

Pridať – pridanie nového zoznamu k vopred zadefinovaným zoznamom. Toto môže byť užitočné, ak chcete logicky rozdeliť niekoľko skupín adries. Napríklad, jeden zoznam blokovaných adries môže obsahovať adresy z externého verejného blacklistu a ďalší zoznam môže obsahovať váš vlastný blacklist, čo umožňuje aktualizáciu externých zoznamov, pričom nenaruší váš používateľský zoznam.

Upraviť – zmena existujúceho zoznamu. Použite túto možnosť na pridanie alebo odstránenie adresy zo zoznamu.

Odstrániť – odstránenie existujúceho zoznamu. Dostupné len pre zoznamy pridané cez tlačidlo **Pridať**, nie pre predvolené zoznamy.

Zoznamy adries

V tejto sekcii môžete definovať zoznamy HTTP(S) adries, ktoré budú blokované, povolené alebo vylúčené z kontroly.

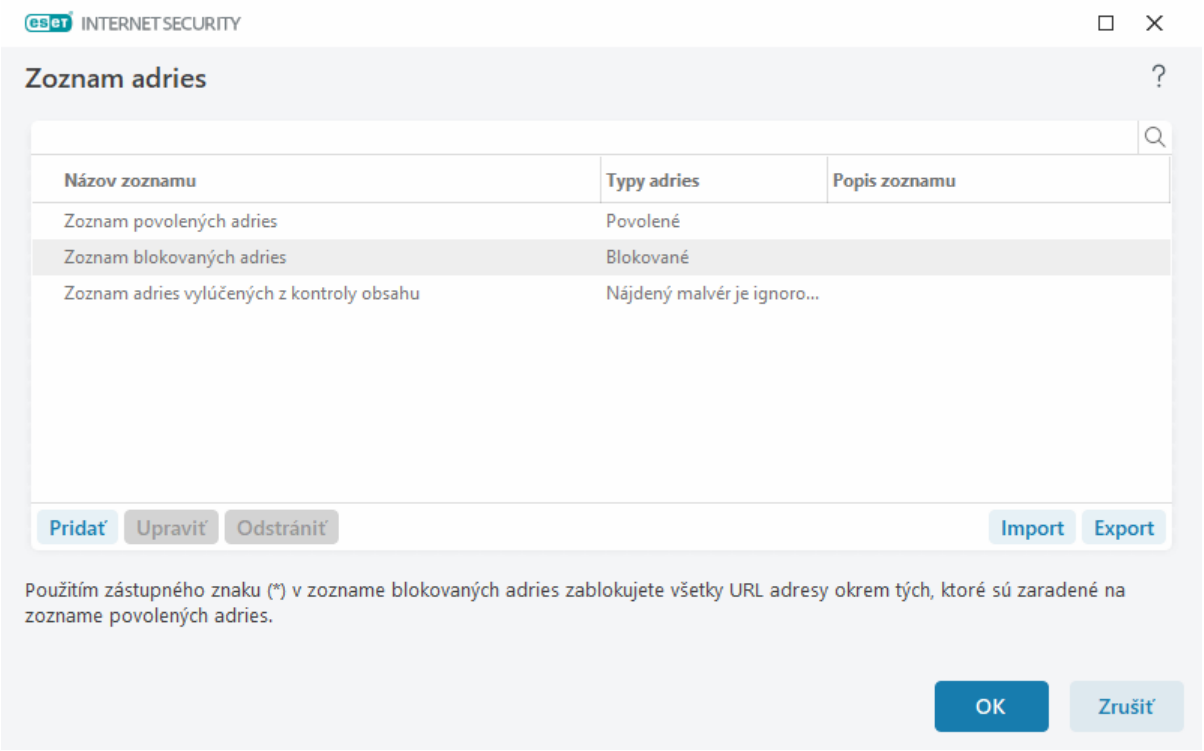
Na základe predvolených nastavení sú k dispozícii tri zoznamy:

• **Zoznam adries vylúčených z kontroly obsahu** – adresy v tomto zozname nebudú kontrolované na prítomnosť škodlivého kódu.

• **Zoznam povolených adries** – pokiaľ je aktívna voľba Povoliť prístup iba na HTTP adresy zaradené do zoznamov povolených adries a zoznam blokovaných adries obsahuje zástupný znak * (takže všetko), používateľovi bude umožnený prístup iba na adresy v tomto zozname. Adresy v tomto zozname budú povolené aj v tom prípade, ak sa nachádzajú aj v zozname blokovaných adries.

• **Zoznam blokovaných adries** – na adresy v tomto zozname nebude používateľovi povolený prístup, ak sa zároveň nenachádzajú aj v zozname povolených adries.

Kliknite na **Pridať** pre vytvorenie nového zoznamu. Pre zmazanie zoznamu kliknite na **Odstrániť**.



Ilustrované inštrukcie

Berte, prosím, na vedomie, že nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:

- Ako vylúčiť bezpečnú webovú stránku z blokovania modulom Ochrany prístupu na web?
- Ako zablokovať webovú stránku prostredníctvom ESET Windows produktu pre domácnosti?

Viac informácií nájdete v kapitole Správa zoznamu URL adries.

Vytvorenie nového zoznamu adries

Toto dialógové okno vám umožňuje nastaviť nový zoznam URL adries/masiek, ktoré budú blokované, povolené alebo vylúčené z kontroly.

Je možné nastaviť:

Typ zoznamu adries – k dispozícii sú tri typy zoznamov:

• **Nájdený malvér je ignorovaný** – adresy v tomto zozname nebudú kontrolované na prítomnosť škodlivého

kódu.

- **Zoznam blokovaných adries** – na adresy v tomto zozname nebude povolený prístup.

- **Zoznam povolených adries** – na adresy v tomto zozname bude povolený prístup. Adresy v tomto zozname budú povolené aj v tom prípade, ak sa nachádzajú aj v zozname blokovaných adries.

Názov zoznamu – zadajte názov nového zoznamu. Toto pole nebude dostupné v prípade zmeny nastavení niektorého z preddefinovaných zoznamov.

Popis zoznamu – zadajte krátky popis zoznamu (nepovinné). Toto pole nebude dostupné v prípade zmeny nastavení niektorého z preddefinovaných zoznamov.

Pre aktivovanie zoznamu kliknite na možnosť **Zoznam je aktívny**. Pri aplikovaní adresy z konkrétneho zoznamu je možné nastaviť upozornenie o tejto udalosti prostredníctvom voľby **Upozorniť pri aplikovaní**. Napríklad pri prístupe na blokovanú alebo povolenú stránku zo zoznamu sa zobrazí oznámenie na ploche. Oznámenie bude obsahovať názov zoznamu.

Závažnosť zapisovania do protokolu – informácie o konkrétnom zozname, ktorý sa používa pri prístupe na webové stránky, sa môžu zapisovať do protokolov.

Ovládacie prvky

Pridať – pridanie novej URL adresy do zoznamu (na pridanie viacerých adries použite oddeľovač).

Upraviť – úprava už existujúcej adresy v zozname. Táto možnosť je dostupná len pre adresy vytvorené pomocou tlačidla **Pridať**.

Odstrániť – odstránenie adries zo zoznamu. Táto možnosť je dostupná len pre adresy vytvorené pomocou tlačidla **Pridať**.

Importovať – import textového súboru s URL adresami (formát súboru *.txt – jedna adresa v riadku a kódovanie UTF-8).

Ako pridať URL masku

Pred pridaním požadovanej masky adresy/domény si prečítajte uvedené inštrukcie.

ESET Internet Security umožňuje používateľovi blokovať prístup na konkrétne webové stránky a zabrániť tomu, aby internetový prehliadač zobrazoval ich obsah. Tiež umožňuje používateľovi špecifikovať adresy, ktoré majú byť vylúčené z kontroly. V prípade, že nepoznáte celý názov vzdialeného servera alebo chcete špecifikovať celú skupinu vzdialených serverov, je možné použiť tzv. masky. V tomto prípade sú povolené špeciálne znaky ? a *, pričom:

- znak ? nahrádza ľubovoľný symbol,

- znak * nahrádza ľubovoľný reťazec textu.

Napríklad *.c?m bude platiť pre všetky adresy, kde posledná časť adresy začína znakom c, končí znakom m a v strede je ľubovoľný znak (.com, .cam a pod.).

Ak je sekvencia „*.“ použitá na začiatku názvu domény, je posudzovaná špecificky. Po prvé zástupný znak „*“ v tomto prípade nepokrýva lomku („/“). Zabráni sa tak obchádzaniu masky – napríklad pomocou masky **.domena.sk* sa nebude vyhodnocovať adresa *http://akakolvekdomena.com/cesta#.domena.sk* (takáto prípona môže byť pripojená k ľubovoľnej URL adrese bez toho, aby ovplyvnila sťahovanie). Po druhé sekvencia „*.“ v tomto špeciálnom prípade tiež pokrýva prázdny reťazec. To umožňuje použiť jednotnú masku pre celú doménu vrátane jej subdomén. Napríklad maskou **.domena.sk* bude vyhodnotená aj adresa *http://domena.sk*. Použitie masky **domena.sk* by bolo nesprávne, pretože by to mohlo tiež zodpovedať adrese *http://inadomena.sk*.

Kontrola komunikácie HTTP(S)

ESET Internet Security v predvolenom nastavení kontroluje komunikáciu cez protokoly HTTP a HTTPS, ktoré využívajú internetové prehliadače a iné aplikácie. Kontrolu tejto komunikácie vypnite len vtedy, ak máte problémy so softvérom tretej strany a chcete zistiť, či môže byť príčinou program ESET Internet Security.

Zapnúť kontrolu komunikácie HTTP – komunikácia cez protokol HTTP sa vždy kontroluje na všetkých portoch a pre všetky aplikácie.

Zapnúť kontrolu komunikácie HTTPS – pri tejto komunikácii sú údaje prenášané medzi serverom a klientom zašifrované. ESET Internet Security kontroluje aj komunikáciu využívajúcu protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Program bude kontrolovať len porty uvedené v časti **Porty používané protokolom HTTPS** bez ohľadu na verziu operačného systému (k prednastaveným hodnotám 443 a 0-65535 môžete pridať ďalšie porty).

ThreatSense

ThreatSense je názov technológie, ktorú tvorí súbor komplexných metód detekcie infiltrácií. Táto technológia je proaktívna, takže poskytuje ochranu aj počas prvých hodín šírenia novej hrozby. K odhaleniu hrozieb využíva kombináciu niekoľkých metód (analýza kódu, emulácia kódu, generické signatúry, generické a vírusové definície), čím efektívne spája ich výhody. Detekčné jadro je schopné kontrolovať niekoľko dátových tokov paralelne, a tak maximalizovať rýchlosť a účinnosť detekcie. Technológia ThreatSense dokáže úspešne eliminovať aj rootkity.

Nastavenia ThreatSense vám umožňujú špecifikovať viacero parametrov kontroly:

- typy súborov a prípony, ktoré sa majú kontrolovať,
- kombinácie rôznych metód detekcie,
- úrovne liečenia atď.

Pre zobrazenie okna s nastaveniami kliknite na **ThreatSense** v Rozšírených nastaveniach príslušných modulov využívajúcich technológiu ThreatSense (pozrite nižšie). Odlišné bezpečnostné scenáre si vyžadujú rôzne nastavenia. Technológia ThreatSense je osobitne nastaviteľná pre tieto moduly:

- Rezidentná ochrana súborového systému
- Kontrola v nečinnosti
- Kontrola pri štarte
- Ochrana dokumentov

- Ochrana e-mailových klientov
- Ochrana prístupu na web
- Kontrola počítača

Parametre ThreatSense sú pre každý modul odlišné. Zmeny v nastavení týchto parametroch môžu výrazne ovplyvniť celkový výkon systému. Príkladom môže byť povolenie pokročilej heuristiky v rámci modulu rezidentnej ochrany súborového systému a voľba vždy kontrolovať runtime archívy, čo môže viesť k spomaleniu systému (pri predvolenom nastavení sú pri týchto metódach kontrolované iba novovytvorené súbory). Preto odporúčame ponechať pôvodné nastavenia ThreatSense pre všetky moduly ochrany okrem Kontroly počítača.

Objekty na kontrolu

Táto sekcia umožňuje nastaviť, ktoré komponenty počítača a súborového systému budú testované na prítomnosť infiltrácií.

Operačná pamäť – slúži na kontrolu prítomnosti hrozieb, ktoré môžu byť zavedené v operačnej pamäti počítača.

Zavádzacie sektory/UEFI – kontroluje zavádzacie sektory na prítomnosť malvéru v hlavnom zavádzacom zázname. Viac o UEFI sa dočítate v slovníku pojmov.

E-mailové súbory – program podporuje nasledujúce prípony súborov: DBX (Outlook Express) a EML.

Archívy – program podporuje nasledujúce prípony: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE a mnoho ďalších.

Samorozbaľovacie archívy – archívy, ktoré nepotrebujú pre svoje rozbalenie iné programy. Ide o SFX (self-extracting) archívy.

Runtime archívy – runtime archívy sa na rozdiel od štandardných archívov po spustení rozbalia v pamäti počítača. Okrem štandardných statických archívov (UPX, yoda, ASPack, FSG atď.) dokáže program rozpoznať vďaka emulácii kódu aj veľa iných typov archívov.

Možnosti kontroly

V tejto sekcii môžete nastaviť, ktoré metódy detekcie sa použijú pri kontrole systému na prítomnosť infiltrácií. K dispozícii sú nasledujúce možnosti:

Heuristika – heuristika je algoritmus, ktorý analyzuje (škodlivú) aktivitu programov. Výhodou heuristiky je schopnosť odhaliť aj taký škodlivý softvér, ktorý v dobe poslednej aktualizácie modulu detekčného jadra programu ešte neexistoval alebo nebol pokrytý. Nevýhodou je (veľmi malá) pravdepodobnosť „falošného poplachu“.

Pokročilá heuristika/DNA vzorky – pokročilá heuristika je jedinečný algoritmus vyvinutý spoločnosťou ESET, ktorý je optimalizovaný pre odhaľovanie počítačových červov a trójskych koní písaných vo vyšších programovacích jazykoch. Použitie pokročilej heuristiky značne zvyšuje možnosti rozpoznávania vírusov a malvéru. Vzorky umožňujú spoľahlivo odhaliť a identifikovať nové vírusy. Vďaka pravidelnej aktualizácii sú nové vzorky k dispozícii zvyčajne už do niekoľkých hodín od objavenia hrozby. Nevýhodou je, že táto metóda odhaľuje iba vírusy na základe známych vzoriek, prípadne ich čiastočne pozmenené verzie.

Liečenie

Nastavenia liečenia určujú správanie programu ESET Internet Security pri čistení infikovaných súborov. Sú dostupné 4 úrovne liečenia:

ThreatSense poskytuje nasledujúce úrovne nápravy (t. j. liečenia) v prípade detegovaných objektov:

Liečenie v ESET Internet Security

Úroveň liečenia	Popis
Vždy vyriešiť detekciu	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých zriedkavých prípadoch (napríklad pri systémových súboroch), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení.
Vyriešiť detekciu a ak to nie je možné, ponechať ju	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých prípadoch (napríklad pri systémových súboroch alebo archívoch s infikovanými aj neškodnými súbormi), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení.
Vyriešiť detekciu a ak to nie je možné, spýtať sa	Program sa pokúsi o liečenie detegovaného objektu. V niektorých prípadoch, keď nie je možné vykonať žiadnu akciu, sa koncovému používateľovi zobrazí interaktívne upozornenie, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Toto nastavenie sa odporúča vo väčšine prípadov.
Vždy sa spýtať koncového používateľa	Koncovému používateľovi sa pri liečení objektov zobrazí interaktívne okno, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Táto úroveň liečenia je určená pre pokročilých používateľov, ktorí vedia, ako postupovať pri detekciách.

Vylúčenia

Prípona je časť názvu súboru, spravidla oddelená bodkou. Prípona určuje typ a obsah súboru. V tejto časti nastavení ThreatSense zvolíte, ktoré typy súborov budú kontrolované.

Ostatné

V rámci konfigurácie parametrov ThreatSense pre Manuálnu kontrolu počítača sú v sekcii **Iné** k dispozícii aj nasledujúce možnosti:

Kontrolovať alternatívne dátové prúdy (ADS) – alternatívne dátové prúdy používané systémom NTFS sú asociácie k súborom a adresárom, ktoré sú pre bežné spôsoby kontroly neviditeľné. Veľký počet vírusov ich preto využíva na svoje maskovanie a ukrytie sa pred prípadným odhalením.

Kontroly na pozadí vykonávať s nízkou prioritou – každá kontrola počítača využíva isté množstvo systémových prostriedkov. Ak práve pracujete s programami náročnými na výkon počítača, presunutím kontroly na pozadie jej môžete priradiť nižšiu prioritu a získať tým viac systémových prostriedkov pre svoje aplikácie.

Zapisovať všetky objekty do protokolu – protokol kontroly zobrazí všetky skontrolované súbory v samorozbaľovacích archívoch, a to aj súbory, ktoré neboli infikované (môže tak dochádzať ku generovaniu veľkého množstva dát a viesť k veľkému súboru protokolu kontroly).

Zapnúť Smart optimalizáciu – pri zapnutej Smart optimalizácii sa použijú optimálne nastavenia na zabezpečenie

najefektívnejšej úrovne kontroly pri zachovaní najvyššej možnej rýchlosti kontroly. Moduly ochrany pri kontrole dômyselne využívajú rozdielne metódy kontroly pre rôzne typy súborov. Ak je Smart optimalizácia vypnutá, pri kontrole sú použité len používateľské nastavenia jadra ThreatSense pre konkrétne moduly.

Zachovať čas posledného prístupu k súborom – pri kontrole súboru nebude zmenený čas prístupu, ale bude ponechaný pôvodný (vhodné pri používaní zálohovacích systémov).

Obmedzenia

V sekcii Obmedzenia môžete nastaviť maximálnu veľkosť kontrolovaných objektov a maximálnu hĺbku kontroly v archívoch.

Nastavenie objektov

Maximálna veľkosť objektu – definuje maximálnu veľkosť skenovaného objektu. Daný modul antivírusu bude kontrolovať len objekty s menšou veľkosťou, ako je definovaná hodnota. Tieto hodnoty odporúčame meniť len pokročilým používateľom, ktorí chcú veľké objekty z určitého dôvodu vylúčiť z kontroly. Predvolená hodnota: neobmedzené.

Maximálny čas kontroly objektu (v sekundách) – definuje maximálny povolený čas na kontrolu súborov v objekte kontajnera (napr. archívy RAR/ZIP alebo e-mail s viacerými prílohami). Toto nastavenie sa netýka samostatných súborov. Ak používateľ zadefinuje určitú hodnotu, po prekročení uvedeného času sa prebiehajúca kontrola skončí bez ohľadu na to, či bol skontrolovaný každý súbor v objekte kontajnera.
V prípade archívu s veľkými súbormi sa kontrola zastaví až po extrahovaní súboru z archívu (napríklad keď používateľ zadefinuje premennú 3 sekundy, ale extrakcia súboru trvá 5 sekúnd). Po uplynutí tohto času sa zostávajúce súbory v archíve nebudú kontrolovať.
Na obmedzenie času kontroly (aj v prípade väčších archívov) použite možnosť **Maximálna veľkosť objektu** a **Maximálna veľkosť súboru v archíve** (neodporúča sa z dôvodu možných bezpečnostných rizík).
Predvolená hodnota: neobmedzené.

Nastavenie kontroly archívov

Úroveň vnorenia archívov – špecifikuje maximálny počet vnorených archívov, do ktorého bude prebiehať antivírusová kontrola. Predvolená hodnota: 10.

Maximálna veľkosť súboru v archíve – špecifikuje maximálnu veľkosť rozbalených súborov v archíve, ktoré sa majú kontrolovať. Maximálna hodnota je **3 GB**.

> Neodporúčame meniť predvolené hodnoty, za normálnych okolností nie je žiadny dôvod na ich zmenu.

Rodičovská kontrola

Možnosť **Zapnúť rodičovskú kontrolu** integruje rodičovskú kontrolu do programu ESET Internet Security. Kliknutím na **Upraviť** vedľa položky Používateľské účty vyberiete z používateľských účtov systému Windows tých používateľov, ktorých má rodičovská kontrola chrániť pred prístupom k nevhodnému alebo škodlivému obsahu na internete.

Používateľské účty

V sekcii Rozšírené nastavenia > **Ochrana** > **Ochrana prístupu na web** > **Rodičovská kontrola** > **Používateľské účty** > **Upraviť** môžete z používateľských účtov systému Windows vybrať tých používateľov, ktorých má rodičovská kontrola chrániť pred prístupom k nevhodnému alebo škodlivému obsahu na internete.

Stĺpce

Účet systému Windows – meno používateľa.

Zapnuté – informuje, či je rodičovská kontrola pre daný účet zapnutá.

Doména – názov domény, do ktorej používateľ patrí.

Dátum narodenia – vek vlastníka používateľského účtu.

Ovládacie prvky

Pridať – zobrazí sa okno pre pridanie používateľského účtu.

Upraviť – táto možnosť vám umožní upraviť zvolený účet.

Odstrániť – odstráni zvolený účet.

Obnoviť – ak ste pridali používateľský účet, ESET Internet Security môže obnoviť zoznam používateľských účtov bez toho, aby ste museli okno zatvoriť.

Nastavenia používateľských účtov

Okno Používateľské účty obsahuje nasledujúce karty:

Všeobecné

Pomocou prepínača vedľa možnosti **Zapnuté** zapnite Rodičovskú kontrolu pre účet Windows zvolený nižšie.

Kliknite na **Vybrať** a vyberte jeden z používateľských účtov Windows na vašom počítači. Obmedzenia nastavené v rodičovskej kontrole ovplyvnia iba štandardné používateľské účty. Správcovské účty môžu kontrolu obísť.

Ak je účet používaný rodičom, vyberte **Rodičovský účet**.

Zadajte **Dátum narodenia dieťaťa**, čím stanovíte úroveň prístupu k webovým stránkam podľa vhodnosti pre daný vek dieťaťa.

Závažnosť zapisovania do protokolu

ESET Internet Security ukladá všetky dôležité udalosti do protokolov, ktoré môžete zobraziť priamo z hlavného menu programu. Kliknite na **Nástroje** > **Protokoly** a z roletového menu **Protokoly** vyberte možnosť **Rodičovská kontrola**.

- **Diagnostické** – zaznamenáva do protokolu informácie dôležité pre ladenie programu.

• **Informácie** – zaznamenáva informatívne správy, napríklad o povolených a blokovaných výnimkách, ako aj všetky udalosti s vyššou závažnosťou.

• **Upozornenie** – zaznamenáva kritické chyby a varovné správy.

• **Žiadne** – nebudú vytvárané žiadne protokoly.

Výnimky

Vytvorenie výnimky môže povoliť alebo zakázať používateľovi prístup k webovým stránkam, ktoré sa nenachádzajú na zozname výnimiek. Tento zoznam je užitočný v prípade, ak chcete regulovať prístup ku konkrétnym stránkam namiesto kategórií. Výnimky vytvorené pre jeden účet môžu byť kopírované a použité pre iný účet. Toto môže byť užitočné, ak chcete vytvoriť identické pravidlá pre deti podobného veku.

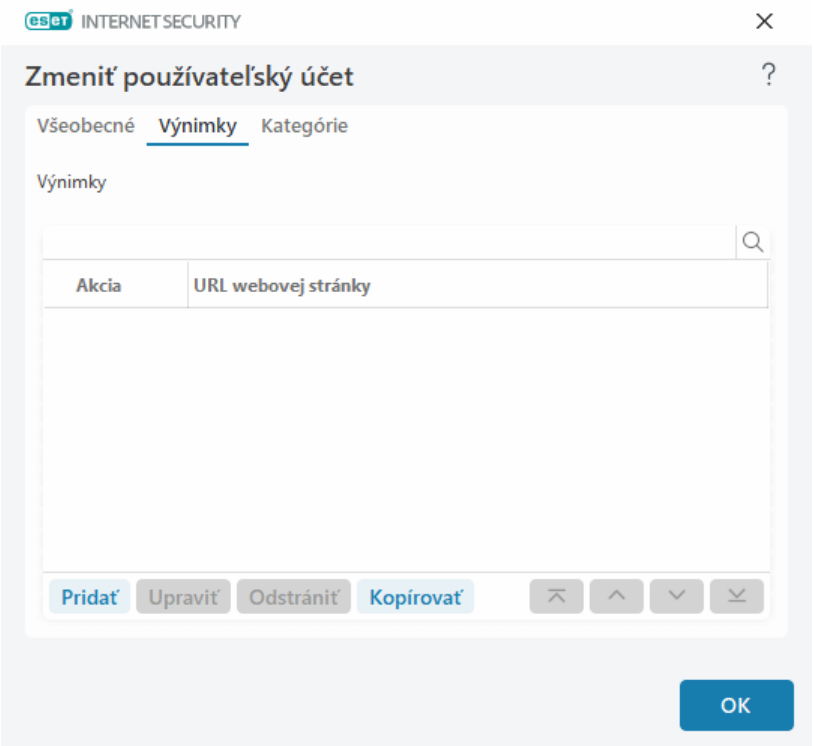
Kliknite na možnosť **Pridať** pre vytvorenie novej výnimky. Z roletového menu zvoľte **Akciu** (napríklad **Blokovať**), zadajte adresu **URL webovej stránky**, pre ktorú je výnimka určená, a kliknite na **OK**. Vytvorená výnimka sa teraz pridá do zoznamu všetkých výnimiek.

Pridať – pridanie novej výnimky.

Upraviť – po kliknutí na túto možnosť môžete zmeniť adresu **URL stránky** alebo **Akciu** zvolenej výnimky.

Odstrániť – odstránenie vybratej výnimky.

Kopírovať – pomocou roletového menu vyberte používateľa, od ktorého chcete skopírovať výnimku.

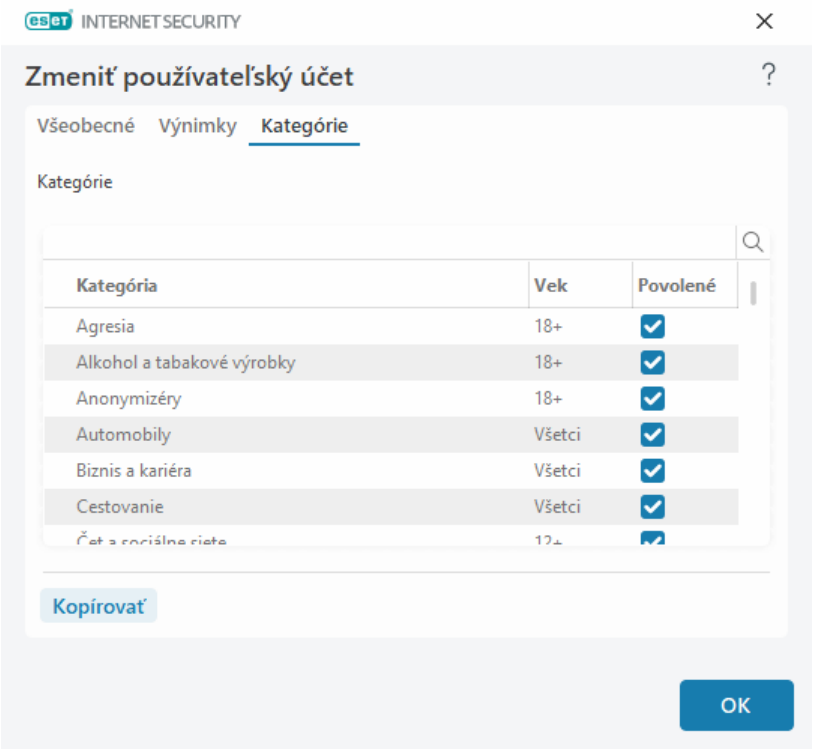


Výnimky potláčajú blokovanie kategórií definovaných pre zvolený účet. Napríklad, ak má účet nastavené blokovanie kategórie **Správy** a zároveň je táto kategória vo výnimkách, účet bude mať k týmto webovým stránkam prístup. Všetky výnimky možno zobraziť v sekcii Výnimky.

Kategórie

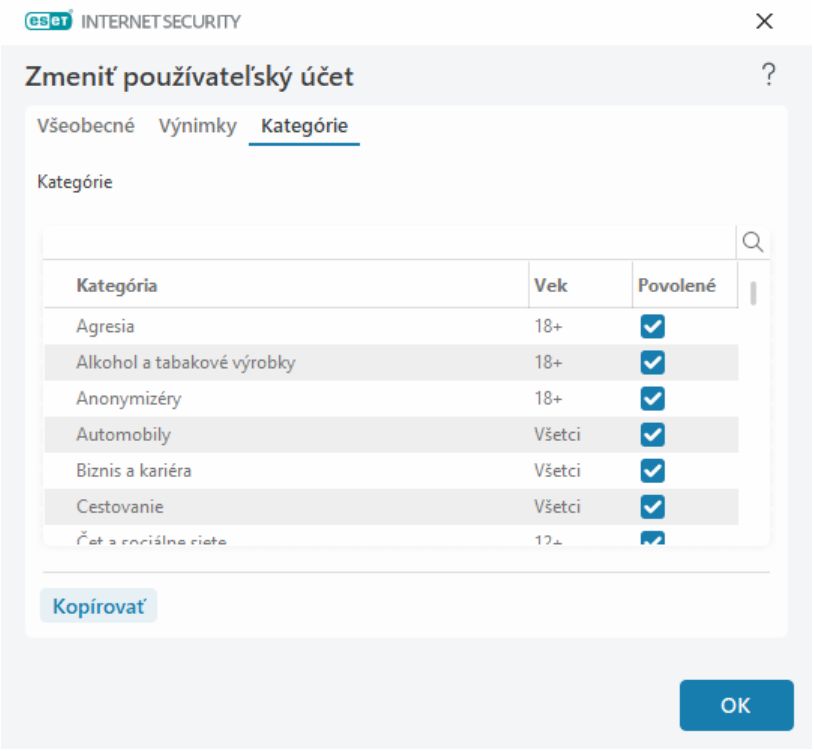
Na karte **Kategórie** môžete definovať všeobecné kategórie webových stránok, ktoré chcete zablokovať alebo povoliť pre jednotlivé účty. Označením začiarkavacieho políčka vedľa kategórie povolíte danú kategóriu. Ak ho neoznačíte, kategória nebude pre daný účet povolená.

Kopírovať – umožňuje kopírovať zoznam povolených alebo blokovaných kategórií od existujúceho používateľského účtu.



Kategórie

V stĺpci **Povolené** označte políčko vedľa kategórie, ktorú chcete povoliť. Ak ponecháte políčko neoznačené, kategória nebude pre daný účet povolená.



Nižšie nájdete niektoré príklady kategórií (skupín), ktorých obsah nemusí byť na prvý pohľad jasný:

- **Rôzne** – zvyčajne privátne (lokálne) IP adresy ako intranet, 127.0.0.0/8, 192.168.0.0/16 a podobne. Ak sa zobrazí chybový kód 403 alebo 404, takáto webová stránka taktiež spadá do tejto kategórie.
- **Nevyriešené** – táto kategória zahŕňa webové stránky, ktoré nebolo možné zaradiť kvôli chybe, ktorá nastala pri pokuse pripojiť sa na databázu rodičovskej kontroly.
- **Nekategorizované** – neznáme webové stránky, ktoré ešte neboli pridané do databázy rodičovskej kontroly.
- **Dynamické** – webové stránky, ktoré používateľa presmerovávajú na iné stránky.

Ochrana prehliadača

Ochrana prehliadača predstavuje ďalšiu úroveň zabezpečenia pre zvýšenie vašej bezpečnosti a súkromia. Chráni pamäť webového prehliadača pred prístupom iných procesov, posilňuje ochranu pred keyloggermi a zabraňuje vkladaniu akýchkoľvek údajov súvisiacich s online platbami, ktoré boli modifikované malvérom, zo schránky do zabezpečeného prehliadača. Ak chcete upraviť konfiguráciu ochrany prehliadača, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana prehliadača** a vyberte si z nasledujúcich možností:

- Ochrana pri platbách a prehliadaní
- Zoznam povolených položiek ochrany prehliadača
- Orámovanie prehliadača

Ochrana pri platbách a prehliadaní

Ochranu pri platbách a prehliadaní môžete nakonfigurovať v rozšírených nastaveniach po kliknutí na **Ochrana** > **Ochrana prehliadača** > **Ochrana pri platbách a prehliadaní**.

Ochrana pri platbách a prehliadaní

Zapnúť ochranu pri platbách a prehliadaní – ak je zapnutá ochrana pri platbách a prehliadaní, všetky podporované webové prehliadače sa budú predvolene spúšťať v zabezpečenom režime.

Ochrana prehliadača

Zabezpečiť všetky prehliadače – všetky podporované webové prehliadače sa spúšťajú v zabezpečenom režime.

Režim inštalácie rozšírení – z roletového menu môžete vybrať, ktoré rozšírenia bude povolené inštalovať do prehliadača zabezpečeného produktom ESET:

- **Základné rozšírenia** – v tomto režime bude možné inštalovať iba základné rozšírenia vyvinuté výrobcom daného prehliadača.
- **Všetky rozšírenia** – bude možné inštalovať všetky rozšírenia podporované daným prehliadačom.

> Zmena režimu inštalácie rozšírení nemá vplyv na už nainštalované rozšírenia prehliadača.

Zabezpečený prehliadač

Rozšírená ochrana pamäte – ak je táto možnosť povolená, pamäť zabezpečeného prehliadača bude chránená pred prístupom iných procesov.

Ochrana klávesnice – ak je táto možnosť povolená, informácie zadávané do zabezpečeného prehliadača prostredníctvom klávesnice budú skryté pred ostatnými aplikáciami. Týmto sa zvyšuje ochrana pred keyloggermi.

Ochrana schránky na kopírovanie – ak je táto možnosť zapnutá, ESET Internet Security zabráni vkladaniu údajov, ktoré súvisia s online platbami a boli modifikované malvérom, zo schránky do zabezpečeného prehliadača. Tým sa zabezpečí ochrana pred prípadnými zmenami vykonanými škodlivým softvérom.

Orámovanie prehliadača – prispôsobte si nastavenia pre farebné orámovanie v chránených prehliadačoch.

Zoznam povolených položiek ochrany prehliadača – spravujte súbory pridané na zoznam povolených položiek ochrany prehliadača.

Ochrana súkromia v prehliadači

Zapnúť ochranu súkromia v prehliadači – ak túto možnosť vypnete, rozšírenie Ochrana súkromia v prehliadači sa odinštaluje zo všetkých podporovaných prehliadačov v každom účte systému Windows.

Zobrazovať oznámenia ochrany súkromia v prehliadači – ak je táto možnosť zapnutá, ESET Internet Security bude zobrazovať oznámenia o ochrane súkromia v prehliadači.

Kontrola skriptov prehliadača

Zapnúť rozšírenú kontrolu skriptov prehliadača – ak je táto možnosť zapnutá, antivírusovej kontrole budú podrobené všetky programy v jazyku JavaScript spúšťané internetovými prehliadačmi.

00

Správa zariadení

ESET Internet Security poskytuje automatickú správu zariadení (CD/DVD/USB atď.). Umožňuje vám blokovať a nastaviť rozšírené prístupové práva a pravidlá na filtrovanie prístupu k zariadeniu. Toto môže byť užitočné v prípade, že správca chce, aby používatelia nemohli používať externé zariadenia s nevyžiadaným obsahom.

Podporované externé zariadenia:

- Diskové úložisko (HDD alebo vymeniteľný USB disk)
- CD/DVD
- USB tlačiareň
- Úložisko FireWire
- Bluetooth zariadenie
- Čítačka smart kariet
- Obrazové zariadenie
- Modem
- Port LPT/COM
- Prenosné zariadenie (zariadenia napájané z batérie, ako sú prehrávače médií, smartfóny, zariadenia typu plug-and-play atď.)
- Všetky typy zariadení

Nastavenia správy zariadení je možné meniť v Rozšírených nastaveniach > **Ochrana** > **Správa zariadení**.

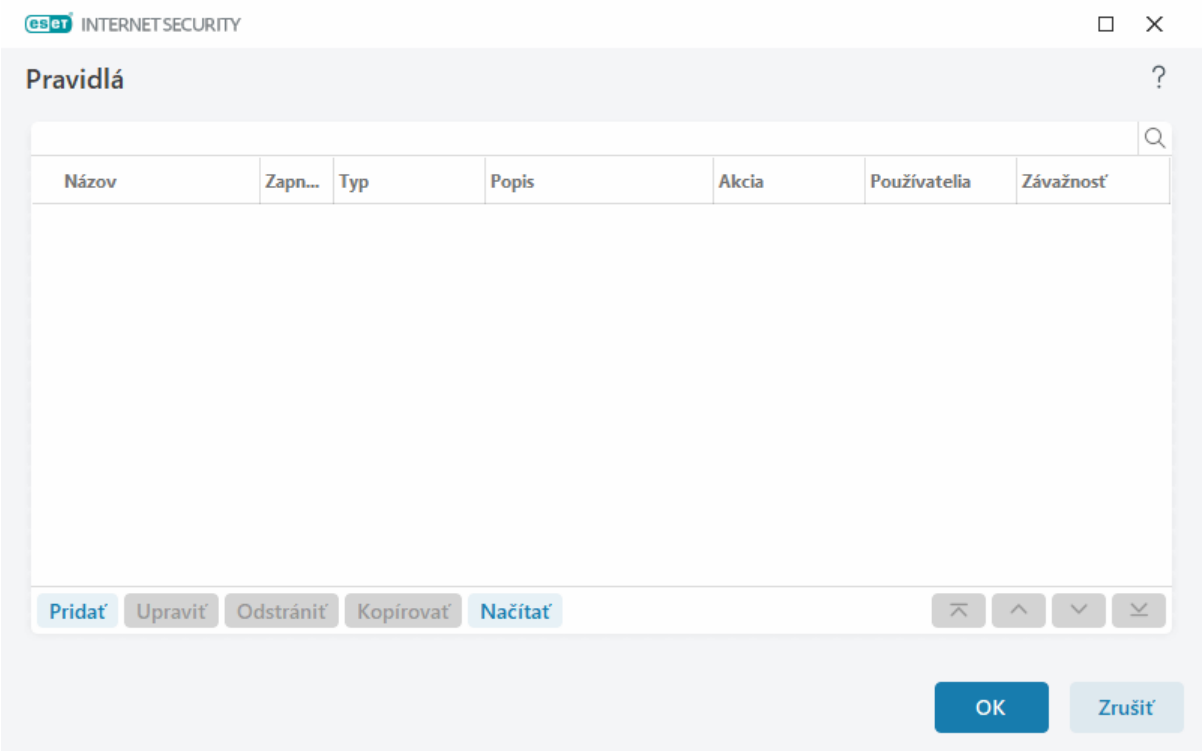
Kliknutím na prepínacie tlačidlo **Zapnúť správu zariadení** povolíte túto funkciu v rámci produktu ESET Internet Security. Aby sa zmena prejavila, musíte počítač reštartovať. Po zapnutí správy zariadení môžete zadefinovať **Pravidlá** v okne editora pravidiel.

> Môžete vytvoriť viacero skupín zariadení, na ktoré sa budú aplikovať rozdielne pravidlá. Môžete tiež vytvoriť len jednu skupinu zariadení, na ktorú aplikujete pravidlo s akciou **Povoliť** alebo **Blokovať zápis**. Vďaka tomu bude zaručené blokovanie neznámych zariadení pripojených k vášmu počítaču.

Pri vložení zariadenia blokovaného existujúcim pravidlom sa zobrazí upozornenie a prístup na zariadenie nebude povolený.

Pravidlá správy zariadení

Editor pravidiel správy zariadení zobrazuje zoznam všetkých existujúcich pravidiel, ktoré vám umožňujú kontrolovať externé zariadenia pripájané k vášmu počítaču.



Jednotlivé zariadenia môžete povoliť alebo blokovať pre vybraného používateľa alebo skupinu používateľov na základe parametrov zariadenia, ktoré zadefinujete v konfigurácii pravidla. Zoznam pravidiel obsahuje popisné informácie ako názov, typ externého zariadenia, akcia, ktorá sa má vykonať po pripojení zariadenia k počítaču, a rozsah vytvorených protokolov. Pozrite si tiež kapitolu Pridanie pravidiel správy zariadení.

Kliknutím na **Pridať** alebo **Upraviť** pridáte či upravíte pravidlo. Kliknutím na **Kopírovať** vytvoríte nové pravidlo s parametrami už existujúceho označeného pravidla. Reťazce XML zobrazené po kliknutí na pravidlo je možné skopírovať do schránky, aby si správcovia systému mohli tieto dáta exportovať/importovať a následne ich použiť.

Podržaním klávesu **CTRL** a kliknutím na pravidlá ich môžete hromadne označiť a aplikovať na ne akcie, napríklad môžete všetky označené pravidlá odstrániť alebo ich presunúť v zozname nahor či nadol. Začiarkavacie políčko **Zapnuté** slúži na aktiváciu alebo deaktiváciu konkrétneho pravidla, čo je užitočné v prípade, že si neželáte pravidlo odstrániť.

Na automatické vyplnenie parametrov zo zariadenia pripojeného k vášmu počítaču kliknite na možnosť **Načítať**.

Pravidlá sú zoradené podľa priority, pričom pravidlá s najvyššou prioritou sú navrchu. Pravidlá môžete jednotlivo alebo v skupinách premiestňovať kliknutím na tlačidlá **Navrch/Vyššie/Nižšie/Naspodok**.

Záznamy v protokoloch si môžete pozrieť v hlavnom okne programu > **Nástroje** > Protokoly.

Do protokolu správy zariadení sa zaznamenávajú informácie o všetkých akciách modulu Správy zariadení.

Zistené zariadenia

Tlačidlo **Načítať** zobrazí okno so zoznamom práve pripojených zariadení s nasledujúcimi informáciami: typ zariadenia, výrobca, model a sériové číslo v prípade, že je dostupné. Ak si chcete prezrieť všetky skryté zariadenia, vyberte možnosť **Zobraziť skryté zariadenia**.

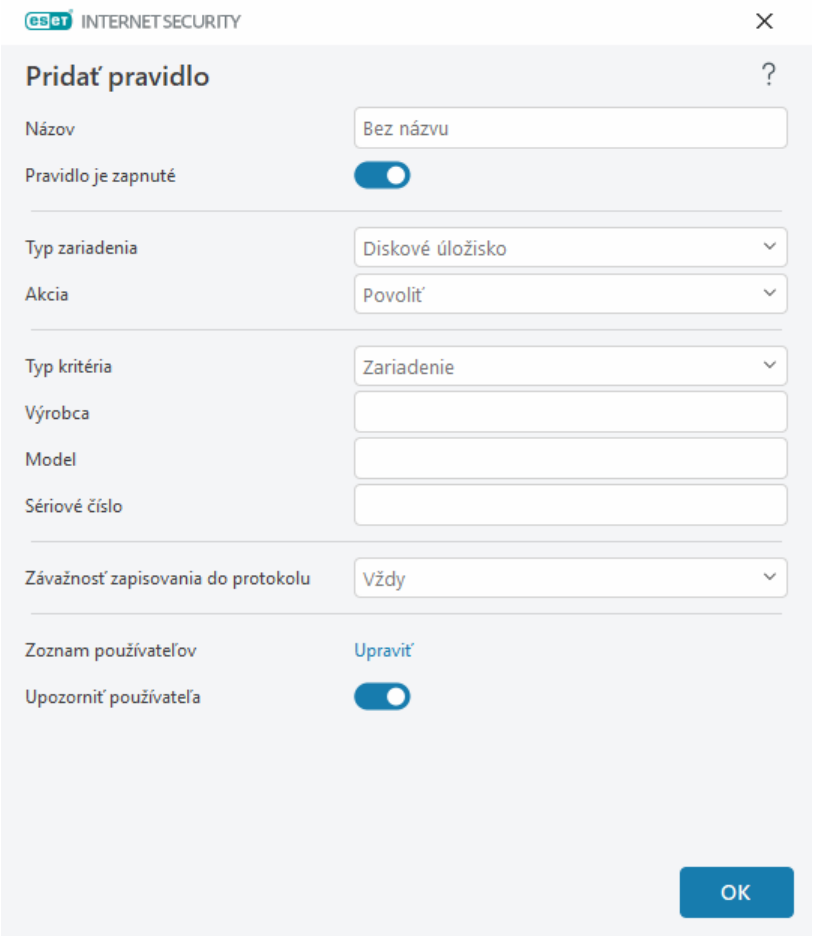
Zvolením konkrétneho zariadenia zo zoznamu Zistené zariadenia a kliknutím na tlačidlo **OK** môžete pridať nové pravidlo správy zariadení s preddefinovanými hodnotami (zobrazené hodnoty je možné upraviť).

Zariadenia v režime nízkej spotreby (režim spánku) sú označené ikonou výkričníka . Ak chcete pre takéto zariadenie pridať pravidlo a aktivovať tlačidlo **OK**, postupujte nasledovne:

- Odpojte a znovu pripojte zariadenie.
- Použite zariadenie (napríklad spustite aplikáciu Fotoaparát v systéme Windows na prebudenie webovej kamery).

Pridanie pravidiel správy zariadení

Pravidlo správy zariadení definuje akciu, ktorá sa má vykonať pri pripojení zariadenia spĺňajúceho kritériá v pravidle k počítaču.



Do poľa **Názov** zadajte popis pravidla na jeho lepšiu identifikáciu. Prepínačom vedľa položky **Pravidlo je zapnuté** aktivujete alebo deaktivujete toto pravidlo, čo je užitočné v prípade, že si neželáte vymazať pravidlo natrvalo.

Typ zariadenia

Z roletového menu vyberte typ externého zariadenia (disk, prenosné zariadenie, Bluetooth, FireWire atď.). Informácia o type zariadenia je prevzatá od operačného systému a je uvedená v systémovom Správcovi zariadení (Device manager), ak je zariadenie pripojené k počítaču. Úložné zariadenia zahŕňajú externé disky alebo čítačky pamäťových kariet pripojené cez USB alebo FireWire. Čítačky smart kariet zahŕňajú čítačky kariet s integrovaným obvodom, ako sú napríklad SIM karty alebo overovacie karty. Medzi zobrazovacie zariadenia patria napríklad skenery alebo digitálne fotoaparáty. Keďže neposkytujú informácie o používateľovi, ale iba o akciách, môžu byť blokované len globálne pre všetkých používateľov.

Akcia

Prístup k zariadeniam bez úložiska môže byť povolený alebo blokovaný. Na druhej strane v rámci prístupových práv k úložným zariadeniam môžete vybrať jednu z nasledujúcich možností:

- **Povoliť** – bude povolený úplný prístup k zariadeniu.
- **Blokovať** – prístup k zariadeniu bude blokovaný.
- **Blokovať zápis** – povolený bude prístup k zariadeniu len na čítanie, nie na zápis.
- **Upozorniť** – pri pripojení zariadenia k počítaču bude používateľ zakaždým informovaný, či je zariadenie povolené alebo blokované, a táto informácia sa tiež zaznamená do protokolu. Program si zariadenia nepamätá, čo znamená, že príslušné oznámenie sa zobrazí aj pri opätovnom pripojení rovnakého zariadenia.

Pre niektoré typy zariadení nemusia byť dostupné všetky akcie (povolenia). V prípade úložného zariadenia sú dostupné všetky štyri akcie. Ak ide o zariadenie, ktoré neslúži na ukladanie dát, sú k dispozícii len tri akcie (napríklad akcia **Blokovať zápis** nie je dostupná pri Bluetooth zariadeniach, takže tieto zariadenia sa dajú len povoliť, blokovať alebo na ne upozorniť).

Typ kritéria

Zvoľte **Zariadenie** alebo **Skupinu zariadení**.

Nasledujúce parametre možno použiť na vyladenie pravidiel pre rôzne zariadenia. V parametroch sa rozlišujú veľké a malé písmená a sú podporované zástupné znaky (*, ?):

- **Výrobca** – filtrovanie podľa názvu výrobcu alebo ID.
- **Model** – názov daného zariadenia.
- **Sériové číslo** – externé zariadenia zvyčajne majú svoje vlastné sériové číslo. V prípade CD/DVD ide o sériové číslo daného média, nie CD mechaniky.

> Ak sú vyššie uvedené údaje prázdne, pravidlo bude tieto polia ignorovať. Pri parametroch filtrovania sa vo všetkých textových poliach rozlišujú veľké a malé písmená a sú podporované zástupné znaky, pričom otáznik (?) nahrádza jeden znak, zatiaľ čo hviezdička (*) nahrádza reťazec v dĺžke nula až viac znakov.

> Na zistenie parametrov zariadenia pripojeného k počítaču najprv vytvorte pravidlo pre daný typ zariadenia a po pripojení zariadenia k počítaču zistite jeho parametre v Protokole správy zariadení.

Závažnosť zapisovania do protokolu

ESET Internet Security ukladá všetky dôležité udalosti do protokolov, ktoré môžete zobraziť priamo z hlavného menu programu. Kliknite na **Nástroje** > **Protokoly** a z roletového menu **Protokoly** vyberte možnosť **Správa zariadení**.

- **Vždy** – zaznamenáva všetky udalosti.
- **Diagnostické** – zaznamenáva do protokolu informácie dôležité pre ladenie programu.
- **Informácie** – zaznamenáva informatívne správy, napríklad o úspešnej aktualizácii, ako aj všetky záznamy vyššie.
- **Upozornenie** – zaznamenáva kritické chyby a varovné správy.
- **Žiadne** – nebudú vytvárané žiadne protokoly.

Zoznam používateľov

Pravidlá je možné priradiť ku konkrétnym používateľom alebo skupine používateľov kliknutím na **Upraviť** vedľa popisu **Zoznam používateľov**.

- **Pridať** – otvorí sa okno **Vybrať objekty typu: Používatelia alebo Skupiny**, kde je možné vybrať konkrétnych používateľov.
- **Odstrániť** – vybraný používateľ bude odstránený z filtra.

Obmedzenia v zozname používateľov

Zoznam používateľov nie je možné definovať pre pravidlá so špecifickými typmi zariadení:

- USB tlačiareň
- Zariadenie Bluetooth
- Čítačka smart kariet
- Obrazové zariadenie
- Modem
- Port LPT/COM

Upozorniť používateľa – pri vložení zariadenia blokovaného existujúcim pravidlom sa zobrazí okno s oznámením.

Skupiny zariadení

Zariadenia pripojené k vášmu počítaču môžu predstavovať bezpečnostné riziko.

Okno Skupiny zariadení je rozdelené na dve časti. Naľavo sa nachádza zoznam vytvorených skupín a napravo zoznam zariadení patriacich do konkrétnej skupiny. Vyberte skupinu zariadení, ktorej zariadenia chcete zobraziť v pravej časti okna.

Ak otvoríte okno Skupiny zariadení a označíte vytvorenú skupinu, môžete pridať alebo odstrániť zariadenia zo zoznamu. Ďalším spôsobom, ako pridať zariadenia do skupiny, je importovať zoznam zariadení zo súboru. Prípadne môžete kliknúť na tlačidlo **Načítať** a všetky zariadenia pripojené k vášmu počítaču sa zobrazia v okne **Zistené zariadenia**. Vyberte zariadenie z načítaného zoznamu a pridajte ho do skupiny kliknutím na **OK**.

Ovládacie prvky

Pridať – môžete pridať skupinu zariadení alebo zariadenie do existujúcej skupiny v závislosti od toho, v ktorej časti okna kliknete na tlačidlo.

Upraviť – môžete zmeniť názov vybranej skupiny alebo parametre vybraného zariadenia (výrobcu, model, sériové číslo).

Odstrániť – odstráni vybranú skupinu alebo zariadenie v závislosti od toho, v ktorej časti okna kliknete na tlačidlo.

Import – importuje zoznam zariadení z textového súboru. Súbor musí spĺňať nasledujúci formát:

- Každé zariadenie začína na novom riadku.
- Pre každé zariadenie musí byť uvedený **Výrobca**, **Model** a **Sériové číslo**, pričom tieto informácie sú oddelené čiarkou.

Príklad obsahu textového súboru:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Export – vyexportuje zoznam zariadení do súboru.

Tlačidlo **Načítať** zobrazí okno so zoznamom práve pripojených zariadení s nasledujúcimi informáciami: typ zariadenia, výrobca, model a sériové číslo v prípade, že je dostupné.

Pridanie zariadenia

Ak chcete pridať zariadenie do existujúcej skupiny, kliknite na tlačidlo **Pridať** v pravom okne. Nasledujúce parametre možno použiť na vyladenie pravidiel pre rôzne zariadenia. V parametroch sa rozlišujú veľké a malé písmená a sú podporované zástupné znaky (*, ?):

- **Výrobca** – filtrovanie podľa názvu výrobcu alebo ID.
- **Model** – názov daného zariadenia.
- **Sériové číslo** – externé zariadenia zvyčajne majú svoje vlastné sériové číslo. V prípade CD/DVD ide o sériové číslo daného média, nie CD mechaniky.
- **Popis** – popis zariadenia pre lepšiu organizáciu.

Ak uvedené parametre nie sú zadefinované, pravidlo nebude tieto polia brať do úvahy. Pri parametroch filtrovania sa vo všetkých textových poliach rozlišujú veľké a malé písmená a sú podporované zástupné znaky, pričom otáznik (?) nahrádza jeden znak, zatiaľ čo hviezdička (*) nahrádza reťazec núl alebo viacerých znakov.

Kliknite na **OK** pre uloženie zmien. Ak chcete opustiť okno **Skupiny zariadení** bez uloženia zmien, kliknite na **Zrušiť**.

Po vytvorení skupiny zariadení musíte pridať nové pravidlo správy zariadení pre vytvorenú skupinu zariadení a vybrať akciu, ktorá sa má vykonať.

Pre niektoré typy zariadení nemusia byť dostupné všetky akcie (povolenia). V prípade úložného zariadenia sú dostupné všetky štyri akcie. Ak ide o zariadenie, ktoré neslúži na ukladanie dát, sú k dispozícii len tri akcie (napríklad akcia **Blokovať zápis** nie je dostupná pri Bluetooth zariadeniach, takže tieto zariadenia sa dajú len povoliť, blokovať alebo na ne upozorniť).

Ochrana webovej kamery

Ochrana webovej kamery vás upozorní na procesy a aplikácie, ktoré využívajú alebo majú prístup k webovej kamere vášho počítača. V prípade, že sa aplikácia pokúša získať prístup k vašej webovej kamere, zobrazí sa okno oznámenia, v ktorom môžete prístup k webovej kamere **povoliť** alebo **zablokovať**. Farba zobrazeného okna oznámenia závisí od toho, akú úroveň rizika pre danú aplikáciu evidujeme.

Nastavenia ochrany webovej kamery je možné meniť v Rozšírených nastaveniach > **Ochrana** > **Správa zariadení** > **Ochrana webovej kamery**.

Ak chcete v programe ESET Internet Security aktivovať funkciu Ochrana webovej kamery, povoľte možnosť **Zapnúť ochranu webovej kamery**.

Následne sa aktivujú **Pravidlá** a budete môcť otvoriť Editor pravidiel.

Ak chcete vypnúť upozornenia na aplikácie s existujúcim pravidlom, ktoré boli zmenené, ale stále majú platný digitálny podpis (napr. v prípade aktualizácie aplikácie), zapnite možnosť **Nezobrazovať upozornenia na prístup k webovej kamere pri zmenených aplikáciách**.

Editor pravidiel ochrany webovej kamery

Toto okno zobrazuje existujúce pravidlá a umožňuje regulovať na základe vami vybraných akcií aplikácie a procesy, ktoré využívajú alebo majú prístup k webovej kamere vášho počítača.

Sú dostupné tieto akcie:

- **Povoliť prístup**
- **Blokovať prístup**

- **Spýtať sa** (pri každom pokuse niektorej aplikácie o prístup k webovej kamere sa používateľovi zobrazí oznámenie)

Ak nechcete dostávať oznámenia pri prístupe aplikácií k webovej kamere, zrušte označenie začiarkavacieho políčka v stĺpci **Oznámiť**.

> **Ilustrované inštrukcie**
> Ako vytvoriť a upraviť pravidlá ochrany webovej kamery v programe ESET Internet Security.

ThreatSense

ThreatSense je názov technológie, ktorú tvorí súbor komplexných metód detekcie infiltrácií. Táto technológia je proaktívna, takže poskytuje ochranu aj počas prvých hodín šírenia novej hrozby. K odhaleniu hrozieb využíva kombináciu niekoľkých metód (analýza kódu, emulácia kódu, generické signatúry, generické a vírusové definície),

čím efektívne spája ich výhody. Detekčné jadro je schopné kontrolovať niekoľko dátových tokov paralelne, a tak maximalizovať rýchlosť a účinnosť detekcie. Technológia ThreatSense dokáže úspešne eliminovať aj rootkity.

Nastavenia ThreatSense vám umožňujú špecifikovať viacero parametrov kontroly:

- typy súborov a prípony, ktoré sa majú kontrolovať,
- kombinácie rôznych metód detekcie,
- úrovne liečenia atď.

Pre zobrazenie okna s nastaveniami kliknite na **ThreatSense** v Rozšírených nastaveniach príslušných modulov využívajúcich technológiu ThreatSense (pozrite nižšie). Odlišné bezpečnostné scenáre si vyžadujú rôzne nastavenia. Technológia ThreatSense je osobitne nastaviteľná pre tieto moduly:

- Rezidentná ochrana súborového systému
- Kontrola v nečinnosti
- Kontrola pri štarte
- Ochrana dokumentov
- Ochrana e-mailových klientov
- Ochrana prístupu na web
- Kontrola počítača

Parametre ThreatSense sú pre každý modul odlišné. Zmeny v nastavení týchto parametroch môžu výrazne ovplyvniť celkový výkon systému. Príkladom môže byť povolenie pokročilej heuristiky v rámci modulu rezidentnej ochrany súborového systému a voľba vždy kontrolovať runtime archívy, čo môže viesť k spomaleniu systému (pri predvolenom nastavení sú pri týchto metódach kontrolované iba novovytvorené súbory). Preto odporúčame ponechať pôvodné nastavenia ThreatSense pre všetky moduly ochrany okrem Kontroly počítača.

Objekty na kontrolu

Táto sekcia umožňuje nastaviť, ktoré komponenty počítača a súborového systému budú testované na prítomnosť infiltrácií.

Operačná pamäť – slúži na kontrolu prítomnosti hrozieb, ktoré môžu byť zavedené v operačnej pamäti počítača.

Zavádzacie sektory/UEFI – kontroluje zavádzacie sektory na prítomnosť malvéru v hlavnom zavádzacom zázname. Viac o UEFI sa dočítate v slovníku pojmov.

E-mailové súbory – program podporuje nasledujúce prípony súborov: DBX (Outlook Express) a EML.

Archívy – program podporuje nasledujúce prípony: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE a mnoho ďalších.

Samorozbaľovacie archívy – archívy, ktoré nepotrebujú pre svoje rozbalenie iné programy. Ide o SFX (self-extracting) archívy.

Runtime archívy – runtime archívy sa na rozdiel od štandardných archívov po spustení rozbalia v pamäti počítača. Okrem štandardných statických archívov (UPX, yoda, ASPack, FSG atď.) dokáže program rozpoznať vďaka emulácii kódu aj veľa iných typov archívov.

Možnosti kontroly

V tejto sekcii môžete nastaviť, ktoré metódy detekcie sa použijú pri kontrole systému na prítomnosť infiltrácií. K dispozícii sú nasledujúce možnosti:

Heuristika – heuristika je algoritmus, ktorý analyzuje (škodlivú) aktivitu programov. Výhodou heuristiky je schopnosť odhaliť aj taký škodlivý softvér, ktorý v dobe poslednej aktualizácie modulu detekčného jadra programu ešte neexistoval alebo nebol pokrytý. Nevýhodou je (veľmi malá) pravdepodobnosť „falošného poplachu“.

Pokročilá heuristika/DNA vzorky – pokročilá heuristika je jedinečný algoritmus vyvinutý spoločnosťou ESET, ktorý je optimalizovaný pre odhaľovanie počítačových červov a trójskych koní písaných vo vyšších programovacích jazykoch. Použitie pokročilej heuristiky značne zvyšuje možnosti rozpoznávania vírusov a malvéru. Vzorky umožňujú spoľahlivo odhaliť a identifikovať nové vírusy. Vďaka pravidelnej aktualizácii sú nové vzorky k dispozícii zvyčajne už do niekoľkých hodín od objavenia hrozby. Nevýhodou je, že táto metóda odhaľuje iba vírusy na základe známych vzoriek, prípadne ich čiastočne pozmenené verzie.

Liečenie

Nastavenia liečenia určujú správanie programu ESET Internet Security pri čistení infikovaných súborov. Sú dostupné 4 úrovne liečenia:

ThreatSense poskytuje nasledujúce úrovne nápravy (t. j. liečenia) v prípade detegovaných objektov:

Liečenie v ESET Internet Security

Úroveň liečenia	Popis
Vždy vyriešiť detekciu	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých zriedkavých prípadoch (napríklad pri systémových súboroch), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení.
Vyriešiť detekciu a ak to nie je možné, ponechať ju	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých prípadoch (napríklad pri systémových súboroch alebo archívoch s infikovanými aj neškodnými súbormi), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení.
Vyriešiť detekciu a ak to nie je možné, spýtať sa	Program sa pokúsi o liečenie detegovaného objektu. V niektorých prípadoch, keď nie je možné vykonať žiadnu akciu, sa koncovému používateľovi zobrazí interaktívne upozornenie, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Toto nastavenie sa odporúča vo väčšine prípadov.
Vždy sa spýtať koncového používateľa	Koncovému používateľovi sa pri liečení objektov zobrazí interaktívne okno, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Táto úroveň liečenia je určená pre pokročilých používateľov, ktorí vedia, ako postupovať pri detekciách.

Vylúčenia

Prípona je časť názvu súboru, spravidla oddelená bodkou. Prípona určuje typ a obsah súboru. V tejto časti nastavení ThreatSense zvolíte, ktoré typy súborov budú kontrolované.

Ostatné

V rámci konfigurácie parametrov ThreatSense pre Manuálnu kontrolu počítača sú v sekcii **Iné** k dispozícii aj nasledujúce možnosti:

Kontrolovať alternatívne dátové prúdy (ADS) – alternatívne dátové prúdy používané systémom NTFS sú asociácie k súborom a adresárom, ktoré sú pre bežné spôsoby kontroly neviditeľné. Veľký počet vírusov ich preto využíva na svoje maskovanie a ukrytie sa pred prípadným odhalením.

Kontroly na pozadí vykonávať s nízkou prioritou – každá kontrola počítača využíva isté množstvo systémových prostriedkov. Ak práve pracujete s programami náročnými na výkon počítača, presunutím kontroly na pozadie jej môžete priradiť nižšiu prioritu a získať tým viac systémových prostriedkov pre svoje aplikácie.

Zapisovať všetky objekty do protokolu – protokol kontroly zobrazí všetky skontrolované súbory v samorozbaľovacích archívoch, a to aj súbory, ktoré neboli infikované (môže tak dochádzať ku generovaniu veľkého množstva dát a viesť k veľkému súboru protokolu kontroly).

Zapnúť Smart optimalizáciu – pri zapnutej Smart optimalizácii sa použijú optimálne nastavenia na zabezpečenie najefektívnejšej úrovne kontroly pri zachovaní najvyššej možnej rýchlosti kontroly. Moduly ochrany pri kontrole dômyselne využívajú rozdielne metódy kontroly pre rôzne typy súborov. Ak je Smart optimalizácia vypnutá, pri kontrole sú použité len používateľské nastavenia jadra ThreatSense pre konkrétne moduly.

Zachovať čas posledného prístupu k súborom – pri kontrole súboru nebude zmenený čas prístupu, ale bude ponechaný pôvodný (vhodné pri používaní zálohovacích systémov).

Obmedzenia

V sekcii Obmedzenia môžete nastaviť maximálnu veľkosť kontrolovaných objektov a maximálnu hĺbku kontroly v archívoch.

Nastavenie objektov

Maximálna veľkosť objektu – definuje maximálnu veľkosť skenovaného objektu. Daný modul antivírusu bude kontrolovať len objekty s menšou veľkosťou, ako je definovaná hodnota. Tieto hodnoty odporúčame meniť len pokročilým používateľom, ktorí chcú veľké objekty z určitého dôvodu vylúčiť z kontroly. Predvolená hodnota: neobmedzené.

Maximálny čas kontroly objektu (v sekundách) – definuje maximálny povolený čas na kontrolu súborov v objekte kontajnera (napr. archívy RAR/ZIP alebo e□mail s viacerými prílohami). Toto nastavenie sa netýka samostatných súborov. Ak používateľ zadefinuje určitú hodnotu, po prekročení uvedeného času sa prebiehajúca kontrola skončí bez ohľadu na to, či bol skontrolovaný každý súbor v objekte kontajnera.
V prípade archívu s veľkými súbormi sa kontrola zastaví až po extrahovaní súboru z archívu (napríklad keď používateľ zadefinuje premennú 3 sekundy, ale extrakcia súboru trvá 5 sekúnd). Po uplynutí tohto času sa zostávajúce súbory v archíve nebudú kontrolovať.
Na obmedzenie času kontroly (aj v prípade väčších archívov) použite možnosť **Maximálna veľkosť objektu** a **Maximálna veľkosť súboru v archíve** (neodporúča sa z dôvodu možných bezpečnostných rizík).

Predvolená hodnota: neobmedzené.

Nastavenie kontroly archívov

Úroveň vnorenia archívov – špecifikuje maximálny počet vnorených archívov, do ktorého bude prebiehať antivírusová kontrola. Predvolená hodnota: 10.

Maximálna veľkosť súboru v archíve – špecifikuje maximálnu veľkosť rozbalených súborov v archíve, ktoré sa majú kontrolovať. Maximálna hodnota je **3 GB**.

Neodporúčame meniť predvolené hodnoty, za normálnych okolností nie je žiadny dôvod na ich zmenu.

Úrovne liečenia

Ak chcete zmeniť nastavenia úrovne liečenia pre požadovaný modul ochrany, rozbaľte sekciu **ThreatSense** (napríklad **Rezidentnú ochranu súborového systému**) a potom v roletovom menu vyberte možnosť **Úroveň liečenia**.

ThreatSense poskytuje nasledujúce úrovne nápravy (t. j. liečenia) v prípade detegovaných objektov:

Liečenie v ESET Internet Security

Úroveň liečenia	Popis
Vždy vyriešiť detekciu	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých zriedkavých prípadoch (napríklad pri systémových súboroch), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení.
Vyriešiť detekciu a ak to nie je možné, ponechať ju	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých prípadoch (napríklad pri systémových súboroch alebo archívoch s infikovanými aj neškodnými súbormi), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení.
Vyriešiť detekciu a ak to nie je možné, spýtať sa	Program sa pokúsi o liečenie detegovaného objektu. V niektorých prípadoch, keď nie je možné vykonať žiadnu akciu, sa koncovému používateľovi zobrazí interaktívne upozornenie, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Toto nastavenie sa odporúča vo väčšine prípadov.
Vždy sa spýtať koncového používateľa	Koncovému používateľovi sa pri liečení objektov zobrazí interaktívne okno, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Táto úroveň liečenia je určená pre pokročilých používateľov, ktorí vedia, ako postupovať pri detekciách.

Prípony súborov vylúčené z kontroly

Vylúčené prípony súborov sú súčasťou nastavení ThreatSense. Ak chcete nakonfigurovať vylúčené prípony súborov, v okne rozšírených nastavení kliknite na **ThreatSense** v rámci ktoréhokoľvek modulu, ktorý využíva technológiu ThreatSense.

Prípona je časť názvu súboru, spravidla oddelená bodkou. Prípona určuje typ a obsah súboru. V tejto časti nastavení ThreatSense zvolíte, ktoré typy súborov budú kontrolované.

Je potrebné rozlišovať vylúčenia procesov, HIPS vylúčenia a vylúčenia súborov/priečinkov.

Prednastavená je kontrola všetkých súborov bez ohľadu na príponu. Do zoznamu súborov vylúčených z kontroly môže byť pridaná akákoľvek prípona.

Vylúčenie prípony z kontroly je rozumné použiť napr. vtedy, keď kontrola určitého typu súboru spôsobuje nesprávne fungovanie daného programu. Odporúča sa napríklad vylúčiť súborové prípony `.edb`, `.eml` a `.tmp` v prípade, že používate Microsoft Exchange server.

Ak chcete pridať novú príponu do zoznamu, kliknite na **Pridať**. Zadajte príponu (napr. tmp) a kliknite na tlačidlo **OK**. Ak označíte možnosť **Zadať viaceré hodnoty**, môžete do textového poľa zadať viacero prípon oddelených riadkami, čiarkami alebo bodkočiarkami (z roletového menu pre oddeľovač viacerých hodnôt vyberte napríklad **Bodkočiarku** a zadajte prípony v tvare `edb;eml;tmp`).
Môžete použiť aj špeciálny znak ? (otáznik). Otáznik nahrádza akýkoľvek znak (napríklad `?db`).

Ak chcete vidieť presnú príponu (ak existuje) súboru v operačnom systéme Windows, vo **Windows Prieskumníkovi** musíte na karte **Zobraziť** začiarknuť políčko **Prípony názvov súborov**.

Doplňujúce parametre ThreatSense

Ak chcete upraviť tieto nastavenia, prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Rezidentná ochrana súborového systému** > **Doplňujúce parametre ThreatSense**.

Doplňujúce parametre ThreatSense pre vytvárané a menené súbory

Pravdepodobnosť napadnutia novovytvorených alebo upravovaných súborov je vyššia ako pri existujúcich súboroch. To je dôvod, prečo program tieto súbory kontroluje s prídavnými parametrami. ESET Internet Security využíva metódy kontroly na základe porovnávania vzoriek spoločne s pokročilou heuristikou, vďaka ktorej možno zachytiť nové hrozby skôr, ako vyjde aktualizácia detekčného jadra.

Okrem novovytvorených súborov sa kontrolujú aj **samorozbaľovacie archívy** (.sfx) a **runtime archívy** (interne komprimované spustiteľné súbory). Predvolene sa archívy kontrolujú až po desiatu vnorenú úroveň a bez ohľadu na ich veľkosť. Ak chcete zmeniť nastavenia kontroly archívov, zrušte označenie možnosti **Predvolené nastavenie kontroly archívov**.

Doplňujúce parametre ThreatSense pre spúšťané súbory:

Pokročilá heuristika pri spustení súboru – predvolene sa pokročilá heuristika používa pri spúšťaní súborov. Ak je zapnutá, odporúčame ponechať zapnutú aj Smart optimalizáciu a ESET LiveGrid®, čím zmiernite vplyv na výkon systému.

Pokročilá heuristika pri spustení súboru z vymeniteľného média – pokročilá heuristika emuluje kód vo virtuálnom prostredí a vyhodnocuje jeho správanie pred tým, ako je kódu umožnené sa spustiť z vymeniteľného média.

Nástroje

V časti Rozšírené nastavenia > **Nástroje**môžete nakonfigurovať pokročilé nastavenia funkcií, ktoré ponúkajú dodatočné zabezpečenie a pomáhajú zjednodušiť správu produktu ESET Internet Security.

- Aktualizácia Microsoft Windows®
- ESET CMD
- Protokoly
- Herný režim
- Diagnostika

Aktualizácia Microsoft Windows®

Aktualizácie operačného systému predstavujú dôležitú súčasť zabezpečenia ochrany používateľov pred zneužitím bezpečnostných zraniteľností a možným infikovaním systému. Preto je dôležité inštalovať aktualizácie systému Microsoft Windows hneď, ako sú dostupné. ESET Internet Security vás informuje o chýbajúcich systémových aktualizáciách na úrovni, ktorú je možné nastaviť v sekcii Rozšírené nastavenia > **Nástroje**. Sú dostupné tieto úrovne:

- **Žiadne aktualizácie** – Nebudú ponúkané žiadne aktualizácie.
- **Voliteľné aplikácie** – Budú ponúkané aktualizácie s nízkou prioritou a všetky nasledovné.
- **Odporúčané aktualizácie** – budú ponúkané bežné aktualizácie a všetky nasledovné.
- **Dôležité aktualizácie** – Budú ponúkané dôležité aktualizácie a všetky nasledovné.
- **Kritické aktualizácie** – Budú ponúkané len kritické aktualizácie.

Dialógové okno – Systémové aktualizácie

Ak sú k dispozícii aktualizácie pre váš operačný systém, v hlavnom okne programu ESET Internet Security v časti **Prehľad** sa zobrazí príslušné oznámenie. Po kliknutí na možnosť **Viac informácií** sa zobrazí okno s aktualizáciami systému.

Okno Aktualizácie systému zobrazuje dostupné aktualizácie, ktoré je možné stiahnuť a nainštalovať. Vedľa názvu aktualizácie je zobrazená jej priorita.

Dvojitým kliknutím na riadok v zozname sa zobrazí okno Informácie o aktualizácii s dodatočnými informáciami.

Kliknutím na **Spustiť aktualizáciu systému** sa stiahnu a nainštalujú všetky zobrazené aktualizácie operačného systému.

Informácie o aktualizácii

Okno Aktualizácie systému zobrazuje zoznam dostupných aktualizácií, ktoré je možné stiahnuť a nainštalovať. Vedľa názvu aktualizácie je zobrazená jej priorita.

Kliknutím na **Spustiť aktualizáciu systému** sa začne sťahovanie a inštalácia aktualizácií operačného systému.

Pravým kliknutím na riadok v zozname a vybratím možnosti **Zobraziť informácie** z kontextového menu sa zobrazí okno s informáciami o aktualizácii.

ESET CMD

Táto funkcia umožňuje používať pokročilé príkazy ecmd. Poskytuje vám možnosť exportovať a importovať nastavenia pomocou príkazového riadka (ecmd.exe). Doposiaľ bolo možné exportovať nastavenia len prostredníctvom grafického používateľského rozhrania. Nastavenia programu ESET Internet Security môžu byť exportované ako súbor *.xml*.

Po aktivovaní funkcie ESET CMD sú k dispozícii dve metódy autorizácie:

- **Žiadna** – žiadna autorizácia. Túto metódu neodporúčame, pretože umožňuje importovanie akejkoľvek nepodpísanej konfigurácie, čo môže predstavovať potenciálne riziko.

- **Heslo pre prístup k rozšíreným nastaveniam** – v rámci autorizácie bude použité heslo, ktoré chráni prístup k nastaveniam programu. Import konfigurácie zo súboru .xml bude umožnený, len ak je daný súbor podpísaný s použitím príslušného hesla (pozrite si sekciu týkajúcu sa podpisovania konfiguračných súborov .xml uvedenú nižšie). Táto metóda autorizácie overuje heslo počas importovania konfigurácie s cieľom zistiť, či je dané heslo zhodné s heslom zadaným v sekcii Nastavenia prístupu. Ak nemáte nastavenú ochranu prístupu pomocou hesla, heslá sa nezhodujú alebo konfiguračný súbor .xml nie je podpísaný, konfigurácia nebude importovaná.

S aktívnou funkciou ESET CMD môžete na import/export konfigurácie programu ESET Internet Security používať príkazový riadok. Príkazy môžete spúšťať manuálne alebo si vytvoriť skript na účely automatizácie.

Na použitie pokročilých ecmd príkazov musíte mať oprávnenia správcu, resp. spustiť príkazový riadok systému Windows (cmd) pomocou možnosti **Spustiť ako správca**. V opačnom prípade sa zobrazí chybové hlásenie **Error executing command**. Pri exportovaní konfigurácie musí tiež existovať cieľový priečinok. Export je možný aj v prípade, že funkcia ESET CMD je v nastaveniach vypnutá.

Konfiguráciu z nainštalovaného produktu vyexportujete príkazom:
```
ecmd /getcfg c:\config\settings.xml
```

Konfiguráciu do nainštalovaného produktu naimportujete príkazom:
```
ecmd /setcfg c:\config\settings.xml
```

Pokročilé ecmd príkazy môžu byť spúšťané len lokálne.

Ako podpísať konfiguračný súbor *.xml*:

1. Stiahnite si nástroj XmlSignTool.

2. Otvorte príkazový riadok systému Windows (cmd) použitím možnosti **Spustiť ako správca**.

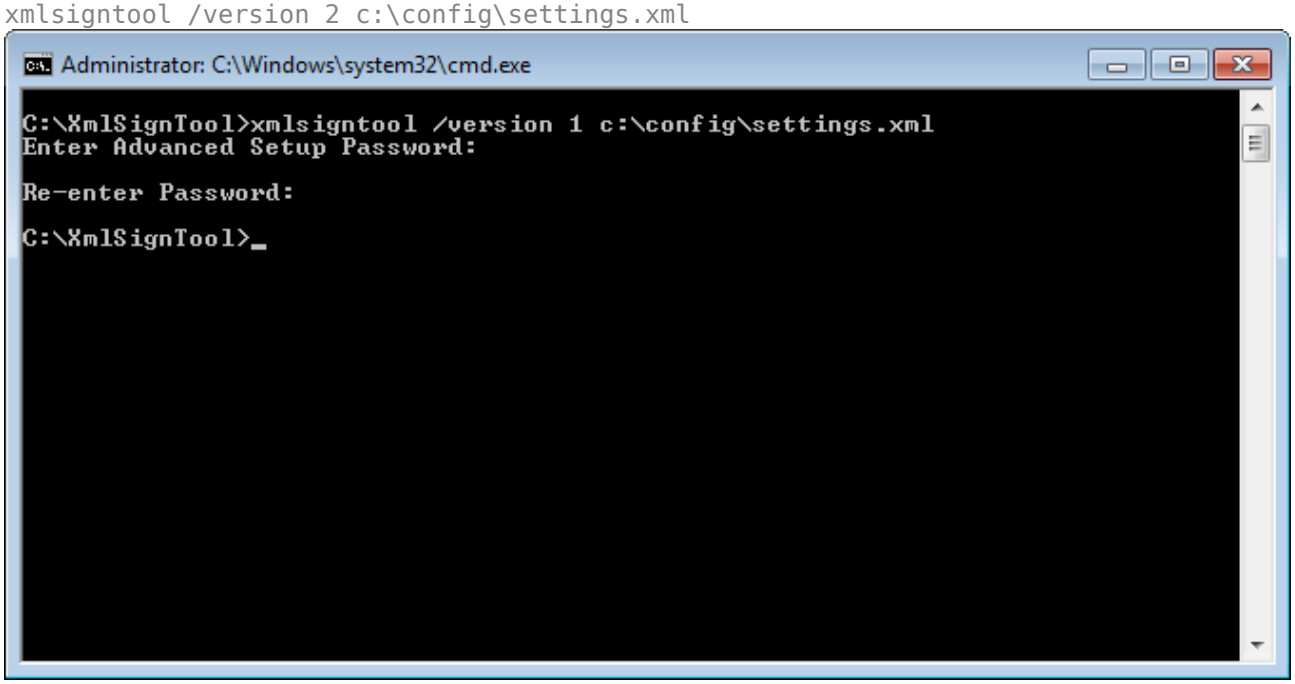
3. Prejdite do priečinka, do ktorého ste uložili spustiteľný súbor `xmlsigntool.exe`.

4. Konfiguračný súbor *.xml* podpíšte nasledujúcim príkazom: `xmlsigntool /version 1|2 <xml_file_path>`

Hodnota parametra `/version` závisí od verzie vášho programu ESET Internet Security. Pre verzie staršie ako ESET Internet Security 11.1 použite `/version 1`. Pre novšie verzie ESET Internet Security použite `/version 2`.

5. Po výzve nástroja XmlSignTool zadajte svoje heslo na ochranu prístupu do rozšírených nastavení. Váš konfiguračný súbor *.xml* je teraz podpísaný a môžete ho prostredníctvom ESET CMD importovať v rámci ďalšej inštalácie ESET Internet Security s využitím autorizácie heslom.

Vyexportovaný konfiguračný súbor podpíšete týmto príkazom:
`xmlsigntool /version 2 c:\config\settings.xml`



Ak sa zmení heslo pre prístup k nastaveniam, ktoré ste zadali v sekcii Nastavenia prístupu, a chcete do produktu naimportovať konfiguračný súbor, ktorý bol podpísaný už skôr pomocou starého hesla, bude potrebné daný konfiguračný súbor *.xml* najskôr opätovne podpísať pomocou vášho nového hesla. Týmto spôsobom môžete použiť a importovať aj starší konfiguračný súbor bez nutnosti ho najskôr exportovať na inom počítači s programom ESET Internet Security.

Aktivovanie ESET CMD bez zvolenia spôsobu autorizácie sa neodporúča, nakoľko sa týmto umožní import akejkoľvek nepodpísanej konfigurácie. Aby ste predišli neoprávneným zmenám zo strany používateľov, nastavte heslo v sekcii Rozšírené nastavenia > **Používateľské rozhranie** > **Nastavenia prístupu**.

Protokoly

Zapisovanie do protokolov v programe ESET Internet Security nastavíte v sekcii Rozšírené nastavenia > **Nástroje** > **Protokoly**. Nastavenia protokolov umožňujú špecifikovať spôsoby manažovania protokolov. Manažment protokolov automaticky vymazáva staré protokoly, čím sa šetrí miesto na disku. Je možné definovať tieto vlastnosti protokolov:

Ukladať záznamy od úrovne – úroveň, od ktorej sa budú zaznamenávať udalosti do protokolov.

- **Diagnostické** – zaznamenávané budú informácie dôležité pre ladenie programu, ako aj všetky udalosti s

vyššou závažnosťou.

• **Informatívne** – zaznamenávané budú informatívne správy, napríklad o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.

• **Upozornenia** – zaznamenávané budú varovné správy a kritické chyby.

• **Chyby** – zaznamenávané budú chyby typu „Chyba pri preberaní súboru“ a kritické chyby.

• **Kritické** – zaznamenávané budú len kritické chyby (chyba pri spustení antivírusovej ochrany, Firewallu a podobne).

Ak vyberiete diagnostickú úroveň podrobnosti protokolov, všetky blokované pripojenia budú zaznamenávané.

Protokoly staršie ako nastavená hodnota v poli **Automaticky mazať záznamy protokolov staršie ako (dní)** budú automaticky zmazané.

Automaticky optimalizovať protokoly – umožňuje automatickú defragmentáciu protokolov, ak počet nevyužitých záznamov prekročí špecifikovaný pomer v percentách nastavený v poli **Pri prekročení počtu nevyužitých záznamov (%)**.

Kliknite na **Optimalizovať** teraz pre spustenie defragmentácie protokolov. Defragmentácia odstraňuje prázdne záznamy v protokoloch, čím sa zefektívni a zrýchli práca s nimi. Viditeľné zlepšenie práce s protokolmi po optimalizácii je očividné hlavne pri väčších množstvách záznamov v protokoloch.

Funkcia **Zapnúť textový protokol** umožňuje okrem klasického ukladania v sekcii Protokoly ukladať súbory protokolov aj v ďalšom formáte:

• **Cieľový priečinok** – priečinok, do ktorého sa budú ukladať protokoly (platí len pre Text/CSV). Každá skupina protokolov má vlastný súbor s predvoleným názvom (napríklad virlog.txt sú protokoly skupiny **Detekcie** v prípade, že ste zvolili ukladanie protokolov do textového súboru).

• **Typ** – ak zvolíte formát **Text**, protokoly sa budú ukladať do textového súboru, pričom údaje budú oddelené tabulátorom. Formát **CSV** tiež predstavuje textové súbory, avšak oddelené čiarkami. Ak vyberiete možnosť **Udalosť**, protokoly budú ukladané v denníku udalostí systému Windows, ktorý si môžete prezrieť cez Zobrazovač denníka udalostí (Event Viewer) v Ovládacom paneli.

• **Odstrániť všetky protokoly** – vymaže všetky uložené protokoly označené v roletovom menu **Typ**. Zobrazí sa vám tiež oznámenie o úspešnom odstránení protokolov.

Na urýchlenie riešenia problémov vás môže technická podpora spoločnosti ESET vyzvať na zaslanie protokolov z vášho počítača. Nástroj ESET Log Collector zjednodušuje zozbieranie potrebných protokolov. Viac informácií o nástroji ESET Log Collector nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Herný režim

Herný režim je funkcia určená pre používateľov, ktorí chcú svoj softvér používať neprerušovane a neželajú si byť vyrušovaní oknami s oznámeniami/upozorneniami, pričom taktiež požadujú minimálne vyťaženie procesora (CPU) antivírusom. Herný režim je možné použiť aj pri prezentáciách, ktoré by mohli byť prerušené aktivitou

antivírusového programu. Zapnutím herného režimu budú okamžite zastavené a potlačené všetky upozornenia programu a aktivity plánovača. Samotná ochrana je aj naďalej spustená na pozadí, avšak nevyžaduje žiadne zásahy používateľa.

Herný režim môžete zapnúť alebo vypnúť v hlavnom okne programu v časti **Nastavenia** > **Ochrana počítača** kliknutím na  alebo  vedľa položky **Herný režim**. Zapnutie herného režimu môže predstavovať potenciálne bezpečnostné riziko, a preto sa ikonka ochrany na lište zmení na oranžovú. Zobrazí sa tiež oranžové varovné hlásenie v hlavnom okne programu: **Herný režim je aktívny**.

Po povolení možnosti **Automaticky zapnúť herný režim, ak je spustená aplikácia na celú obrazovku** v sekcii Rozšírené nastavenia > **Nástroje** > **Herný režim** sa herný režim automaticky zapne vždy pri spustení aplikácie na celú obrazovku a po jej skončení sa vypne.

Môžete si tiež zvoliť možnosť **Automaticky vypnúť herný režim po** a zadať čas, po ktorom sa herný režim automaticky vypne.

Ak je firewall v interaktívnom režime a zapnete herný režim, môžete mať ťažkosti s pripojením na internet. To môže byť problém, ak napríklad spustíte hru, ktorá sa pripája na internet. Je to spôsobené tým, že za bežných okolností by si firewall vyžiadal používateľské potvrdenie pripojenia (ak nie sú definované žiadne pravidlá alebo výnimky pre spojenia), ale v hernom režime sú všetky vyskakovacie okná vypnuté. Na povolenie komunikácie je potrebné definovať pravidlá komunikácie pre každú aplikáciu, ktorá by mohla byť v konflikte s týmto správaním, alebo zvoliť iný Režim filtrovania v sekcii Firewall. Majte tiež na pamäti, že ak pri zapnutom hernom režime pracujete s aplikáciou alebo webovou stránkou, ktorá predstavuje potenciálne riziko, bude zablokovaná. Nezobrazí sa však žiadne vysvetlenie alebo upozornenie, pretože sú vypnuté všetky akcie vyžadujúce zásah používateľa.

Diagnostika

Diagnostika poskytuje výpisy zlyhaní procesov ESET (napr. ekrn). Ak aplikácia prestane fungovať, vygeneruje sa výpis. Toto môže vývojárom pomôcť pri diagnostike a oprave rôznych problémov súvisiacich s ESET Internet Security.

Kliknite na roletové menu vedľa položky **Typ výpisu** a vyberte jednu z troch dostupných možností:

- Vyberte možnosť **Žiadny**, ak chcete vypnúť túto funkciu.

- **Skrátený** (predvolené) – zaznamená menší súbor užitočných informácií, ktoré môžu pomôcť identifikovať príčinu nečakaného zastavenia aplikácie. Tento druh výpisu môže byť užitočný, keď je obmedzený priestor na disku. Vzhľadom na obmedzené množstvo zahrnutých informácií však nemusia byť analýzou tohto výpisu objavené chyby, ktoré neboli priamo spôsobené procesom bežiacim v čase problému.

- **Úplný** – zaznamená celý obsah systémovej pamäte, keď sa aplikácia nečakane zastaví. Kompletný výpis z pamäte môže obsahovať dáta procesov, ktoré bežali v čase, keď bol výpis zozbieraný.

Cieľový priečinok – priečinok, do ktorého sa pri zlyhaní vygeneruje výpis.

Otvoriť diagnostický priečinok – na otvorenie cieľového adresára v novom okne nástroja *Windows Prieskumník* kliknite na **Otvoriť**.

Vytvoriť diagnostický výpis – kliknite na tlačidlo **Vytvoriť** pre vytvorenie diagnostických súborov výpisu v

Cieľovom adresári.

Vytváranie rozšírených protokolov

Zapnúť rozšírené protokoly marketingových správ – umožňuje zaznamenávať všetky udalosti súvisiace so zasielaním marketingových správ do produktu.

Zapnúť rozšírené protokoly antispamového jadra – umožňuje zaznamenávať všetky udalosti, ktoré sa vyskytnú počas antispamovej kontroly. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace s Antispamovým jadrom ESET.

Zapnúť rozšírené protokoly jadra Anti-Theft – umožňuje zaznamenávať všetky udalosti modulu Anti-Theft pre umožnenie diagnostiky a riešenia problémov.

Zapnúť rozšírené protokoly ochrany prehliadača – umožňuje zaznamenávať všetky udalosti modulu Ochrana pri platbách a prehliadaní.

Zapnúť rozšírené protokoly kontroly počítača – umožňuje zaznamenávať všetky udalosti, ku ktorým dôjde počas kontroly súborov a priečinkov Kontrolou počítača.

Zapnúť rozšírené protokoly správy zariadení – umožňuje zaznamenávať všetky udalosti modulu Správa zariadení. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace so Správou zariadení.

Zapnúť rozšírené protokoly Direct Cloud – umožňuje zaznamenávať všetky udalosti modulu ESET LiveGrid®. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace s ESET LiveGrid®.

Zapnúť rozšírené protokoly ochrany dokumentov – umožňuje zaznamenávať všetky udalosti modulu Ochrana dokumentov, aby bolo možné jednoduchšie diagnostikovať a opraviť prípadné problémy.

Zapnúť rozšírené protokoly ochrany e mailových klientov – umožňuje zaznamenávať všetky udalosti týkajúce sa ochrany e mailových klientov a pluginu e mailových klientov s cieľom umožniť diagnostiku a riešenie problémov.

Zapnúť rozšírené protokoly jadra – umožňuje zaznamenávať všetky udalosti, ku ktorým dochádza v jadre ESET (ekrn).

Zapnúť rozšírené protokoly licencovania – umožňuje zaznamenávať všetku komunikáciu produktu s aktivačnými servermi alebo servermi ESET License Manager spoločnosti ESET.

Zapnúť sledovanie pamäte – umožňuje zaznamenávať všetky udalosti, ktoré pomôžu vývojárom diagnostikovať úniky pamäte.

Zapnúť rozšírené protokoly ochrany siete – umožňuje zaznamenávať všetky sieťové dáta prechádzajúce firewallom vo formáte PCAP. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy týkajúce sa firewallu.

Zapnúť rozšírené protokoly kontroly sieťovej komunikácie – umožňuje zaznamenávať všetky dáta prechádzajúce kontrolou sieťovej komunikácie vo formáte PCAP. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy týkajúce sa kontroly sieťovej komunikácie.

Zapnúť rozšírené protokoly operačného systému – umožňuje zaznamenávať dodatočné informácie o operačnom systéme, ako sú spustené procesy, aktivita procesora a operácie disku. Toto môže pomôcť pri diagnostike a oprave problémov s produktom ESET spustenom na vašom operačnom systéme.

Zapnúť rozšírené protokoly rodičovskej kontroly – umožňuje zaznamenávať všetky udalosti modulu Rodičovskej kontroly. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace s Rodičovskou kontrolou.

Zapnúť rozšírené protokoly push správ – umožňuje zaznamenávať všetky udalosti, ku ktorým dôjde pri zasielaní push správ.

Zapnúť rozšírené protokoly rezidentnej ochrany súborového systému – umožňuje zaznamenávať všetky udalosti, ku ktorým dôjde počas kontroly súborov a priečinkov Rezidentnou ochranou súborového systému.

Zapnúť rozšírené protokoly aktualizačného jadra – umožňuje zaznamenávať všetky udalosti, ktoré sa vyskytnú počas procesu aktualizácie. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace s aktualizačným jadrom.

Protokoly je možné nájsť v nasledujúcom umiestnení: *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Technická podpora

Keď kontaktujete technickú podporu spoločnosti ESET priamo z produktu ESET Internet Security, máte možnosť odoslať aj údaje o systémových nastaveniach. Ak chcete, aby sa údaje odosielali automaticky, z roletového menu **Odoslať systémové nastavenia** zvoľte možnosť **Vždy odosielať**. Ak chcete, aby sa pred odoslaním údajov zobrazovala výzva, vyberte možnosť **Spýtať sa pred odoslaním**.

Pripojenie

V určitých sieťach môže byť pripájanie počítačov na internet zabezpečované pomocou proxy servera. Ak používate proxy server, je potrebné špecifikovať jeho nastavenia. V opačnom prípade sa ESET Internet Security a moduly produktu nebudú môcť automaticky aktualizovať. V rámci ESET Internet Security je nastavenie proxy servera dostupné v dvoch rozličných častiach Rozšírených nastavení.

Globálne nastavenia proxy servera môžete nakonfigurovať v sekcii Rozšírené nastavenia > **Pripojenie** > **Proxy server**. Proxy server zadaný v tejto sekcii bude použitý programom ESET Internet Security ako globálne nastavenie proxy servera. Danými nastaveniami sa budú riadiť všetky moduly vyžadujúce prístup na internet.

Ak chcete špecifikovať globálne nastavenia proxy servera, aktivujte možnosť **Používať proxy server** a zadajte adresu **proxy servera** spolu s číslom **portu**.

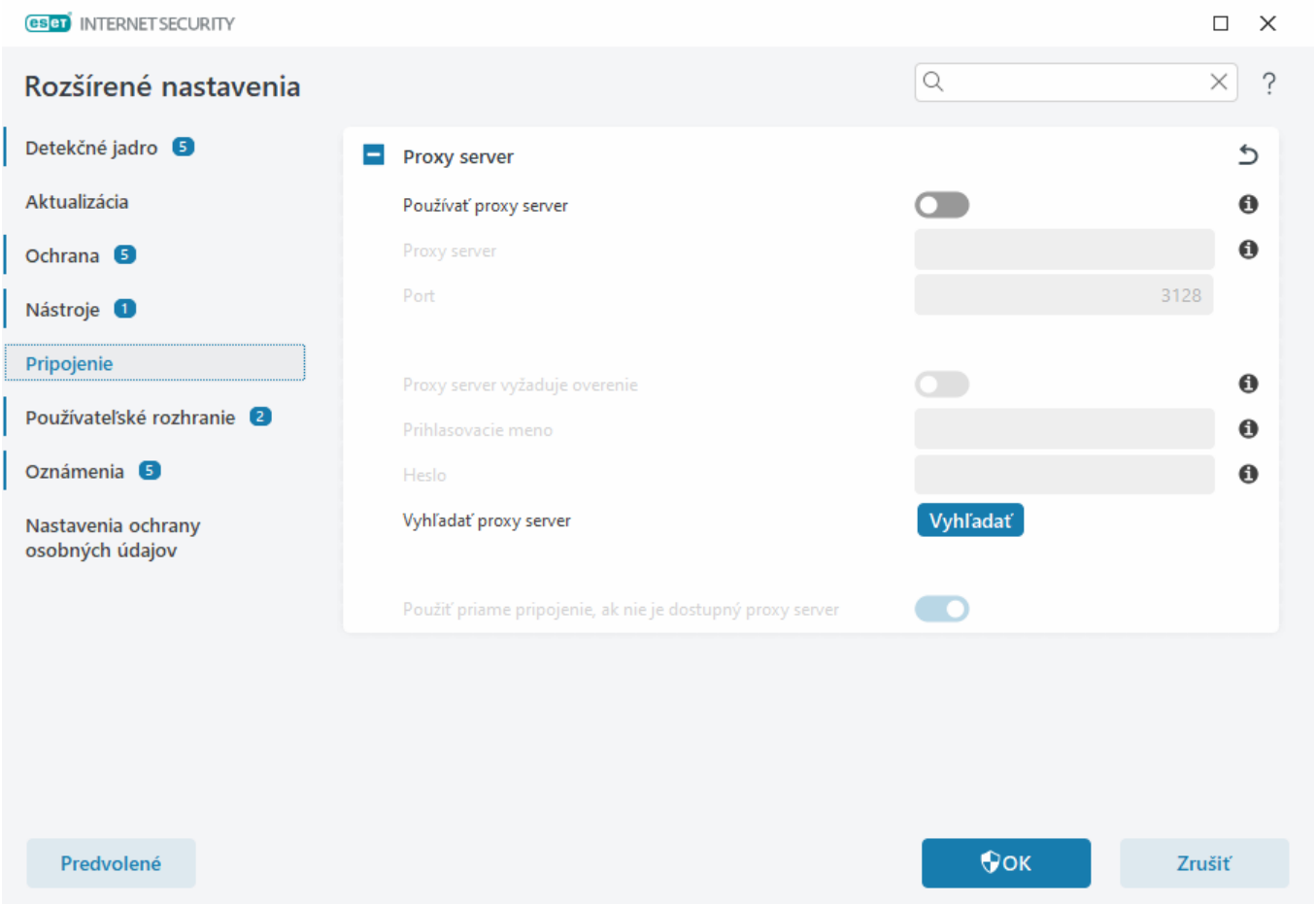
V prípade, že si komunikácia s proxy serverom vyžaduje overenie, vyberte možnosť **Proxy server vyžaduje overenie** a do príslušných polí zadajte platné **prihlasovacie meno** a **heslo**. Kliknutím na možnosť **Vyhľadať proxy server** sa automaticky nájdu a vyplnia nastavenia proxy servera. ESET Internet Security skopíruje parametre špecifikované pre Internet Explorer alebo Google Chrome.

Budete musieť manuálne zadať prihlasovacie meno a heslo v sekcii **Proxy server**.

Použiť priame pripojenie, ak proxy nie je k dispozícii – ak je produkt ESET Internet Security nakonfigurovaný tak, aby sa pripájal cez proxy, no proxy nie je dostupné, ESET Internet Security sa pokúsi pripojiť na servery spoločnosti ESET priamo.

Nastavenia proxy servera môžete nakonfigurovať aj v sekcii Rozšírené nastavenia > **Aktualizácia** > **Profily** > **Aktualizácie** > **Možnosti pripojenia** po zvolení možnosti **Pripojenie prostredníctvom proxy servera** v roletovom

menu **Režim proxy**. Táto konfigurácia sa vzťahuje len na aktualizácie a odporúča sa pre prenosné počítače, ktoré prijímajú aktualizácie modulov zo vzdialených miest. Ďalšie informácie nájdete v kapitole Pokročilé nastavenia aktualizácie.



Používateľské rozhranie

Ak chcete nakonfigurovať správanie grafického používateľského rozhrania (GUI) programu, otvorte Rozšírené nastavenia > **Používateľské rozhranie**.

V sekcii Prvky používateľského rozhrania môžete nastaviť vizuálnu stránku programu a použité efekty.

Odinštalovaniu alebo neoprávneným zmenám v konfigurácii vášho bezpečnostného produktu ESET môžete predchádzať prostredníctvom ochrany nastavení heslom, ktorú nastavíte v časti Nastavenia prístupu.

Možnosti na zmenu správania systémových oznámení, upozornení pri detekcii a stavov aplikácie nájdete v sekcii Oznámenia.

Prvky používateľského rozhrania

Nastavenia pracovného prostredia programu ESET Internet Security (GUI) môžete podľa potreby meniť v časti Rozšírené nastavenia > **Používateľské rozhranie** > **Prvky používateľského rozhrania**.

Farebný režim – v roletovom menu zvoľte farebný motív grafického rozhrania ESET Internet Security:

• **Rovnaký ako systémová farba** – farebný motív programu ESET Internet Security sa nastaví podľa operačného systému.

• **Tmavý** – ESET Internet Security bude mať tmavý motív (tmavý režim).

• **Svetlý** – ESET Internet Security bude mať štandardný svetlý motív.

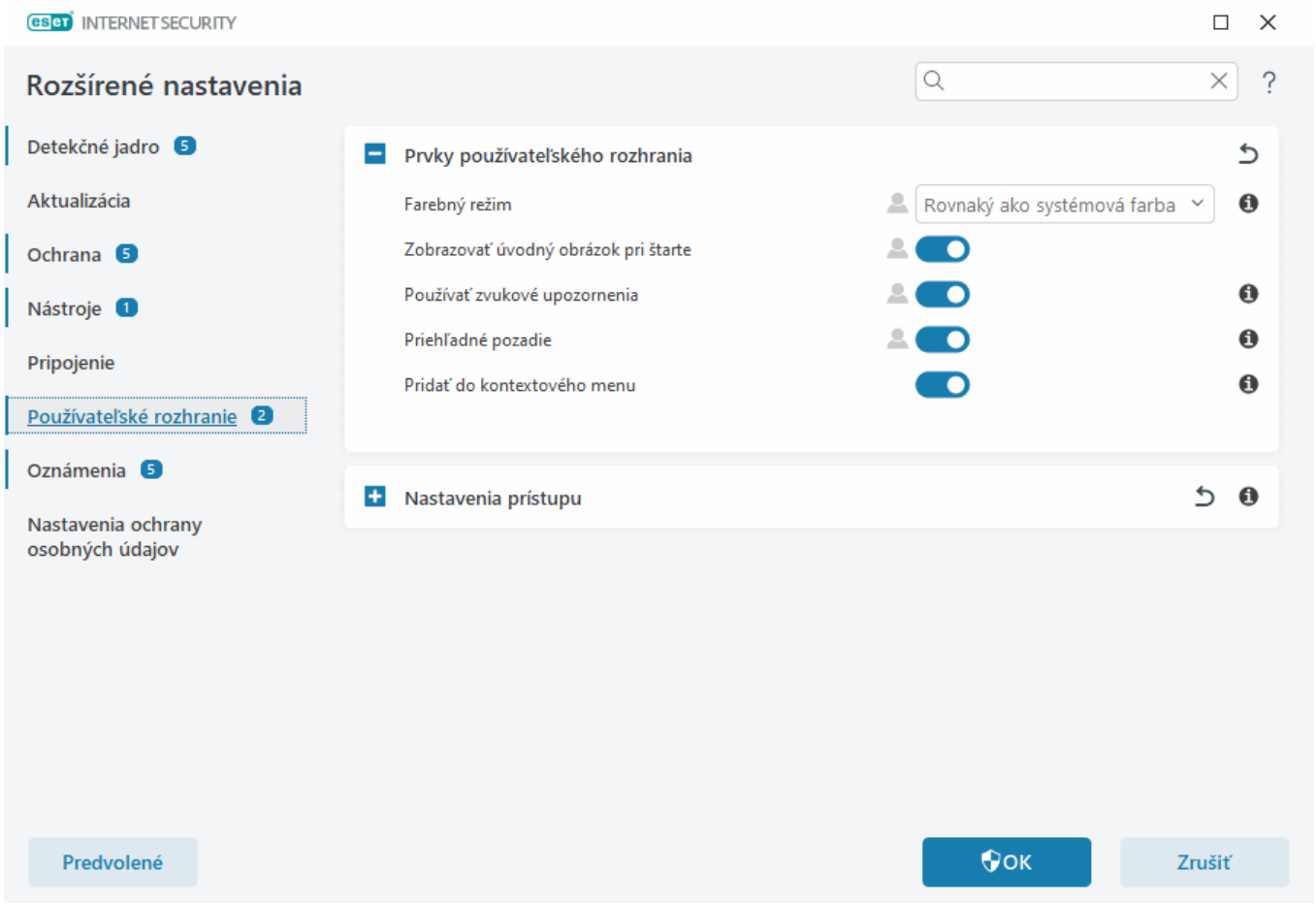
Farebný motív grafického rozhrania ESET Internet Security môžete vybrať aj v pravom hornom rohu hlavného okna programu.

Zobrazovať úvodný obrázok pri štarte – pri štarte sa bude zobrazovať úvodný obrázok programu ESET Internet Security.

Používať zvukové upozornenia – program bude signalizovať dôležité udalosti pomocou zvukových efektov (napríklad pri nájdení hrozby pri kontrole počítača alebo po dokončení kontroly).

Priehľadné pozadie – umožňuje zapnúť efekt priehľadného pozadia hlavného okna programu. Priehľadné pozadie je k dispozícii len pre najnovšie verzie systému Windows (RS4 a novšie).

Pridať do kontextového menu – integruje ovládacie prvky programu ESET Internet Security do kontextového menu systému.



Nastavenia prístupu

Správne nastavenie ESET Internet Security je veľmi dôležité pre zachovanie celkovej bezpečnosti vášho systému. Neoprávnené zmeny nastavení môžu vystaviť systém nebezpečenstvu a ohroziť tým stabilitu a ochranu vášho

systému. Aby ste predišli neoprávneným zmenám nastavení alebo neželanému odinštalovaniu produktu, rozšírené nastavenia ESET Internet Security sa dajú ochrániť heslom. Nastavenia prístupu je možné konfigurovať v sekcii Rozšírené nastavenia > **Používateľské rozhranie** > **Nastavenia prístupu**.

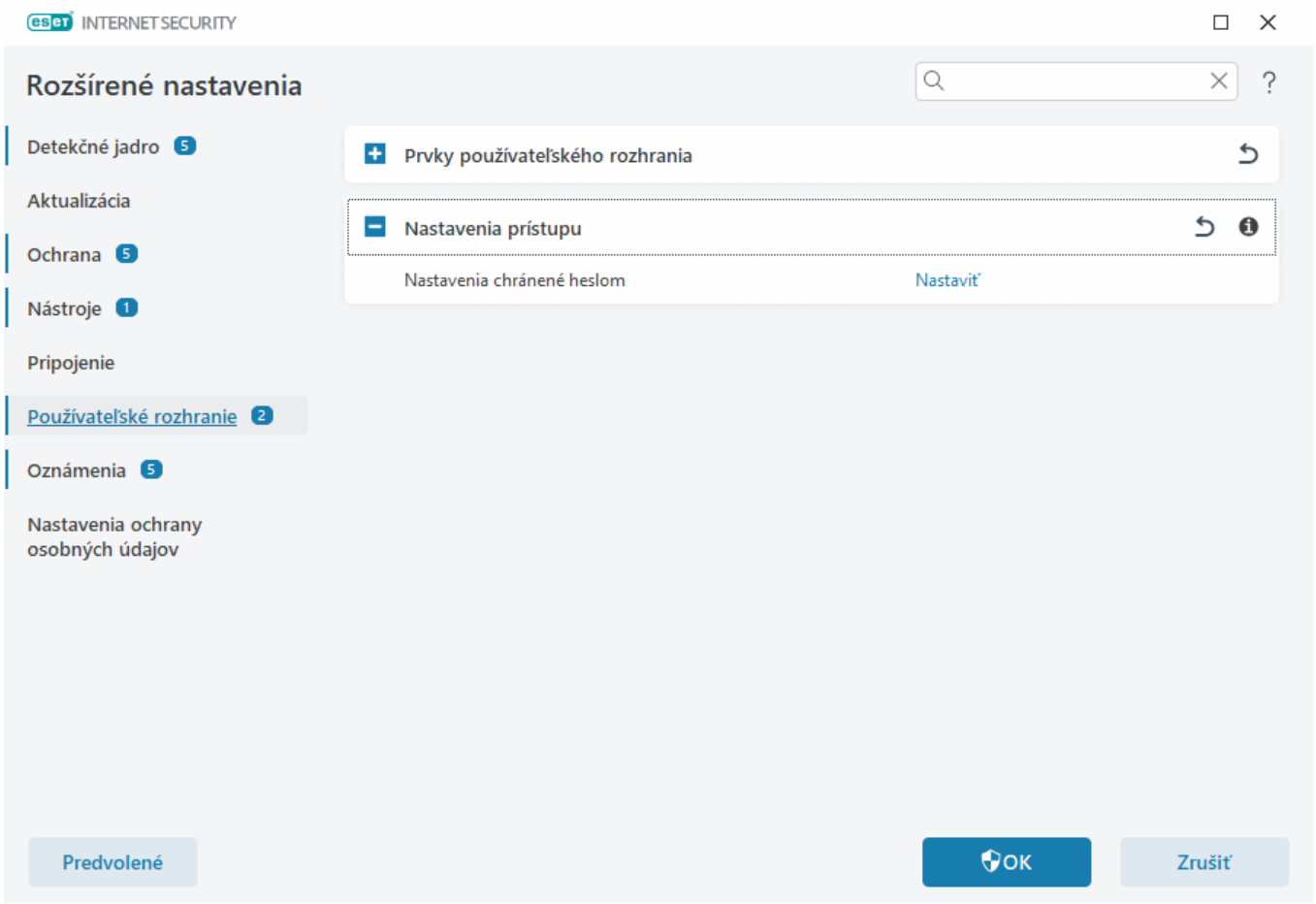
Ak si chcete nastaviť heslo na ochranu prístupu k nastaveniam a na ochranu pred neoprávneným odinštalovaním ESET Internet Security, kliknite na možnosť **Nastaviť** vedľa popisu **Nastavenia chránené heslom**.

Ak máte aktivovanú ochranu rozšírených nastavení programu a pokúsite sa o prístup k týmto nastaveniam, zobrazí sa vám okno s výzvou na zadanie príslušného hesla. Ak ste toto heslo zabudli alebo stratili, kliknite na možnosť **Obnoviť heslo** a zadajte e-mailovú adresu, ktorú ste uviedli pri nákupe/registrácii predplatného. Spoločnosť ESET vám na túto adresu zašle e-mail s overovacím kódom a inštrukciami, ako obnoviť vaše heslo.

- Ako obnoviť prístup k rozšíreným nastaveniam

Ak chcete zmeniť heslo, kliknite na možnosť **Zmeniť heslo** vedľa popisu **Ochrana nastavení heslom**.

Ak chcete odstrániť heslo, kliknite na možnosť **Odstrániť** vedľa popisu **Ochrana nastavení heslom**.



Heslo na ochranu rozšírených nastavení

Na ochranu rozšírených nastavení produktu ESET Internet Security a zabránenie neoprávneným zmenám zadajte nové heslo do polí **Nové heslo** a **Potvrdiť heslo**. Kliknite na tlačidlo **OK**.

V prípade, že chcete zmeniť existujúce heslo:

1. Zadajte pôvodné heslo do poľa **Staré heslo**.

2. Zadajte nové heslo do polí **Nové heslo** a **Potvrdiť heslo**.

3. Kliknite na tlačidlo **OK**.

Toto heslo sa bude vyžadovať pri prístupe k rozšíreným nastaveniam.

V prípade, že heslo zabudnete, si prečítajte článok Ako obnoviť heslo pre prístup k programovým nastaveniam v produktoch ESET pre domácnosti.

Ak chcete získať späť svoj stratený aktivačný kľúč ESET, zistiť dátum konca platnosti predplatného alebo iné informácie týkajúce sa vášho predplatného k produktu ESET Internet Security, prečítajte si článok Zabudol som svoj aktivačný kľúč.

Podpora programov na čítanie textu z obrazovky

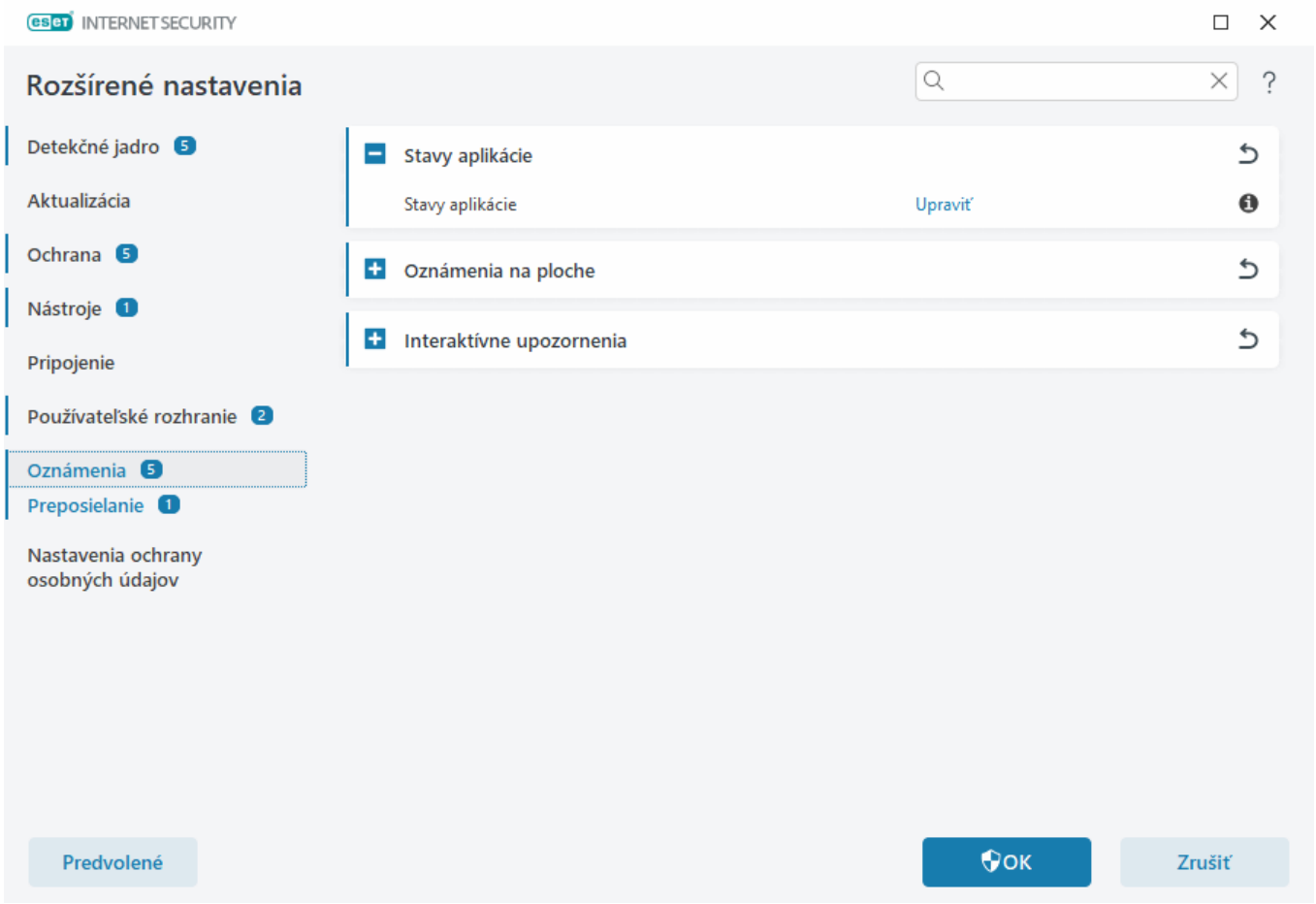
ESET Internet Security je možné používať s programami na čítanie textu z obrazovky, vďaka čomu sa používatelia so zrakovým postihnutím môžu orientovať v produkte alebo konfigurovať nastavenia. Podporované sú nasledujúce programy na čítanie z obrazovky: (JAWS, NVDA, Narrator).

Ak sa chcete uistiť, že softvér na čítanie z obrazovky má prístup ku grafickému rozhraniu programu ESET Internet Security, postupujte podľa inštrukcií v našom článku Databázy znalostí.

Oznámenia

Na správu oznámení v programe ESET Internet Security otvorte Rozšírené nastavenia > **Oznámenia**. Konfigurovať môžete nasledujúce typy oznámení:

- Stavy aplikácie – oznámenia, ktoré sa zobrazujú v hlavnom okne programu v sekcii **Prehľad**.
- Oznámenia na ploche – malé okná oznámení, ktoré sa zobrazujú vedľa systémového panela úloh.
- Interaktívne upozornenia – výstražné upozornenia a okná správ, ktoré si vyžadujú interakciu používateľa.
- Preposielanie (e□mailové oznámenia) – oznámenia zasielané na vopred špecifikovanú e□mailovú adresu.



Stavy aplikácie

Stavy aplikácie – po kliknutí na možnosť **Upraviť** môžete vybrať, ktoré stavy aplikácie sa budú zobrazovať v hlavnom okne programu v sekcii **Prehľad**.

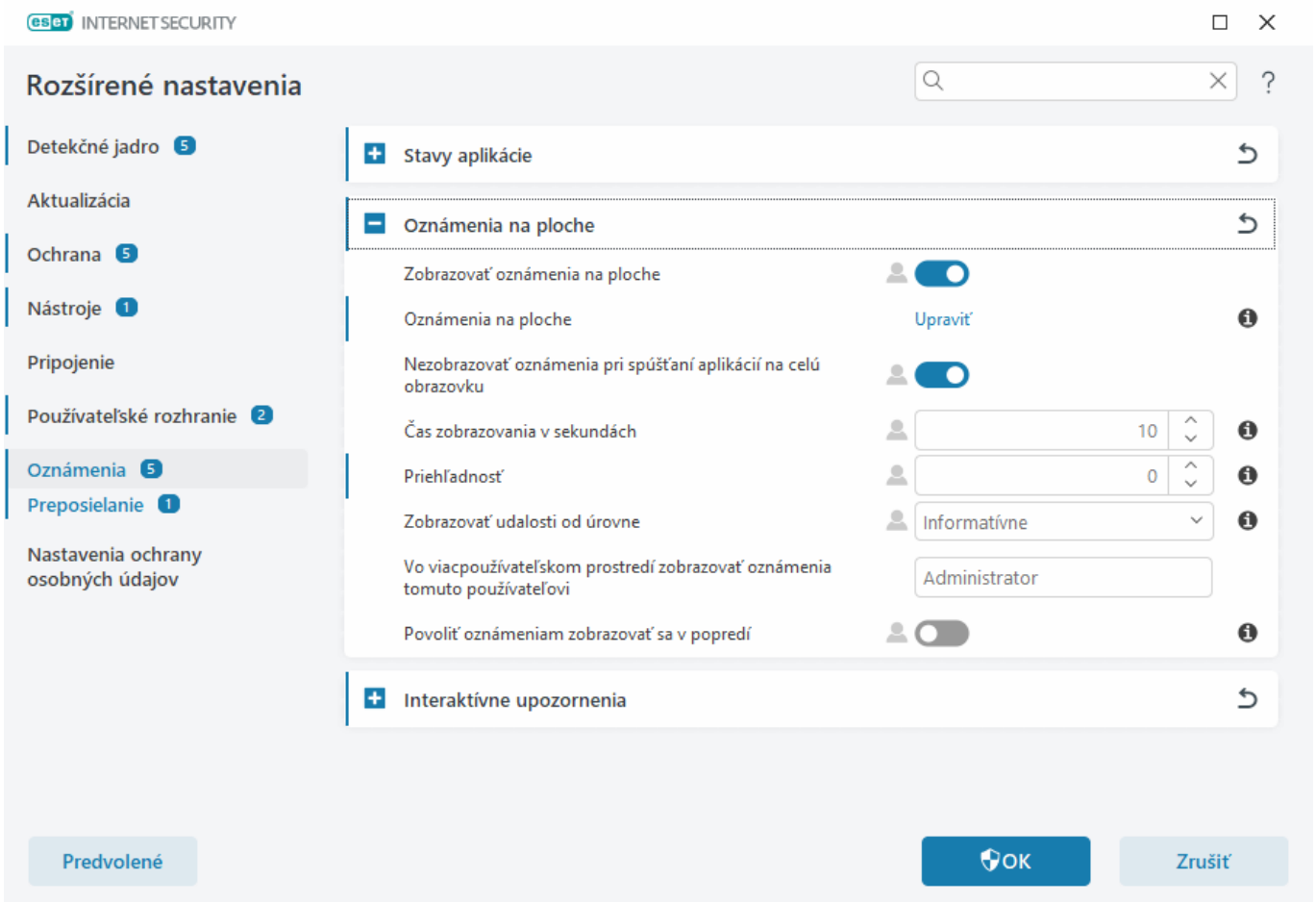
Dialógové okno – stavy aplikácie

V tomto dialógovom okne môžete vybrať stavy aplikácie, ktoré budú a, naopak, nebudú zobrazované. Napríklad zobrazovanie stavu pri pozastavení antivírusovej a antispyvérovej ochrany alebo pri spustení herného režimu.

Stav aplikácie bude zobrazený aj v prípade, že váš produkt nie je aktivovaný alebo vášmu predplatnému uplynula platnosť.

Oznámenia na ploche

Oznámenia na ploche sa zobrazujú v podobe malého okna s oznámením vedľa systémového panela úloh. Na základe predvolených nastavení sa okno oznámenia zobrazí na 10 sekúnd, potom pomaly zmizne. Oznámenia informujú používateľa o úspešných aktualizáciách produktu, nových pripojených zariadeniach, dokončených antivírusových kontrolách alebo nájdených hrozbách.



Zobrazovať oznámenia na ploche – odporúčame ponechať túto možnosť zapnutú, aby vás mohol produkt informovať o nových udalostiach.

Oznámenia na ploche – ak chcete zapnúť alebo vypnúť konkrétne oznámenia na ploche, kliknite na možnosť **Upraviť**.

Nezobrazovať oznámenia pri spúšťaní aplikácií na celú obrazovku – táto možnosť vám umožňuje potlačiť zobrazovanie všetkých oznámení, ktoré nevyžadujú interakciu používateľa, pri spúšťaní aplikácií v režime na celú obrazovku.

Čas zobrazovania v sekundách – umožňuje nastaviť, ako dlho bude oznámenie zobrazené na ploche. Hodnota musí byť v rozmedzí 3 – 30 sekúnd.

Priehľadnosť – umožňuje nastaviť priehľadnosť okna s oznámením. Podporované je rozmedzie od 0 (nepriehľadné okno) do 80 (veľmi vysoká priehľadnosť).

Zobrazovať udalosti od úrovne – umožňuje nastaviť, od akej úrovne závažnosti sa majú oznámenia zobrazovať. Z roletového menu vyberte jednu z týchto možností:

- **Diagnostické** – zobrazia sa informácie dôležité pre ladenie programu, ako aj všetky udalosti s vyššou závažnosťou.
- **Informatívne** – zobrazia sa informatívne správy, napríklad o neobvyklých sieťových aktivitách alebo o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.
- **Upozornenia** – zobrazia sa varovné správy a chyby vrátane kritických (napr. ak zlyhala aktualizácia).

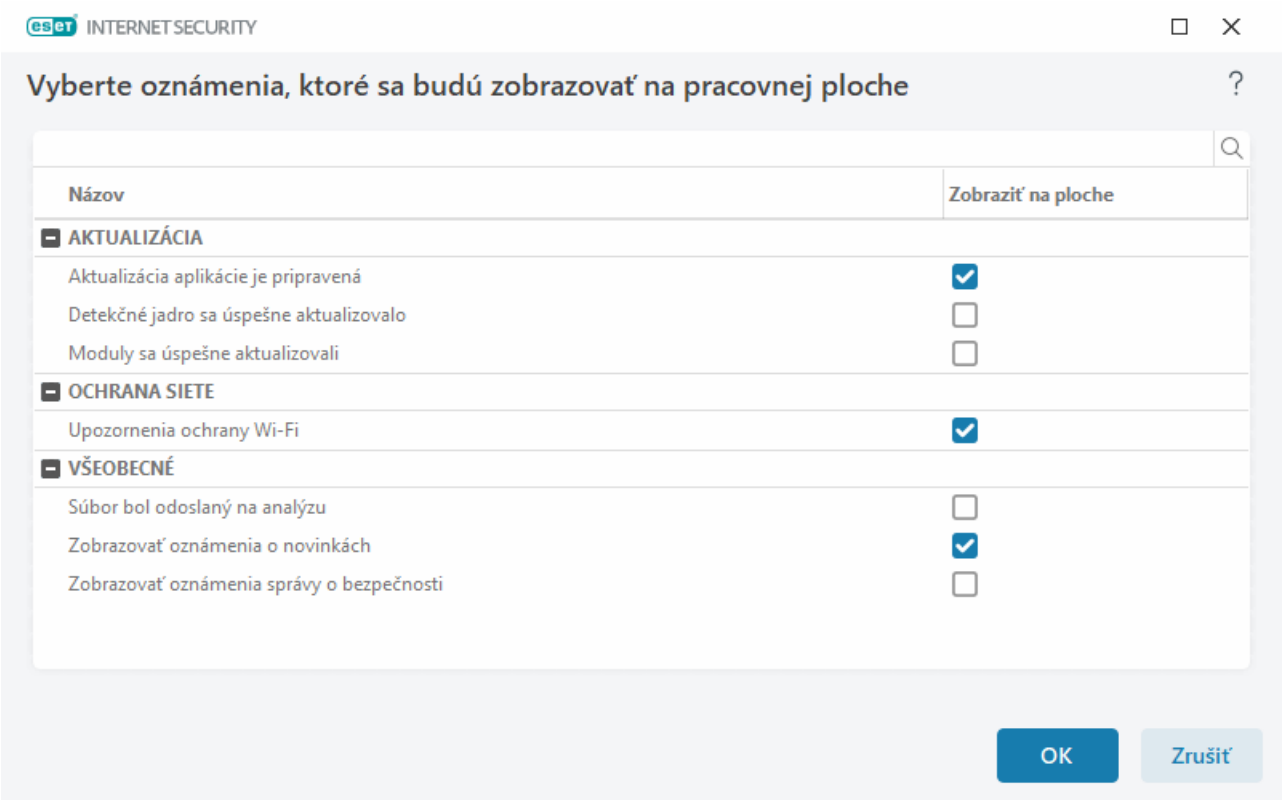
- **Chyby** – zobrazia sa chyby (napr. ochrana dokumentov nie je spustená) vrátane kritických chýb.
- **Kritické** – zobrazia sa len kritické chyby (napr. nespustenie antivírusovej ochrany alebo infikovaný systém).

Vo viacpoužívateľskom prostredí zobrazovať oznámenia tomuto používateľovi – umožňuje vybrať účet, ktorému sa budú zobrazovať oznámenia na ploche. Ak napríklad na počítači nepoužívate správcovský účet, zadajte celý názov používateľského účtu, ktorému sa majú oznámenia zobrazovať. Oznámenia na ploche môže dostávať len jeden používateľský účet.

Povoliť oznámeniam zobrazovať sa v popredí – oznámenia sa budú zobrazovať v popredí obrazovky a budú dostupné pomocou klávesovej skratky **Alt + Tab**.

Zoznam oznámení na ploche

Ak chcete upraviť zobrazovanie oznámení na ploche (v pravom dolnom rohu obrazovky), prejdite v Rozšírených nastaveniach do sekcie **Oznámenia** > **Oznámenia na ploche**. Kliknite na **Upraviť** vedľa popisu **Oznámenia na ploche** a v stĺpci **Zobraziť** označte príslušné políčka jednotlivých oznámení.



Všeobecné

Zobrazovať oznámenia správy o bezpečnosti – oznámenie sa vám zobrazí vždy vtedy, keď sa vygeneruje nová verzia Správy o bezpečnosti.

Zobrazovať oznámenia o novinkách – oznámenia o všetkých nových a vylepšených funkciách v najnovšej verzii produktu.

Súbor bol odoslaný na analýzu – oznámenie sa vám zobrazí vždy vtedy, keď ESET Internet Security odošle súbor na analýzu.

Strážca siete

Upozorniť na novoobjavené sieťové zariadenia – zobrazí sa vám oznámenie vždy, keď sa k sieti pripojí nové zariadenie.

Ochrana siete

Sieťový profil bol zmenený – oznámenie sa vám zobrazí v prípade, že došlo k zmene sieťového profilu.

Upozornenia ochrany Wi-Fi – pri pokuse o pripojenie k sieti Wi-Fi so slabým alebo žiadnym heslom dostanete upozornenie.

Aktualizácia

Aktualizácia aplikácie je pripravená – oznámenie sa vám zobrazí v prípade, že je k dispozícii aktualizácia na novú verziu produktu ESET Internet Security.

Detekčné jadro sa úspešne aktualizovalo – oznámenie sa vám zobrazí vždy vtedy, keď produkt aktualizuje svoje detekčné jadro.

Moduly sa úspešne aktualizovali – oznámenie sa vám zobrazí vždy vtedy, keď produkt aktualizuje svoje programové súčasti.

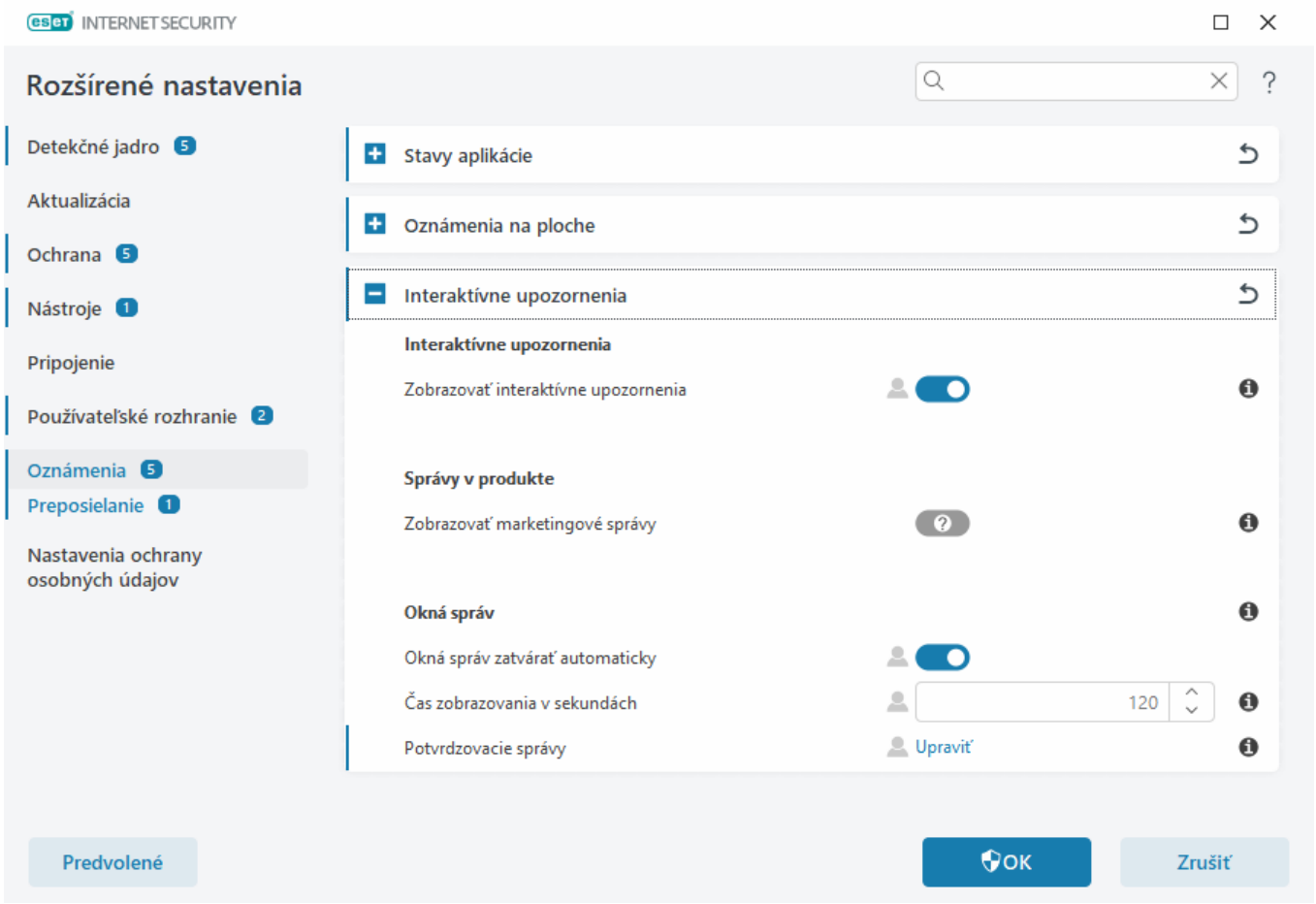
Ak chcete upraviť všeobecné nastavenia oznámení zobrazovaných na ploche (napríklad ako dlho má byť správa zobrazená alebo od akej úrovne závažnosti chcete byť o udalosti informovaný), prejdite do časti Oznámenia na ploche v Rozšírených nastaveniach po kliknutí na **Oznámenia**.

Interaktívne upozornenia

Hľadáte informácie o častých upozorneniach a oznámeniach?

- Našla sa hrozba
- Adresa bola zablokovaná
- Produkt nie je aktivovaný
- Zmena na produkt s väčším počtom funkcií
- Zmena na produkt s menším počtom funkcií
- Aktualizácia je k dispozícii
- Informácie o aktualizáciách nie sú konzistentné
- Riešenie chybového hlásenia „Aktualizácia modulov nebola úspešná“
- Riešenie problémov pri aktualizácii modulov
- Sieťová hrozba bola zablokovaná
- Certifikát webovej stránky bol zrušený

Interaktívne upozornenia v sekcii Rozšírené nastavenia > **Oznámenia** vám umožňujú nastaviť, ako má ESET Internet Security pracovať s upozorneniami na detekcie v prípade, že je potrebná interakcia používateľa (napr. potenciálne phishingové stránky).



Interaktívne upozornenia

Po vypnutí možnosti **Zobrazovať interaktívne upozornenia** sa nebudú zobrazovať žiadne okná upozornení ani dialógové okná prehliadača, avšak toto nastavenie je vhodné len v určitých situáciách. Odporúčame ponechať túto možnosť zapnutú.

Správy v produkte

Správy umiestňované priamo v produkte sú prostriedkom, ako môžeme používateľov informovať o novinkách a akciách od spoločnosti ESET. Zasielanie týchto marketingových informácií vyžaduje váš súhlas. Preto vám na základe predvolených nastavení nie sú zasielané žiadne marketingové správy (zobrazuje sa ikona otáznika). Aktivovaním tejto možnosti vyjadríte svoj súhlas s prijímaním marketingových informácií. Ak si takýto druh informácií neprajete dostávať, možnosť **Zobrazovať marketingové správy** deaktivujte.

Okná správ

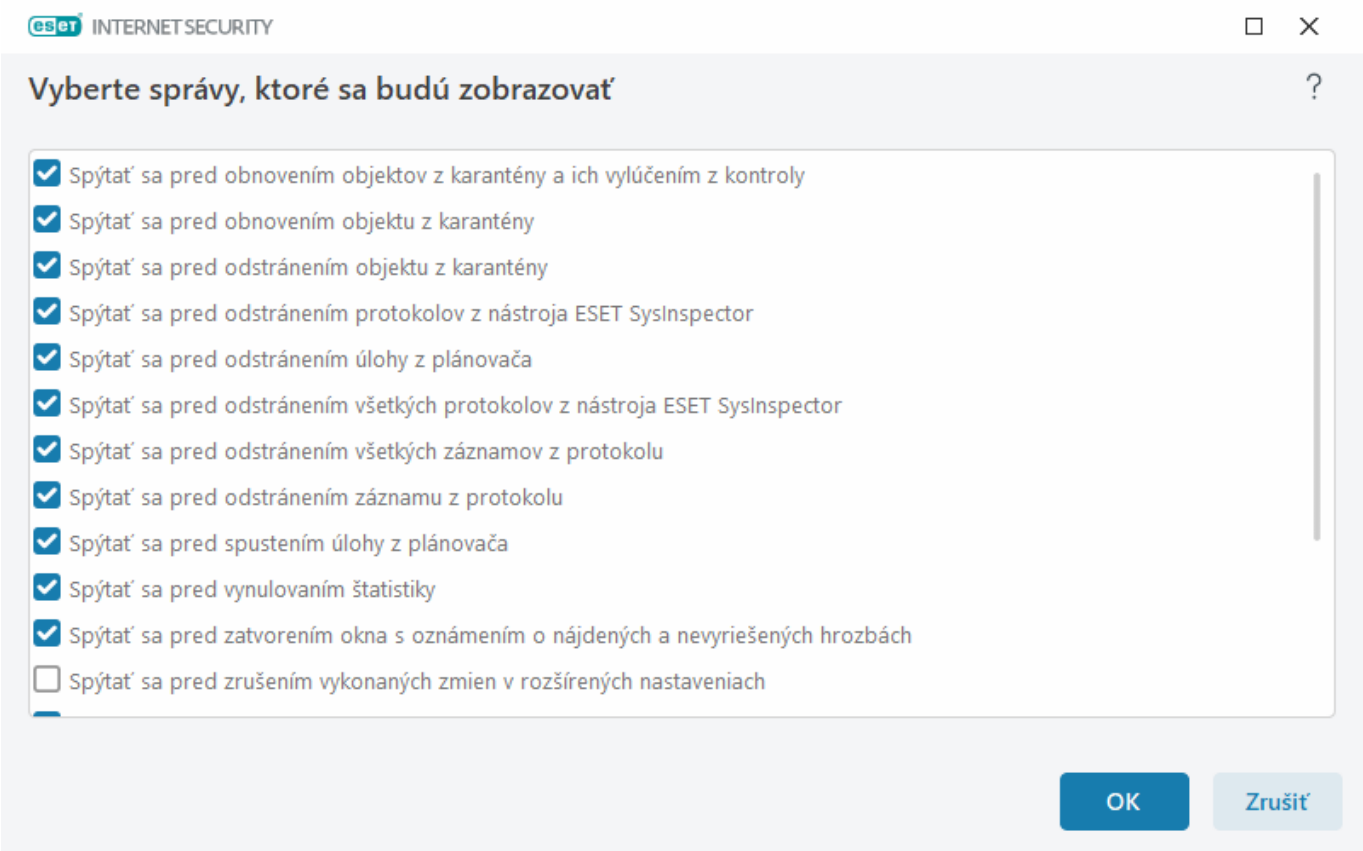
Ak si želáte, aby sa okná správ zatvárali automaticky po uplynutí určitého času, vyberte možnosť **Okná správ zatvárať automaticky**. Po uplynutí nastaveného času sa okno s oznámením zatvorí, ak tak dovtedy neurobí sám používateľ.

Čas zobrazovania v sekundách – umožňuje nastaviť, ako dlho bude upozornenie zobrazené. Hodnota musí byť v rozmedzí 10 – 999 sekúnd.

Potvrdzovacie správy – kliknutím na **Upraviť** si zobrazíte zoznam potvrdzovacích správ, pre ktoré môžete zvoliť, či sa majú alebo nemajú zobrazovať.

Potvrdzovacie správy

Ak chcete upraviť nastavenia potvrdzovacích správ, prejdite v Rozšírených nastaveniach do sekcie **Oznámenia** > **Interaktívne upozornenia** a vedľa popisu **Potvrdzovacie správy** kliknite na tlačidlo **Upraviť**.



Potvrdzovacie správy sa zobrazujú v programe ESET Internet Security pred vykonaním akcií. Môžete označiť začiarkavacie políčka vedľa jednotlivých potvrdzovacích správ, ak chcete ich zobrazovanie povoliť, alebo ak ich zobrazovanie chcete naopak zakázať, zrušte ich označenie.

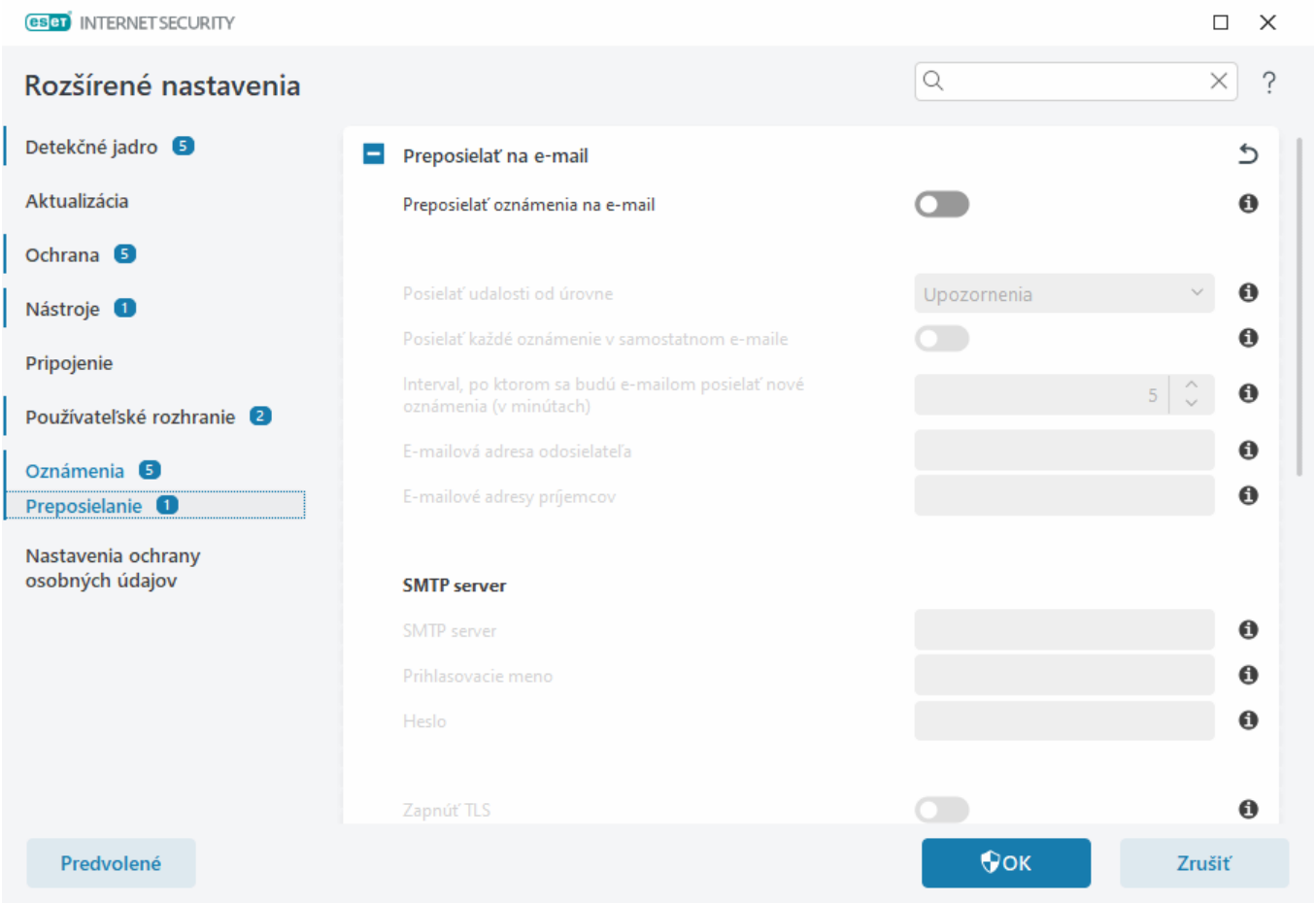
Na nasledujúcich odkazoch nájdete viac informácií o jednotlivých funkciách, ktorých sa potvrdzovacie správy týkajú:

- Spýtať sa pred odstránením protokolov z nástroja ESET SysInspector
- Spýtať sa pred odstránením všetkých protokolov z nástroja ESET SysInspector
- Spýtať sa pred odstránením objektu z karantény
- Spýtať sa pred zrušením vykonaných zmien v rozšírených nastaveniach
- Spýtať sa pred zatvorením okna s oznámením o nájdených a nevyriešených hrozbách
- Spýtať sa pred odstránením záznamu z protokolu
- Spýtať sa pred odstránením úlohy z plánovača
- Spýtať sa pred odstránením všetkých záznamov z protokolu
- Spýtať sa pred vynulovaním štatistiky

- Spýtať sa pred obnovením objektu z karantény
- Spýtať sa pred obnovením objektov z karantény a ich vylúčením z kontroly
- Spýtať sa pred spustením úlohy z plánovača
- Zobraziť oznámenia o výsledku antispamovej kontroly
- Zobraziť oznámenia o výsledku antispamovej kontroly pre e-mailové klienty
- Zobraziť potvrdzovacie dialógové okná produktu pre e-mailové klienty Outlook Express a Windows Mail
- Zobraziť potvrdzovacie dialógové okná produktu pre e-mailového klienta Windows Live Mail
- Zobraziť potvrdzovacie dialógové okná produktu pre e-mailového klienta Microsoft Outlook

Preposielanie

ESET Internet Security podporuje automatické odosielanie e-mailových oznámení pri výskyte udalostí so zvolenou úrovňou závažnosti. Ak chcete aktivovať posielanie e-mailových oznámení otvorte Rozšírené nastavenia > **Oznámenia** > **Preposielanie** a zapnite možnosť **Preposielať oznámenia na e-mail**.



V roletovom menu **Posielať udalosti od úrovne** je možné nastaviť minimálnu úroveň závažnosti oznámení, ktoré majú byť prostredníctvom e-mailu odosielané.

- **Diagnostické** – zaznamenávané budú informácie dôležité pre ladenie programu, ako aj všetky udalosti s

vyššou závažnosťou.

• **Informatívne** – zaznamenávané budú informatívne správy, napríklad o neobvyklých sieťových aktivitách alebo o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.

• **Varovania** – zaznamenávané budú varovné správy a kritické chyby (napr. ak zlyhala aktualizácia).

• **Chyby** – zaznamenávané budú chyby (napr. ochrana dokumentov nie je spustená) a kritické chyby.

• **Kritické** – zaznamenávané budú len kritické chyby (napr. chyba pri spustení antivírusovej ochrany alebo našla sa hrozba).

Posielať každé oznámenie v samostatnom e□maile – každé oznámenie bude odoslané v samostatnom e-maile. Výsledkom môže byť veľký počet prijatých e□mailov v priebehu krátkeho času.

Interval, po ktorom sa budú e-mailom posielať nové oznámenia (v min.) – časový interval v minútach, po ktorom budú nové oznámenia posielané na e□mail. Ak zadáte hodnotu 0, oznámenia sa budú odosielať ihneď po ich vytvorení.

E-mailová adresa odosielateľa – toto pole špecifikuje adresu odosielateľa, ktorá bude zobrazená v hlavičke e□mailovej správy s oznámením.

E-mailové adresy príjemcov – toto pole špecifikuje adresy príjemcov, ktoré budú zobrazené v hlavičke e□mailovej správy s oznámením. Je možné zadať viacero e□mailových adries. Jednotlivé adresy treba oddeliť bodkočiarkou.

SMTP server

SMTP server – SMTP server, pomocou ktorého budú odosielané oznámenia (napr. smtp.provider.com:587, pričom preddefinované číslo portu je 25).

SMTP servery, ktoré využívajú šifrovanie TLS, sú produktom ESET Internet Security podporované.

Prihlasovacie meno a **heslo** – v prípade, že SMTP server vyžaduje overenie, do týchto polí je potrebné zadať platné prihlasovacie meno a heslo pre prístup k SMTP serveru.

Zapnúť TLS – zabezpečiť upozornenia a oznámenia pomocou TLS šifrovania.

Otestovať SMTP spojenie – testovací e□mail sa odošle na e mailovú adresu príjemcu. Je potrebné vyplniť server SMTP, prihlasovacie meno, heslo, adresu odosielateľa a adresy príjemcov.

Formát správy

Komunikácia medzi programom, vzdialeným používateľom alebo správcom systému je zabezpečená prostredníctvom e□mailov alebo LAN správ (pomocou služby Windows Messenger service). Možnosť **Použiť predvolený formát správy** je optimálna vo väčšine situácií. V niektorých prípadoch však môže byť potrebné zmeniť formát správ týkajúcich sa udalostí.

Formát správ o udalostiach – formát správ o udalostiach zobrazovaných na vzdialených počítačoch.

Formát správ o hrozbách – správy obsahujúce upozornenia o hrozbách majú preddefinovaný formát. Meniť tento formát sa neodporúča. Môžu však nastať situácie, keď budete potrebovať formát správy zmeniť (napríklad v

prípade, že používate systém na automatické spracovanie e□mailov).

Znaková sada – konvertuje e□mailovú správu do ANSI kódovania, ktoré je nastavené v regionálnych nastaveniach systému Windows (napr. windows-1250, Unicode (UTF-8), ACSII 7-bit alebo japončina (ISO-2022-JP)). Výsledkom je, že napríklad znak "á" sa zmení na "a" a neznámy symbol bude označený ako "?".

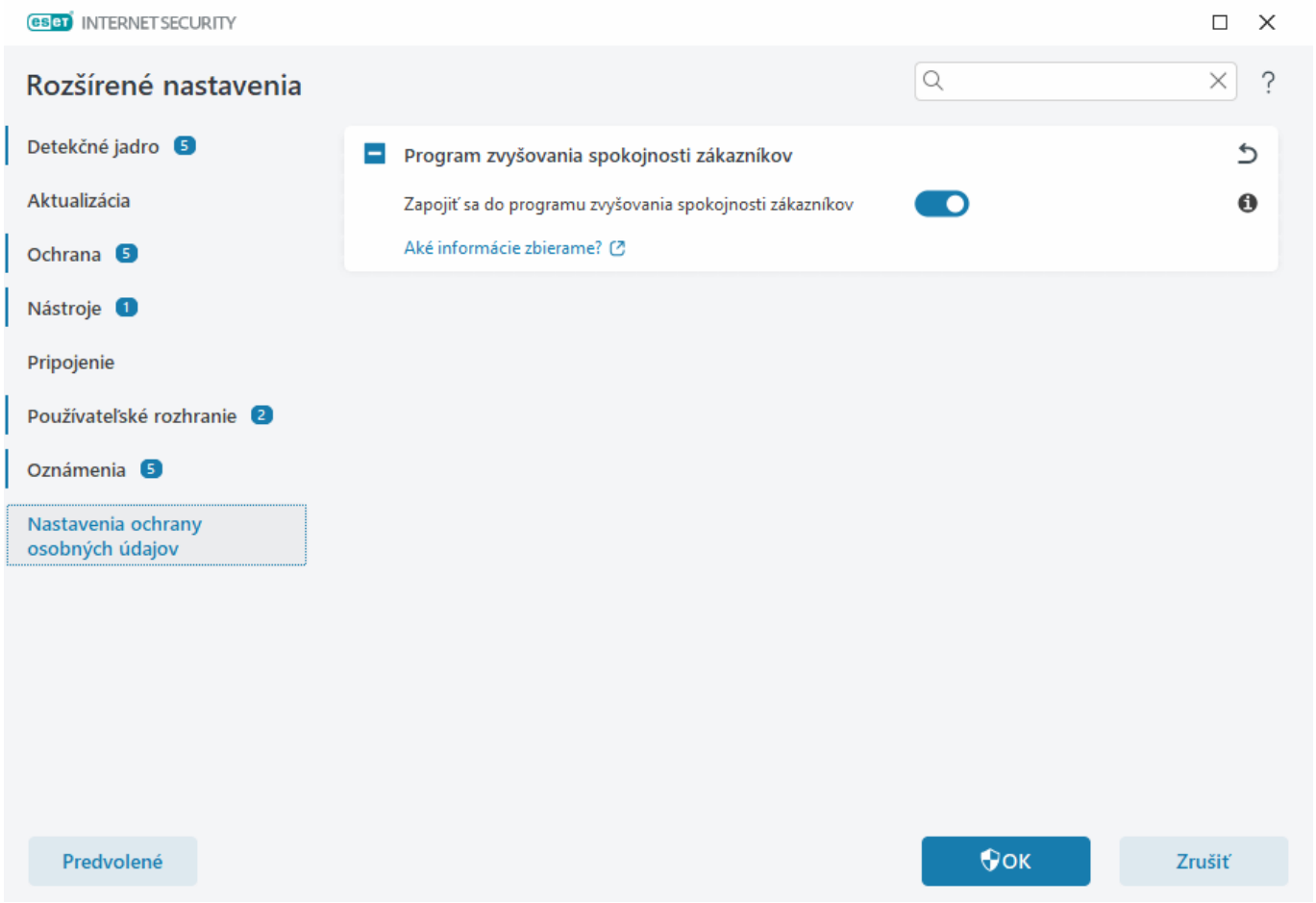
Použiť Quoted-printable kódovanie – e□mailová správa bude zakódovaná do Quoted-printable ((QP)) formátu, ktorý využíva ASCII znaky, čím sa môžu prostredníctvom e□mailu bezchybne prenášať špeciálne (národné) znaky v 8□bitovom formáte (áéíóú).

- **%TimeStamp%** – dátum a čas udalosti.
- **%Scanner%** – modul, ktorý zaznamenal udalosť.
- **%ComputerName%** – názov počítača, na ktorom došlo k udalosti.
- **%ProgramName%** – program, ktorý spôsobil udalosť.
- **%InfectedObject%** – názov škodlivého súboru, e□mailovej správy a pod.
- **%VirusName%** – názov infiltrácie.
- **%Action%** – akcia, ktorá bola vykonaná pre konkrétnu infiltráciu.
- **%ErrorDescription%** – popis chyby, ktorá nesúvisí s vírusom.

Kľúčové slová **%InfectedObject%** a **%VirusName%** sa využívajú iba v upozorneniach týkajúcich sa hrozieb, pričom kľúčové slovo **%ErrorDescription%** sa využíva iba v upozorneniach, ktoré súvisia s určitou udalosťou.

Nastavenia ochrany osobných údajov

Otvorte Rozšírené nastavenia > **Nastavenia súkromia**.



Program zvyšovania spokojnosti zákazníkov

Pomocou prepínacieho tlačidla vedľa možnosti **Zapojiť sa do programu zvyšovania spokojnosti zákazníkov** sa môžete stať súčasťou programu. Poskytnete tak spoločnosti ESET anonymné informácie týkajúce sa používania našich produktov. Zozbierané dáta nám pomôžu produkt zlepšovať a zvyšovať vašu spokojnosť s jeho používaním, pričom nebudú nikdy zdieľané s tretími stranami. Aké informácie zbierame?

Vrátiť späť na predvolené nastavenia

Kliknite na možnosť **Predvolené** v okne Rozšírené nastavenia pre vrátenie všetkých nastavení programu a modulov na predvolené hodnoty. Nastavenia budú obnovené do stavu, ktorý mali po inštalácii.

Prezrite si aj kapitolu Import a export nastavení.

Vrátiť späť predvolené nastavenia v tejto sekcii

Kliknite na ikonu spätnej šípky , ak si želáte všetky nastavenia v aktuálne zobrazenej sekcii vrátiť späť na predvolené hodnoty.

Majte na pamäti, že kliknutím na **Vrátiť späť na predvolené** sa všetky vami vykonané zmeny stratia.

Vrátiť späť obsah tabuliek – po zvolení tejto možnosti sa stratia manuálne aj automaticky pridané pravidlá, úlohy a profily.

Prezrite si aj kapitolu Import a export nastavení.

Chyba pri ukladaní nastavení

Toto chybové hlásenie indikuje, že nastavenia neboli uložené správne a vyskytla sa chyba.

Zvyčajne to znamená, že používateľ, ktorý sa pokúsil zmeniť parametre programu:

- má nedostatočné prístupové práva alebo nemá potrebné oprávnenia pre operačný systém, aby mohol upravovať konfiguračné súbory a systémovú databázu Registry.
  > Pre vykonanie požadovaných zmien sa musí prihlásiť správca systému.

- nedávno povolil Učiaci sa režim v HIPS alebo firewalle a pokúsil sa vykonať zmeny v Rozšírených nastaveniach.
  > Aby sa uložili vaše nastavenia a vyhli ste sa konfliktu konfigurácie, zatvorte okno Rozšírených nastavení bez uloženia a skúste požadované zmeny vykonať znova.

Druhá najčastejšia príčina je, že program nepracuje správne, je poškodený, a preto je ho potrebné preinštalovať.

Modul kontroly cez príkazový riadok

Antivírusový modul programu ESET Internet Security je možné spustiť cez príkazový riadok – manuálne (príkazom „ecls“) alebo pomocou súboru typu „bat“.

Spustenie kontroly ESET cez príkazový riadok:

```
ecls [MOŽNOSTI..] SÚBORY..
```

Pri spúšťaní manuálnej kontroly cez príkazový riadok môžete použiť nasledujúce parametre a prepínače:

Možnosti

/base-dir=PRIEČINOK	načítať moduly z PRIEČINKA
/quar-dir=PRIEČINOK	umiestniť PRIEČINOK do karantény
/exclude=MASKA	vylúčiť z kontroly súbory zodpovedajúce MASKE
/subdir	kontrolovať podpriečinky (predvolené)
/no-subdir	nekontrolovať podpriečinky
/max-subdir-level=ÚROVEŇ	podpriečinky kontrolovať len do určitej úrovne
/symlink	sledovať symbolické prepojenia (predvolené)
/no-symlink	preskočiť symbolické prepojenia
/ads	kontrolovať ADS (predvolené)
/no-ads	nekontrolovať ADS
/log-file=SÚBOR	zapísať výstup do SÚBORU
/log-rewrite	prepísať výstupný súbor (predvolene sa dopíše)
/log-console	zapísať výstup do konzoly (predvolené)
/no-log-console	nezapisovať výstup do konzoly

/log-all	zapisovať do protokolu aj neinfikované súbory
/no-log-all	nezapisovať do protokolu neinfikované súbory (predvolené)
/aind	zobraziť indikátor aktivity
/auto	skontrolovať a automaticky vyliečiť všetky lokálne disky

Možnosti kontroly

/files	kontrolovať súbory (predvolené)
/no-files	nekontrolovať súbory
/memory	kontrolovať pamäť
/boots	kontrolovať zavádzacie sektory
/no-boots	nekontrolovať zavádzacie sektory (predvolené)
/arch	kontrolovať archívy (predvolené)
/no-arch	nekontrolovať archívy
/max-obj-size=VEĽKOSŤ	kontrolovať len súbory menšie ako VEĽKOSŤ megabajtov (predvolene 0 = neobmedzené)
/max-arch-level=ÚROVEŇ	podradené archívy kontrolovať len do danej úrovne hĺbky
/scan-timeout=LIMIT	archívy kontrolovať najviac po daný LIMIT sekúnd
/max-arch-size=VEĽKOSŤ	kontrolovať len súbory v archíve menšie ako daná VEĽKOSŤ (predvolene 0 = neobmedzené)
/max-sfx-size=VEĽKOSŤ	kontrolovať len súbory v samorozbaľovacích archívoch menšie ako VEĽKOSŤ megabajtov (predvolene 0 = neobmedzené)
/mail	kontrolovať e-mailové súbory (predvolené)
/no-mail	nekontrolovať e-mailové súbory
/mailbox	kontrolovať e-mailové schránky (predvolené)
/no-mailbox	nekontrolovať e-mailové schránky
/sfx	kontrolovať samorozbaľovacie archívy (predvolené)
/no-sfx	nekontrolovať samorozbaľovacie archívy
/rtp	kontrolovať runtime archívy (predvolené)
/no-rtp	nekontrolovať runtime archívy
/unsafe	kontrolovať potenciálne nebezpečné aplikácie
/no-unsafe	nekontrolovať potenciálne nebezpečné aplikácie (predvolené)
/unwanted	kontrolovať potenciálne nechcené aplikácie
/no-unwanted	nekontrolovať potenciálne nechcené aplikácie (predvolené)
/suspicious	kontrolovať podozrivé aplikácie (predvolené)
/no-suspicious	nekontrolovať podozrivé aplikácie
/pattern	používať signatúry (predvolené)
/no-pattern	nepoužívať signatúry
/heur	zapnúť heuristiku (predvolené)
/no-heur	vypnúť heuristiku
/adv-heur	zapnúť pokročilú heuristiku (predvolené)

/no-adv-heur	vypnúť pokročilú heuristiku
/ext-exclude=PRÍPONY	vylúčiť z kontroly dvojbodkou oddelené PRÍPONY súborov
/clean-mode=REŽIM	použiť REŽIM liečenia infikovaných objektov K dispozícii sú nasledujúce možnosti: • `none` (predvolené) – infikované súbory nebudú automaticky liečené. • `standard` – ecls.exe sa pokúsi infikované súbory automaticky vyliečiť alebo zmazať. • `strict` – ecls.exe sa pokúsi automaticky vyliečiť alebo zmazať infikované súbory bez zásahu používateľa (pred vymazaním súborov sa používateľovi nezobrazí výzva na potvrdenie akcie). • `rigorous` – ecls.exe vymaže infikované súbory bez predchádzajúceho pokusu o liečenie, a to bez ohľadu na druh súboru. • `delete` – ecls.exe odstráni infikované súbory bez toho, aby sa najskôr pokúsil ich vyliečiť, nevymaže však citlivé súbory ako napríklad systémové súbory Windows.
/quarantine	uložiť infikované súbory (pri liečení) do karantény (doplnková akcia pri liečení súborov)
/no-quarantine	neukladať kópie infikovaných súborov do karantény

Všeobecné možnosti

/help	zobraziť pomocníka a ukončiť
/version	zobraziť informáciu o verzii a ukončiť
/preserve-time	zachovať čas posledného prístupu

Výstupné kódy

0	nenašla sa žiadna hrozba
1	našla sa hrozba, ale bola odstránená
10	niektoré súbory nemohli byť skontrolované (a môže ísť o hrozbu)
50	našla sa hrozba
100	chyba

Výstupné kódy väčšie ako 100 znamenajú, že súbor nebol skontrolovaný, a teda môže byť infikovaný.

Najčastejšie otázky

Táto kapitola obsahuje odpovede na najčastejšie kladené otázky a problémy, s ktorými sa môžete stretnúť. Kliknite na názov kapitoly pre riešenie vášho problému:

- Ako aktualizovať ESET Internet Security
- Program ESET Internet Security objavil hrozbu
- Ako odstrániť vírus z počítača
- Ako povoliť komunikáciu pre určitú aplikáciu

- Ako povoliť Rodičovskú kontrolu pre konkrétny účet
- Ako vytvoriť novú úlohu v Plánovači
- Ako naplánovať týždennú kontrolu
- Ako obnoviť prístup k rozšíreným nastaveniam
- Ako cez ESET HOME vyriešiť problém deaktivovaného produktu

Ak nie je váš problém zahrnutý v zozname vyššie, skúste hľadať priamo v Online pomocníkovi programu ESET Internet Security.

Ak nenájdete riešenie svojho problému na stránkach Online pomocníka pre ESET Internet Security, skúste navštíviť pravidelne aktualizovanú Databázu znalostí spoločnosti ESET. Odkazy na najnavštevovanejšie články znalostnej databázy:

- Ako obnovím svoje predplatné?
- Dostávam chybu aktivácie pri inštalácii môjho bezpečnostného produktu ESET. Čo to znamená?
- Aktivácia produktu ESET pre Windows určeného pre domácnosti pomocou aktivačného kľúča
- Ako odinštalujem a znovu nainštalujem produkt ESET určený pre domácnosti?
- Zobrazilo sa mi chybové hlásenie o predčasne ukončenej inštalácii produktu ESET
- Čo mám spraviť po obnovení svojho predplatného ESET? (produkt pre domácnosti)
- Čo ak sa zmení moja e-mailová adresa?
- Ako prenesiem produkt ESET na nový počítač alebo zariadenie?
- Ako spustím Windows v núdzovom režime (Safe Mode)?
- Ako vylúčiť bezpečnú webovú stránku z blokovania?
- Povoliť programu na čítanie textu z obrazovky prístup ku grafickému rozhraniu ESET

Ak vám pomocník programu ani znalostná databáza nepomohli, môžete kontaktovať technickú podporu spoločnosti ESET.

Ako aktualizovať ESET Internet Security

Aktualizácia produktu ESET Internet Security môže byť vykonaná manuálne alebo automaticky. Na spustenie aktualizácie prejdite do sekcie **Aktualizácia** v hlavnom okne programu a následne kliknite na **Overiť dostupnosť aktualizácií**.

Na základe predvolených nastavení inštalácie je vytvorená úloha v plánovači, ktorá spúšťa automatickú aktualizáciu každú hodinu. Ak chcete zmeniť tento interval, môžete tak urobiť v sekcii **Nástroje** > Plánovač.

Ako odstrániť vírus z počítača

Ak má váš počítač príznaky infekcie malvérom, tzn. je pomalší, často zamŕza a podobne, odporúčame nasledovné kroky:

1. V hlavnom okne programu kliknite na **Kontrola počítača**.

2. Kliknutím na možnosť **Skontrolovať váš počítač** spustite kontrolu systému.

3. Po ukončení kontroly si pozrite protokol so zoznamom skontrolovaných, infikovaných a vyliečených súborov.

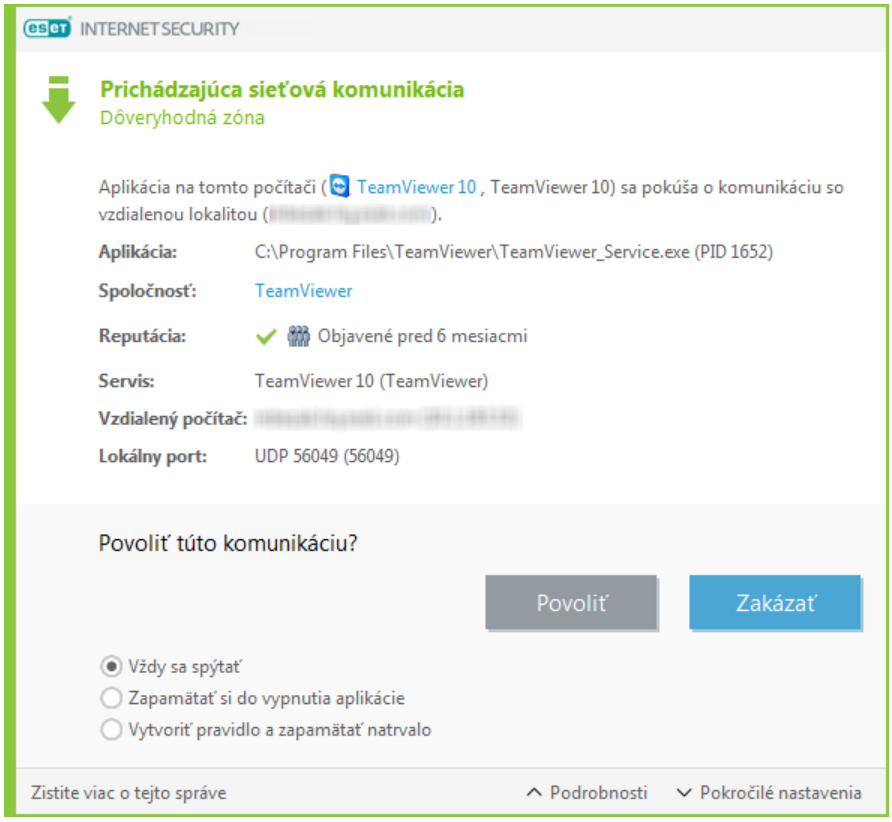
4. Ak chcete skontrolovať len určité časti svojho počítača, kliknite na možnosť **Vlastná kontrola** a vyberte ciele kontroly.

Ďalšie informácie:

- Článok databázy znalostí spoločnosti ESET
- Karanténa

Ako povoliť komunikáciu pre určitú aplikáciu

Ak pri zapnutom interaktívnom režime firewall zachytí nové sieťové spojenie, na ktoré sa neuplatňuje žiadne pravidlo, zobrazí sa výzva **povoliť** alebo **zakázať** toto spojenie. Ak chcete, aby produkt ESET Internet Security vykonal zvolenú akciu zakaždým, keď sa daná aplikácia pokúsi nadviazať spojenie, označte možnosť **Vytvoriť pravidlo a zapamätať natrvalo**.



V nastaveniach firewallu môžete nové pravidlá pre aplikácie vytvoriť aj pred tým, ako ESET Internet Security

deteguje ich sieťovú komunikáciu. V hlavnom okne programu prejdite do sekcie **Nastavenia** > **Ochrana siete**. Kliknite na ⚙ vedľa položky **Firewall** > **Konfigurovať** > **Pokročilé** > **Pravidlá** > **Upraviť**.

Kliknite na **Pridať** a na karte **Všeobecné** zadajte názov, smer a komunikačný protokol nového pravidla. V tomto okne môžete tiež zvoliť akciu, ktorá sa má vykonať v prípade uplatnenia pravidla.

Na karte **Lokálna strana** zadajte cestu k aplikácii (*.exe) a lokálny komunikačný port. Kliknite na kartu **Vzdialená strana** a zadajte vzdialenú adresu a port (ak je to potrebné). Novovytvorené pravidlo bude aplikované hneď, ako sa aplikácia pokúsi nadviazať sieťovú komunikáciu.

Ako povoliť Rodičovskú kontrolu pre konkrétny účet

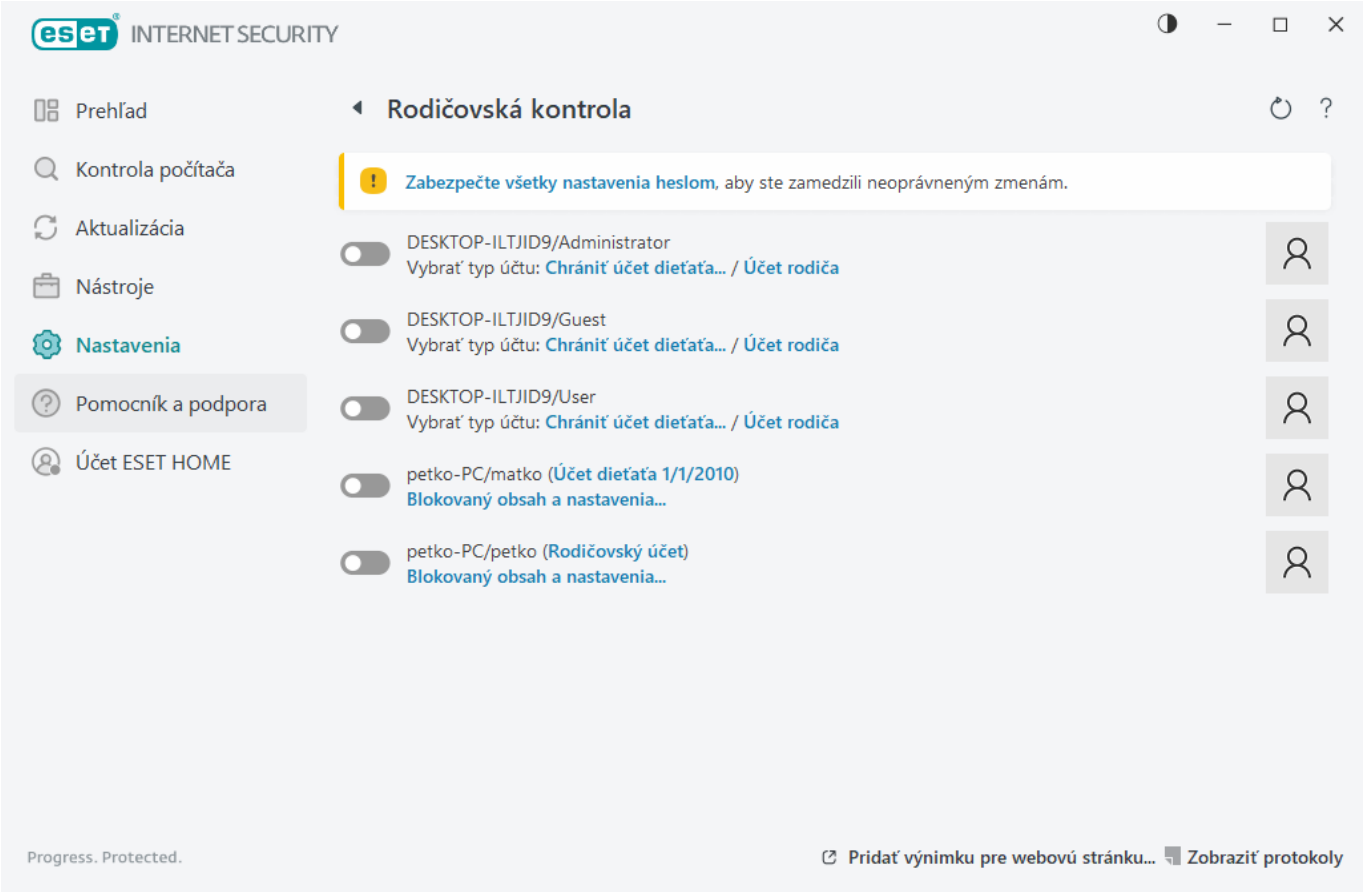
Pre aktiváciu Rodičovskej kontroly pre konkrétny používateľský účet postupujte podľa nasledujúcich inštrukcií:

1. V predvolenom nastavení je Rodičovská kontrola v produkte ESET Internet Security vypnutá. Rodičovskú kontrolu môžete aktivovať dvoma spôsobmi:

   - V hlavnom okne programu v sekcii **Nastavenia** > **Ochrana internetu** > **Rodičovská kontrola** kliknite na prepínacie tlačidlo a zmeňte stav modulu rodičovskej kontroly na zapnutý.

   - Prejdite do sekcie Rozšírené nastavenia > **Ochrana** > **Ochrana prístupu na web** > **Rodičovská kontrola** a kliknite na prepínacie tlačidlo vedľa možnosti **Zapnúť rodičovskú kontrolu**.

2. V hlavnom okne programu kliknite na **Nastavenia** > **Ochrana internetu** > **Rodičovská kontrola**. Napriek tomu, že je **Rodičovská kontrola Zapnutá**, musíte ešte nastaviť požadovaný používateľský účet. Kliknite na šípku a v nasledujúcom okne vyberte **Chrániť účet dieťaťa** alebo **Účet rodiča**. V zobrazenom okne zadajte dátum narodenia na určenie úrovne prístupu a webových stránok vhodných pre príslušný vek. Rodičovská kontrola bude teraz pre daný používateľský účet plne funkčná. Kliknite na **Blokovaný obsah a nastavenia** pod konkrétnym používateľským účtom, ak si želáte zmeniť kategórie webových stránok, ktoré budú povolené alebo blokované, na karte Kategórie. Pre povolenie či blokovanie vlastných webových stránok (ktoré nepatria ani do jednej predvolenej kategórie) kliknite na kartu Výnimky.



Ako vytvoriť novú úlohu v Plánovači

Novú úlohu možno vytvoriť v časti **Nástroje** > **Plánovač** kliknutím na tlačidlo **Pridať plánovanú úlohu** alebo vyvolaním kontextového menu pravým tlačidlom myši a zvolením možnosti **Pridať**. Na výber je päť typov plánovaných úloh:

- **Spustenie externej aplikácie** – výber aplikácie, ktorá má byť spustená plánovačom.
- **Údržba protokolov** – v protokoloch môžu zostávať stopy po vymazaných záznamoch. Táto úloha pravidelne optimalizuje záznamy v protokoloch, čím sa zefektívni a zrýchli práca s nimi.
- **Kontrola súborov spúšťaných pri štarte počítača** – kontroluje súbory, ktoré sa spúšťajú pri štarte alebo prihlásení do systému.
- **Vytvorenie záznamu o stave počítača** – vytvára záznam o stave počítača cez nástroj ESET SysInspector, ktorý slúži na zhromažďovanie podrobných informácií o systémových súčastiach (napr. ovládače, aplikácie) a posudzuje úroveň rizika každej súčasti.
- **Manuálna kontrola počítača** – vykoná kontrolu diskov, jednotlivých priečinkov a súborov na počítači.
- **Aktualizácia** – zabezpečuje aktualizáciu programových modulov.

Keďže medzi najčastejšie používané plánované úlohy patrí **Aktualizácia**, podrobnejšie popíšeme pridanie aktualizačnej úlohy.

Z roletového menu **Plánovaná úloha** vyberte možnosť **Aktualizácia**. Zadajte názov úlohy do poľa **Názov úlohy** a kliknite na **Ďalej**. Vyberte interval vykonania úlohy. K dispozícii sú nasledujúce možnosti: **Raz**, **Opakovane**,

Denne, **Týždenne** a **Pri udalosti**. Možnosť **Nespúšťať úlohu, ak je počítač napájaný z batérie** je dobré použiť, ak prenosný počítač nie je zapojený do elektrickej siete a chcete v tomto čase minimalizovať jeho systémové prostriedky. Zadajte čas/dátum alebo interval, v ktorom bude úloha vykonaná, do poľa **Vykonanie úlohy**. Ďalej je potrebné zadefinovať akciu, ktorá sa vykoná v prípade, že v stanovenom termíne nebude možné úlohu spustiť. Na výber sú nasledujúce možnosti, kedy môže byť úloha opätovne spustená:

- **V najbližšom naplánovanom čase**
- **Hneď ako to bude možné**
- **Okamžite, ak od posledného naplánovaného spustenia uplynul stanovený časový interval v hodinách** (pričom interval je možné definovať priamo pri potvrdení tejto voľby v poli **Čas od posledného spustenia**)

V ďalšom kroku nastavte profil, ktorý sa použije pri aktualizácii. Keď skončíte s úpravami, kliknite na **Dokončiť**.

Zobrazí sa okno umožňujúce vybrať profily, ktoré budú použité pri plánovanej úlohe. Je možné zadefinovať primárny a alternatívny profil. Alternatívny profil sa použije v prípade, že úlohu nebude možné vykonať použitím primárneho profilu. Na uloženie plánovanej úlohy kliknite na **Dokončiť**. Úloha bude následne pridaná do zoznamu úloh Plánovača.

Ako naplánovať pravidelnú týždňovú kontrolu počítača

Ak chcete naplánovať pravidelnú úlohu, otvorte hlavné okno programu a kliknite na **Nástroje** > **Plánovač**. Nižšie je popísaný stručný návod, ako vytvoriť úlohu, ktorá bude pravidelne každý týždeň kontrolovať lokálne disky. Podrobné inštrukcie nájdete v našom článku Databázy znalostí.

Na naplánovanie úlohy postupujte nasledovne:

1. Kliknite na **Pridanie plánovanej úlohy** v hlavnom okne Plánovača.
2. Zadajte názov úlohy a z roletového menu **Typ úlohy** vyberte možnosť **Manuálna kontrola počítača**.
3. Ako frekvenciu opakovania úlohy vyberte možnosť **Týždenne**.
4. Vyberte čas a deň v týždni vykonania úlohy.
5. Označte možnosť **Vykonať úlohu hneď, ako to bude možné**, ktorá zabezpečí, že ak sa úloha nespustí v naplánovanom čase (napríklad ak je počítač vypnutý), spustí sa hneď, ako to bude opäť možné.
6. Skontrolujte prehľad nastavení naplánovanej úlohy a kliknite na **Dokončiť**.
7. V roletovom menu **Ciele kontroly** si zvoľte **Lokálne disky**.
8. Kliknite na **Dokončiť** pre pridanie úlohy.

Ako obnoviť prístup k rozšíreným nastaveniam

chráneným heslom

Ak máte aktivovanú ochranu rozšírených nastavení programu a pokúsite sa o prístup k týmto nastaveniam, zobrazí sa vám okno s výzvou na zadanie príslušného hesla. Ak ste toto heslo zabudli alebo stratili, kliknite na možnosť **Obnoviť heslo** a následne zadajte e‑mailovú adresu, ktorú ste uviedli pri registrácii predplatného. Spoločnosť ESET vám na túto adresu zašle e‑mail s overovacím kódom. Tento kód zadajte do príslušného poľa v zobrazenom okne a nastavte si nové heslo. Overovací kód je platný sedem dní.

Obnoviť heslo prostredníctvom účtu ESET HOME – túto možnosť využite v prípade, že predplatné použité na aktiváciu produktu máte priradené k účtu ESET HOME. Zadajte e‑mailovú adresu, s ktorou sa prihlasujete do účtu ESET HOME.

Ak si neviete spomenúť na e‑mailovú adresu alebo máte problém s obnovením hesla, kliknite na **Kontaktovať technickú podporu**. Následne vás presmerujeme na webovú stránku spoločnosti ESET, z ktorej môžete kontaktovať oddelenie technickej podpory.

Vygenerovať kód pre technickú podporu – pomocou tejto možnosti vygenerujete kód pre špecialistov technickej podpory. Bude vám doručený overovací kód, ktorý skopírujte a následne kliknite na možnosť **Mám overovací kód**. Zadajte overovací kód a nastavte si nové heslo. Overovací kód je platný sedem dní.

Viac sa dozviete v článku Ako obnoviť heslo pre prístup k programovým nastaveniam v produktoch ESET pre domácnosti.

Ako cez ESET HOME vyriešiť problém deaktivovaného produktu

Produkt nie je aktivovaný

Toto chybové hlásenie sa zobrazí, keď vlastník predplatného deaktivuje váš produkt ESET Internet Security z portálu ESET HOME alebo s vami prestane zdieľať predplatné, ktoré používate v účte ESET HOME. Tento problém vyriešite nasledovne:

- Kliknite na možnosť **Aktivovať** a ESET Internet Security aktivujte niektorým z dostupných spôsobov aktivácie.
- Vlastníka predplatného kontaktujte s informáciou, že váš produkt ESET Internet Security bol deaktivovaný, prípadne že už viac nemáte k dispozícii zdieľané predplatné. Vlastník licencie môže tento problém vyriešiť cez ESET HOME.

Produkt je deaktivovaný a zariadenie odpojené

Toto chybové hlásenie sa zobrazí po odstránení zariadenia z účtu ESET HOME. Tento problém vyriešite nasledovne:

- Kliknite na možnosť **Aktivovať** a ESET Internet Security aktivujte niektorým z dostupných spôsobov aktivácie.
- Informujte vlastníka predplatného o tom, že váš produkt ESET Internet Security bol deaktivovaný

a zariadenie bolo odpojené od účtu ESET HOME.

• Ak ste vlastníkom predplatného vy a tieto zmeny ste nevykonali, v účte ESET HOME si skontrolujte sekciu Informácie o aktivite. Ak nájdete podozrivú aktivitu, zmeňte si heslo k účtu ESET HOME a kontaktujte technickú podporu spoločnosti ESET.

Produkt je deaktivovaný a zariadenie odpojené

Toto chybové hlásenie sa zobrazí po odstránení zariadenia z účtu ESET HOME. Tento problém vyriešite nasledovne:

• Kliknite na možnosť **Aktivovať** a ESET Internet Security aktivujte niektorým z dostupných spôsobov aktivácie.

• Informujte vlastníka predplatného o tom, že váš produkt ESET Internet Security bol deaktivovaný a zariadenie bolo odpojené od účtu ESET HOME.

• Ak ste vlastníkom predplatného vy a tieto zmeny ste nevykonali, v účte ESET HOME si skontrolujte sekciu Informácie o aktivite. Ak nájdete podozrivú aktivitu, zmeňte si heslo k účtu ESET HOME a kontaktujte technickú podporu spoločnosti ESET.

Produkt nie je aktivovaný

Toto chybové hlásenie sa zobrazí, keď vlastník predplatného deaktivuje váš produkt ESET Internet Security z portálu ESET HOME alebo s vami prestane zdieľať predplatné, ktoré používate v účte ESET HOME. Tento problém vyriešite nasledovne:

• Kliknite na možnosť **Aktivovať** a ESET Internet Security aktivujte niektorým z dostupných spôsobov aktivácie.

• Vlastníka predplatného kontaktujte s informáciou, že váš produkt ESET Internet Security bol deaktivovaný, prípadne že už viac nemáte k dispozícii zdieľané predplatné. Vlastník licencie môže tento problém vyriešiť cez ESET HOME.

0

Program zvyšovania spokojnosti zákazníkov

Zapojením sa do Programu zvyšovania spokojnosti zákazníkov poskytnete spoločnosti ESET anonymné informácie týkajúce sa používania našich produktov. Podrobnejšie informácie o spracovaní údajov nájdete v Zásadách ochrany osobných údajov.

Váš súhlas

Zapojenie sa do tohto programu je dobrovoľné a je založené na vašom súhlase. Ak sa rozhodnete zapojiť sa do programu, vaša účasť bude pasívna, čo znamená, že nebudete musieť robiť žiadne ďalšie kroky. Svoj súhlas môžete kedykoľvek zrušiť zmenou nastavení produktu. Po zrušení vášho súhlasu nebudeme môcť ďalej spracovávať vaše anonymné údaje.

Svoj súhlas môžete kedykoľvek zrušiť zmenou nastavení produktu:

- Ako zmením nastavenie programu zvyšovania spokojnosti zákazníkov v ESET Windows produkte pre domácnosti?

Aké typy informácií zbierame?

Údaje o používaní produktu

Tieto informácie nám umožňujú získať podrobnejší prehľad o tom, ako naši zákazníci používajú naše produkty. Vďaka tomu dokážeme napríklad zistiť, ktoré funkcie sú používané najčastejšie, ktoré nastavenia používatelia upravujú alebo koľko času používatelia strávia používaním konkrétneho produktu.

Údaje o zariadeniach

Tieto informácie zozbieravame s cieľom lepšie porozumieť, kde a na akých zariadeniach sa naše produkty používajú. Medzi typické príklady patrí model zariadenia, krajina, verzia a názov operačného systému.

Diagnostické údaje pre riešenie problémov

Ide o informácie týkajúce sa problémov a chýb, ku ktorým došlo počas používania našich produktov. Môžeme napríklad zistiť, aký problém sa presne vyskytol a aké kroky k nemu viedli.

Prečo tieto informácie zbierame?

Vďaka týmto anonymným informáciám pre vás môžeme naše produkty neustále zlepšovať. Pomáha nám to zabezpečovať, aby boli naše produkty čo najviac relevantné, ľahko použiteľné a bezchybné.

Kto spravuje tieto informácie?

Spoločnosť ESET, spol. s r. o. je jediným správcom údajov zhromaždených v rámci tohto programu. Žiadne z týchto informácií nebudú poskytnuté tretím stranám.

Licenčná dohoda s koncovým používateľom

S účinnosťou od 19. októbra 2021.

DÔLEŽITÉ: Pred stiahnutím, inštaláciou, kopírovaním alebo použitím si pozorne prečítajte nižšie uvedené podmienky používania produktu. **INŠTALÁCIOU, STIAHNUTÍM, KOPÍROVANÍM ALEBO POUŽITÍM SOFTVÉRU VYJADRUJETE SVOJ SÚHLAS S TÝMITO PODMIENKAMI A BERIETE NA VEDOMIE ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV.**

Licenčná dohoda s koncovým používateľom

Podľa podmienok tejto Dohody s koncovým používateľom (Dohoda“) uzatvorenej medzi spoločnosťou ESET, spol. s r. o., so sídlom Einsteinova 24, 85101 Bratislava, Slovak Republic, zapísanej v Obchodnom registri okresného súdu Bratislava I, oddiel Sro, vložka č. 3586/B, IČO: 31333532 („ESET“ alebo „Poskytovateľ“) a vami, fyzickou alebo právnickou osobou („Vy“ alebo „Koncový používateľ“) máte právo na používanie Softvéru uvedeného v článku 1 tejto Dohody. Softvér uvedený v článku 1 tejto Dohody môže byť v súlade so zmluvnými podmienkami uvedenými nižšie uložený na dátovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov

Poskytovateľa alebo získaný z iných zdrojov.

TOTO NIE JE KÚPNA ZMLUVA ALE DOHODA O PRÁVACH KONCOVÉHO POUŽÍVATEĽA. Poskytovateľ zostáva vlastníkom kópie Softvéru a prípadného fyzického média, na ktorom sa Softvér dodáva v obchodnom balení, ako aj všetkých kópií Softvéru, na ktoré má Koncový používateľ právo podľa tejto Dohody.

Kliknutím na položku „Súhlasím“ alebo „Súhlasím…“ pri inštalácii, sťahovaní, kopírovaní alebo používaní Softvéru vyjadrujete svoj súhlas s podmienkami a požiadavkami tejto Dohody a prijímate Zásady ochrany osobných údajov. Ak s niektorými podmienkami a požiadavkami tejto Dohody a/alebo Zásad ochrany osobných údajov nesúhlasíte, bezodkladne kliknite na možnosť zrušenia, zrušte inštaláciu alebo sťahovanie, prípadne zničte alebo vráťte Softvér, inštalačné médium, priloženú dokumentáciu a potvrdenie o platbe späť Poskytovateľovi alebo v obchode, kde ste Softvér získali.

SÚHLASÍTE S TÝM, ŽE VAŠE POUŽÍVANIE SOFTVÉRU JE ZNAKOM TOHO, ŽE STE SI PREČÍTALI TÚTO DOHODU, ROZUMIETE JEJ, A SÚHLASÍTE S TÝM, ŽE STE VIAZANÝ JEJ USTANOVENIAMI.

1. **Softvér**. Pojem „Softvér“ v tejto zmluve označuje (i) počítačový program, ku ktorému je priložená táto Zmluva, vrátane všetkých jeho súčastí, (ii) celý obsah diskov, CD-ROM, DVD médií, e-mailov a ich všetkých prípadných príloh alebo iných médií, ku ktorým je priložená táto Zmluva, vrátane Softvéru dodaného vo forme objektového kódu na dátovom nosiči, elektronickou poštou alebo stiahnutého cez internet, (iii) so Softvérom súvisiace vysvetľujúce písomné materiály a akúkoľvek dokumentáciu, najmä akýkoľvek popis Softvéru, jeho špecifikácie, popis vlastností, popis ovládania, popis operačného prostredia, v ktorom sa Softvér používa, pokyny na použitie alebo inštaláciu Softvéru alebo akýkoľvek popis používania Softvéru („Dokumentácia“), (iv) kópie Softvéru, opravy prípadných chýb Softvéru, dodatky k Softvéru, rozšírenia Softvéru, modifikované verzie Softvéru a aktualizácie súčastí Softvéru, ak sú dodané, na ktoré vám Poskytovateľ udeľuje licenciu v zmysle článku 3. tejto Zmluvy. Softvér sa dodáva výlučne vo forme spustiteľného objektového kódu.

2. **Inštalácia, počítač a licenčný kľúč**. Softvér dodaný na pamäťovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov je nutné inštalovať. Softvér je potrebné inštalovať do správne nakonfigurovaného počítača, ktorý spĺňa minimálne požiadavky uvedené v Dokumentácii. Spôsob inštalácie je popísaný v Dokumentácii. Do počítača, do ktorého inštalujete Softvér, sa nesmú inštalovať žiadne počítačové programy ani hardvér, ktorý by mohol mať na Softvér negatívny vplyv. Počítač znamená hardvér vrátane, okrem iného, osobných počítačov, notebookov, pracovných staníc, vreckových počítačov, smartfónov, ručných elektronických zariadení a ďalších elektronických zariadení, pre ktoré je Softvér určený a v ktorých sa bude inštalovať a/alebo používať. Licenčný kľúč znamená jedinečnú postupnosť symbolov, písmen, číslic alebo špeciálnych znakov poskytnutú Koncovému používateľovi a umožňujúcu legálne používanie Softvéru, jeho konkrétnej verzie alebo predĺženie obdobia licencie v súlade s touto Dohodou.

3. **Licencia**. Za predpokladu, že ste súhlasili s podmienkami tejto zmluvy a dodržiavate všetky jej zmluvné podmienky, poskytovateľ vám udeľuje nasledujúce práva („licencia“):

a) **Inštalácia a používanie**. Máte nevýhradné a neprevoditeľné, časovo obmedzené právo inštalovať Softvér na pevný disk počítača alebo na iné podobné médium slúžiace na trvalé ukladanie dát, inštaláciu a na ukladanie Softvéru do pamäte počítačového systému, na vykonávanie, na ukladanie a na zobrazovanie Softvéru.

b) **Stanovenie počtu licencií.** Právo na použitie Softvéru sa viaže na počet Koncových používateľov. Jedným Koncovým používateľom sa pritom rozumie: (i) inštalácia Softvéru na jednom počítačovom systéme, alebo (ii) ak sa rozsah licencie viaže na počet poštových schránok, potom sa rozumie jedným Koncovým používateľom užívateľ počítača, ktorý si pomocou Mail User Agent („MUA“) preberá elektronickú poštu. Ak MUA preberá elektronickú poštu a následne ju automaticky rozdeľuje viacerým používateľom potom sa počet Koncových používateľov stanovuje podľa skutočného počtu užívateľov, pre ktorých je elektronická pošta rozdeľovaná. V prípade, že poštový server vykonáva funkciu poštovej brány, je počet Koncových používateľov zhodný s počtom užívateľov poštových serverov, pre ktoré poskytuje táto brána služby. Pokiaľ je jednému používateľovi smerovaný ľubovoľný

počet adries elektronickej pošty (napríklad pomocou aliasov) a preberá si ich jeden používateľ, a správy nie sú automaticky na strane klienta rozdeľované pre viac používateľov, je potrebná licencia pre jeden počítač. Jednu licenciu nesmiete súčasne používať na viacerých počítačoch. Koncový používateľ smie zadať licenčný kľúč v Softvéri len v rozsahu, v ktorom má Koncový používateľ právo používať Softvér v súlade s obmedzením vyplývajúcim z počtu Licencií pridelených Poskytovateľom. Licenčný kľúč sa považuje za dôverný – Licenciu nesmiete zdieľať s tretími stranami a ani nesmiete tretím stranám umožniť používať licenčný kľúč, ak to nie je povolené v tejto Dohode alebo Poskytovateľom. Ak dôjde k neoprávnenému použitiu vášho licenčného kľúča, okamžite informujte Poskytovateľa.

c) **Home/Business Edition.** Verzia Softvéru Home Edition je určená výlučne na domáce a rodinné používanie v súkromných alebo nekomerčných prostrediach. Na použitie v komerčnom prostredí, ako aj na použitie Softvéru na mailových serveroch, mail relay serveroch, mailových bránach alebo internetových bránach musíte získať Softvér vo verzii Business Edition.

d) **Trvanie Licencie.** Vaše právo používať Softvér je časovo obmedzené.

e) **OEM Softvér.** Softvér klasifikovaný ako OEM je obmedzený len na počítač, s ktorým bol získaný. Nie je ho možné preniesť na iný počítač.

f) **NFR, TRIAL Softvér.** Softvér označený ako „Nepredajný“, „Not-for-resale“, NFR alebo TRIAL nemôžete previesť za protihodnotu alebo používať na iný účel, ako na predvádzanie, testovanie jeho vlastností alebo vyskúšanie.

g) **Zánik Licencie.** Licencia zaniká automaticky uplynutím obdobia, na ktoré bola udelená. Ak nedodržíte ktorékoľvek ustanovenie tejto Dohody má Poskytovateľ právo odstúpiť od Dohody bez toho, aby bol dotknutý akýkoľvek nárok alebo prostriedok, ktorý má Poskytovateľ pre takýto prípad k dispozícii. V prípade zrušenia licencie musíte softvér a všetky záložné kópie okamžite odstrániť, zničiť alebo na svoje náklady vrátiť spoločnosti ESET alebo na miesto, kde ste softvér získali. Zánikom Licencie je tiež Poskytovateľ oprávnený ukončiť možnosť Koncového používateľa používať funkcie Softvéru, ktoré vyžadujú pripojenie k serverom Poskytovateľa alebo serverom tretích strán.

4. **Funkcie so zhromažďovaním údajov a požiadavky na pripojenie na internet.** Softvér na svoje správne fungovanie vyžaduje pripojenie na internet a musí sa v pravidelných intervaloch pripájať na servery Poskytovateľa alebo servery tretích strán. Takisto vyžaduje zhromažďovanie príslušných údajov v súlade so Zásadami ochrany osobných údajov. Pripojenie na internet a zhromažďovanie údajov je nevyhnutné na tieto funkcie Softvéru:

a) **Aktualizácia Softvéru.** Poskytovateľ môže príležitostne vydávať aktualizácie alebo inovácie Softvéru („Update“), nie je však povinný poskytovať Update. Táto funkcia je pri štandardnom nastavení Softvéru zapnutá, preto sa Update nainštaluje automaticky, okrem prípadov, keď Koncový používateľ automatickú inštaláciu Update zakázal. Pre poskytovanie aktualizácii sa vyžaduje overenie pravosti Licencie vrátane informácií o počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, v súlade so Zásadami ochrany osobných údajov.

Na poskytovanie akýchkoľvek aktualizácií sa môžu vzťahovať Zásady Ukončenia životného cyklu („Zásady Ukončenia životného cyklu“), ktoré sú k dispozícii na adrese https://go.eset.com/eol_home. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebudú sa poskytovať žiadne aktualizácie.

b) **Preposielanie infiltrácií a informácií Poskytovateľovi.** Softvér obsahuje funkcie, ktoré zhromažďujú vzorky počítačových vírusov a iných škodlivých počítačových programov, ako aj podozrivých, problémových, potenciálne nechcených alebo potenciálne nebezpečných objektov, ako sú napríklad súbory, URL adresy, IP pakety a ethernetové rámce („Infiltrácie“), a potom ich odosiela Poskytovateľovi vrátane, nie však výhradne, informácií o procese inštalácie, počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, a/alebo informácií o prevádzke a fungovaní Softvéru („Informácie“.) Informácie a Infiltrácie môžu obsahovať údaje (vrátane náhodne alebo neúmyselne získaných osobných údajov) o Koncovom používateľovi alebo iných používateľoch počítača, v ktorom

je Softvér nainštalovaný, a súboroch postihnutých Infiltráciami spolu so súvisiacimi metaúdajmi.

Informácie a Infiltrácie sa môžu zhromažďovať prostredníctvom nasledujúcich funkcií Softvéru:

i. Súčasťou funkcie LiveGrid Reputation System je zhromažďovanie a odosielanie jednosmerných hodnôt hash súvisiacich s infiltráciami Poskytovateľovi. Táto funkcia sa zapína v štandardných nastaveniach Softvéru.

ii. Súčasťou funkcie LiveGrid Feedback System je zhromažďovanie a odosielanie Infiltrácií spolu so súvisiacimi metaúdajmi a Informáciami Poskytovateľovi. Túto funkciu môže aktivovať Koncový používateľ počas inštalácie Softvéru.

Poskytovateľ použije získané Informácie a Infiltrácie iba na účely analýzy a preskúmania Infiltrácií, vylepšenia Softvéru a overenia pravosti Licencie, pričom vykoná primerané opatrenia na zachovanie zabezpečenia získaných Infiltrácií a Informácií. Aktivovaním tejto funkcie Softvéru môže Poskytovateľ zhromažďovať a spracúvať Infiltrácie a Informácie v súlade so zásadami ochrany osobných údajov a príslušnými právnymi predpismi. Tieto funkcie môžete kedykoľvek deaktivovať.

Na účely tejto Dohody je potrebné zhromažďovať, spracúvať a ukladať údaje umožňujúce Poskytovateľovi identifikovať vás v súlade so Zásadami ochrany osobných údajov. Týmto beriete na vedomie, že Poskytovateľ kontroluje s využitím vlastných prostriedkov, či Softvér používate v súlade s ustanoveniami tejto Dohody. Zároveň týmto beriete na vedomie, že na účely tejto Dohody je počas komunikácie medzi Softvérom a počítačovými systémami Poskytovateľa alebo jeho obchodných partnerov v rámci distribučnej a podpornej siete Poskytovateľa potrebný prenos údajov na zabezpečenie funkčnosti Softvéru a oprávnenia na používanie Softvéru a na ochranu práv Poskytovateľa.

Po uzavretí tejto Dohody je Poskytovateľ alebo ľubovoľný jeho obchodný partner v rámci distribučnej a podpornej siete Poskytovateľa oprávnený na účely fakturácie, plnenia tejto Dohody a prenosu oznámení do vášho počítača v nevyhnutnom rozsahu prenášať, spracovávať a uchovávať dôležité údaje, ktoré vás umožnia identifikovať.

Podrobné informácie o ochrane súkromia, ochrane osobných údajov a vašich právach ako dotknutej osoby sú uvedené v zásadách ochrany osobných údajov dostupných na webových stránkach Poskytovateľa a prístupných priamo počas procesu inštalácie. Prístup k nim môžete získať aj v pomocníkovi softvéru.

5. **Výkon práv Koncového používateľa**. Práva Koncového používateľa musíte vykonávať osobne alebo prostredníctvom svojich prípadných zamestnancov. Softvér môžete použiť výlučne na zabezpečenie svojej činnosti a na ochranu len tých počítačových systémov, pre ktoré ste získali Licenciu.

6. **Obmedzenie práv.** Nesmiete Softvér kopírovať, šíriť, oddeľovať jeho časti alebo vytvárať od Softvéru odvodené diela. Pri používaní Softvéru ste povinný dodržiavať nasledovné obmedzenia:

a) Môžete pre seba vytvoriť jedinú kópiu Softvéru na médiu určenom na trvalé ukladanie dát ako záložnú kópiu, za predpokladu, že vaša archívna záložná kópia sa nebude inštalovať alebo používať na inom počítači. Vytvorenie akejkoľvek ďalšej kópie Softvéru je porušením tejto Dohody.

b) Softvér nesmiete používať, upravovať, prekladať, reprodukovať, alebo prevádzať práva na používanie Softvéru alebo kópií Softvéru inak, než je výslovne uvedené v tejto Dohode.

c) Softvér nesmiete predať, sublicencovať, prenajať alebo prenajať si, vypožičať si ho alebo používať na poskytovanie komerčných služieb.

d) Softvér nesmiete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsiť získať zdrojový kód Softvéru s výnimkou rozsahu, v ktorom je takéto obmedzenie výslovne zakázané zákonom.

e) Súhlasíte s tým, že budete používať Softvér iba spôsobom, ktorý je v súlade so všetkými platnými právnymi predpismi v právnom systéme, v ktorom Softvér používate, najmä v súlade s platnými obmedzeniami vyplývajúcimi z autorského práva a ďalších práv duševného vlastníctva.

f) Súhlasíte s tým, že budete používať Softvér a jeho funkcie výlučne spôsobom, ktorý neobmedzí možnosti iných Koncových používateľov na prístup k týmto službám. Poskytovateľ si vyhradzuje právo obmedziť rozsah služieb poskytovaných jednotlivým Koncovým používateľom tak, aby umožnil ich využívanie čo najväčšiemu počtu Koncových používateľov. Obmedzenie rozsahu služieb môže znamenať aj úplné zrušenie možnosti používať niektorú z funkcií Softvéru a likvidáciu Údajov a informácií na serveroch Poskytovateľa alebo serveroch tretích strán spojených danou funkciou Softvéru.

g) Súhlasíte s tým, že nebudete vykonávať žiadne činnosti zahŕňajúce použitie licenčného kľúča v rozpore s podmienkami tejto Dohody alebo vedúce k poskytnutiu licenčného kľúča akejkoľvek osobe, ktorá nie je oprávnená používať Softvér, ako napríklad prenos použitého alebo nepoužitého licenčného kľúča v akejkoľvek forme, ako aj neoprávnená reprodukcia alebo distribúcia duplikovaných alebo generovaných licenčných kľúčov alebo používanie Softvéru v dôsledku použitia licenčného kľúča získaného od iného zdroja ako od Poskytovateľa.

7. **Autorské práva**. Softvér a všetky práva, najmä vlastnícke práva a práva duševného vlastníctva k nemu, sú vlastníctvom spoločnosti ESET a/alebo jej poskytovateľov licencií. Tieto sú chránené ustanoveniami medzinárodných dohôd a všetkými ďalšími aplikovateľnými zákonmi krajiny, v ktorej sa Softvér používa. Štruktúra, organizácia a kód Softvéru sú obchodnými tajomstvami a dôvernými informáciami spoločnosti ESET a/alebo jej poskytovateľov licencií. Softvér nesmiete kopírovať, s výnimkou uvedenou v ustanovení článku 6 písmeno a). Akékoľvek kópie, ktoré smiete vytvoriť podľa tejto Zmluvy, musia obsahovať rovnaké upozornenia na autorské a vlastnícke práva, aké sú uvedené na Softvéri. V prípade, že v rozpore s ustanoveniami tejto Dohody budete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsite získať zdrojový kód, súhlasíte s tým, že takto získané informácie sa budú automaticky a neodvolateľne považovať za prevedené na Poskytovateľa a vlastnené v plnom rozsahu Poskytovateľom od okamihu ich vzniku, tým nie sú dotknuté práva Poskytovateľa spojené s porušením tejto Dohody.

8. **Výhrada práv**. Všetky práva k Softvéru, okrem práv ktoré Vám ako Koncovému používateľovi Softvéru boli výslovne udelené v tejto Dohode, si Poskytovateľ vyhradzuje pre seba.

9. **Viaceré jazykové verzie, verzie pre viac operačných systémov, viaceré kópie**. V prípade ak Softvér podporuje viaceré platformy alebo jazyky, alebo ak ste získali viac kópii Softvéru, môžete Softvér používať len na takom počte počítačových systémov a v takých verziách, na ktoré ste získali Licenciu. Verzie alebo kópie Softvéru, ktoré nepoužívate nesmiete predať, prenajať, sublicencovať, zapožičať alebo previesť na iné osoby.

10. **Začiatok a trvanie Dohody.** Táto Dohoda je platná a účinná odo dňa, kedy ste odsúhlasili túto Dohodu. Dohodu môžete kedykoľvek ukončiť tak, že natrvalo odinštalujete zničíte alebo na svoje vlastné náklady vrátite Softvér, všetky prípadné záložné kópie a všetok súvisiaci materiál, ktorý ste získali od Poskytovateľa alebo jeho obchodných partnerov. Na vaše právo používať Softvér a ktorúkoľvek z jeho funkcií sa môžu vzťahovať Zásady Ukončenia životného cyklu. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, vaše právo používať Softvér zanikne. Bez ohľadu na spôsob zániku tejto Dohody, ustanovenia jej článkov 7, 8, 11, 13, 19 a 21 zostávajú v platnosti bez časového obmedzenia.

11. **VYHLÁSENIA KONCOVÉHO POUŽÍVATEĽA**. AKO KONCOVÝ POUŽÍVATEĽ UZNÁVATE, ŽE SOFTVÉR JE POSKYTOVANÝ "AKO STOJÍ A LEŽÍ", BEZ VÝSLOVNEJ ALEBO IMPLIKOVANEJ ZÁRUKY AKÉHOKOĽVEK DRUHU A V MAXIMÁLNEJ MIERE DOVOLENEJ APLIKOVATEĽNÝMI ZÁKONMI. ANI POSKYTOVATEĽ, ANI JEHO POSKYTOVATELIA LICENCIÍ, ANI DRŽITELIA AUTORSKÝCH PRÁV NEPOSKYTUJÚ AKÉKOĽVEK VÝSLOVNÉ ALEBO IMPLIKOVANÉ PREHLÁSENIA ALEBO ZÁRUKY, NAJMÄ NIE ZÁRUKY PREDAJNOSTI ALEBO VHODNOSTI PRE KONKRÉTNY ÚČEL ALEBO ZÁRUKY, ŽE SOFTVÉR NEPORUŠUJE ŽIADNE PATENTY, AUTORSKÉ PRÁVA, OCHRANNÉ ZNÁMKY ALEBO INÉ

PRÁVA TRETÍCH STRÁN. NEEXISTUJE ŽIADNA ZÁRUKA ZO STRANY POSKYTOVATEĽA ANI ŽIADNEJ ĎALŠEJ STRANY, ŽE FUNKCIE, KTORÉ OBSAHUJE SOFTVÉR, BUDÚ VYHOVOVAŤ VAŠÍM POŽIADAVKÁM, ALEBO ŽE PREVÁDZKA SOFTVÉRU BUDE NERUŠENÁ A BEZCHYBNÁ. PREBERÁTE ÚPLNÚ ZODPOVEDNOSŤ A RIZIKO ZA VÝBER SOFTVÉRU PRE DOSIAHNUTIE VAMI ZAMÝŠĽANÝCH VÝSLEDKOV A ZA INŠTALÁCIU, POUŽÍVANIE A VÝSLEDKY, KTORÉ SO SOFTVÉROM DOSIAHNETE.

12. **Žiadne ďalšie záväzky.** Táto Dohoda nezakladá na strane Poskytovateľa a jeho prípadných poskytovateľov licencií okrem záväzkov konkrétne uvedených v tejto Dohode žiadne iné záväzky.

13. **OBMEDZENIE ZODPOVEDNOSTI**. V MAXIMÁLNEJ MIERE, AKÚ DOVOĽUJE APLIKOVATEĽNÉ PRÁVO, V ŽIADNOM PRÍPADE NEBUDE POSKYTOVATEĽ, JEHO ZAMESTNANCI ALEBO JEHO POSKYTOVATELIA LICENCIÍ ZODPOVEDAŤ ZA AKÝKOĽVEK UŠLÝ ZISK, PRÍJEM ALEBO PREDAJ, ALEBO ZA AKÚKOĽVEK STRATU DÁT, ALEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARANIE NÁHRADNÝCH TOVAROV ALEBO SLUŽIEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÚ UJMU, ZA PRERUŠENIE PODNIKANIA, ZA STRATU OBCHODNÝCH INFORMÁCIÍ, ANI ZA AKÉKOĽVEK ŠPECIÁLNE, PRIAME, NEPRIAME, NÁHODNÉ, EKONOMICKÉ, KRYCIE, TRESTNÉ, ŠPECIÁLNE ALEBO NÁSLEDNÉ ŠKODY, AKOKOĽVEK ZAPRÍČINENÉ, ČI UŽ VYPLYNULI ZO ZMLUVY, ÚMYSELNÉHO KONANIA, NEDBALOSTI ALEBO INEJ SKUTOČNOSTI, ZAKLADAJÚCEJ VZNIK ZODPOVEDNOSTI, VZNIKNUTÉ INŠTALÁCIOU, POUŽÍVANÍM ALEBO NEMOŽNOSŤOU POUŽÍVAŤ SOFTVÉR, A TO AJ V PRÍPADE, ŽE POSKYTOVATEĽ ALEBO JEHO POSKYTOVATELIA LICENCIÍ BOLI UVEDOMENÍ O MOŽNOSTI TAKÝCHTO ŠKÔD. NAKOĽKO NIEKTORÉ ŠTÁTY A NIEKTORÉ PRÁVNE SYSTÉMY NEDOVOĽUJÚ VYLÚČENIE ZODPOVEDNOSTI, ALE MÔŽU DOVOĽOVAŤ OBMEDZENIE ZODPOVEDNOSTI, JE ZODPOVEDNOSŤ POSKYTOVATEĽA, JEHO ZAMESTNANCOV ALEBO POSKYTOVATEĽOV LICENCIÍ OBMEDZENÁ DO VÝŠKY CENY, KTORÚ STE ZAPLATILI ZA LICENCIU.

14. Žiadne ustanovenie tejto Dohody sa nedotýka práv strany, ktorej zákon priznáva práva a postavenie spotrebiteľa, pokiaľ je s nimi v rozpore.

15. **Technická podpora**. Technickú podporu poskytuje ESET alebo ním poverená tretia strana na základe vlastného uváženia bez akýchkoľvek záruk alebo prehlásení. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebude sa poskytovať žiadna technická podpora. Koncový používateľ je povinný pred poskytnutím technickej podpory zálohovať všetky jeho existujúce dáta, softvér a programové vybavenie. ESET a/alebo ním poverená tretia strana nepreberajú zodpovednosť za poškodenie alebo stratu dát, majetku, softvéru alebo hardvéru alebo ušlý zisk pri poskytovaní technickej podpory. ESET a/alebo ním poverená tretia strana si vyhradzuje právo na rozhodnutie, že riešený problém presahuje rozsah technickej podpory. ESET si vyhradzuje právo odmietnuť, pozastaviť alebo ukončiť poskytovanie technickej podpory na základe vlastného uváženia. Informácie o Licencii, Informácie a ďalšie údaje v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely poskytovania technickej pomoci.

16. **Prevod Licencie**. Softvér môžete preniesť z jedného počítačového systému na iný počítačový systém, pokiaľ to nie je v rozpore s Dohodou. Pokiaľ to nie je v rozpore s Dohodou, Koncový používateľ môže jednorazovo trvalo previesť Licenciu a všetky práva z tejto Dohody na iného Koncového používateľa iba so súhlasom Poskytovateľa za podmienky, že (i) pôvodný Koncový používateľ si neponechá žiadnu kópiu Softvéru, (ii) prevod práv musí byť priamy, teda z pôvodného Koncového používateľa na nového Koncového používateľa, (iii) nový Koncový používateľ musí prebrať všetky práva a povinnosti, ktoré má podľa tejto Dohody pôvodný Koncový používateľa (iv) pôvodný Koncový používateľ musí odovzdať novému Koncovému používateľovi doklady umožňujúce overenie legality Softvéru ako je uvedené v článku 17.

17. **Overenie pravosti Softvéru.** Koncový používateľ musí preukázať právo na používanie Softvéru jedným z týchto spôsobov: (i) prostredníctvom osvedčenia o licencii vydaného Poskytovateľom alebo treťou stranou určenou Poskytovateľom, (ii) prostredníctvom písomnej licenčnej zmluvy, ak takáto zmluva bola uzavretá, (iii) predložením e-mailu odoslaného Poskytovateľom, ktorý obsahuje podrobnosti o licencii (meno používateľa a heslo). Informácie o Licencii a identifikačné údaje Koncového používateľa v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely overenia pravosti Softvéru.

18. **Licencovanie pre štátne orgány a vládu USA**. Softvér sa poskytuje štátnym orgánom vrátane vlády Spojených štátov amerických s licenčnými právami a obmedzeniami popísanými v tejto Dohode.

19. **Súlad s kontrolou obchodu**.

a) Zaväzujete sa, že Softvér nebudete priamo alebo nepriamo vyvážať, opätovne vyvážať ani ho inak nesprístupníte žiadnej osobe, ani ho nepoužijete akýmkoľvek spôsobom, ktorý by spôsobil, že spoločnosť ESET alebo jej holdingové spoločnosti, dcérske spoločnosti alebo dcérske spoločnosti jej holdingových spoločností spolu s osobami ovládanými jej holdingovými spoločnosťami („Pobočky“) porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu, ktoré zahŕňajú:

i. všetky zákony, ktoré kontrolujú, obmedzujú alebo vynucujú licenčné podmienky vývozu, opätovného vývozu alebo prenosu výrobkov, softvéru, technológií alebo služieb vydaných alebo prijatých akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje a

ii. všetky ekonomické, finančné, obchodné alebo iné sankcie, obmedzenia, embargá, zákazy dovozu alebo vývozu, zákazy prevodu prostriedkov alebo aktív alebo poskytovania služieb alebo iné porovnateľné opatrenie prijaté akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje.

(právne predpisy, na ktoré sa odkazuje v bodoch i. a ii. vyššie, ďalej spoločne „Zákony na kontrolu obchodu“).

b) Spoločnosť ESET si vyhradzuje právo s okamžitou platnosťou pozastaviť alebo ukončiť plnenie svojich povinností vyplývajúcich z tejto dohody v prípade, že:

i. Spoločnosť ESET rozhodne podľa svojho najlepšieho vedomia a svedomia, že Používateľ porušil alebo pravdepodobne poruší ustanovenia článku 19 bodu (a) Dohody; alebo

ii. Koncový používateľ a/alebo Softvér sa stanú predmetom zákonov na kontrolu obchodu, následkom čoho spoločnosť ESET podľa svojho najlepšieho vedomia a svedomia rozhodne, že ďalšie plnenie jej povinností vyplývajúcich z Dohody by mohlo mať za následok, že spoločnosť ESET a jej Pobočky porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu.

c) Žiadna časť Dohody nie je zamýšľaná a nesmie byť interpretovaná tak, že podnecuje niektorú zo strán či od nej vyžaduje, aby konala alebo sa zdržala konania spôsobom (či s takýmto konaním či nekonaním súhlasila), ktorý akýmkoľvek spôsobom porušuje platné zákony na kontrolu obchodu alebo sa týmito zákonmi postihuje či zakazuje.

20. **Oznámenia**. Všetky oznámenia, vrátený Softvér a Dokumentáciu je potrebné doručiť na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, bez toho, aby bolo dotknuté právo spoločnosti ESET oznámiť vám akékoľvek zmeny tejto Dohody, Zásad ochrany osobných údajov, Zásad Ukončenia životného cyklu a Dokumentácie v súlade s článkom 22 Dohody. Spoločnosť ESET vám môže posielať e-maily, oznámenia v aplikácii prostredníctvom Softvéru alebo uverejniť komunikáciu na svojej webovej lokalite. Súhlasíte s tým, že budete od spoločnosti ESET dostávať právnu komunikáciu v elektronickej forme vrátane akejkoľvek komunikácie o zmene podmienok, osobitných podmienok alebo zásad ochrany osobných údajov, akýchkoľvek návrhov/prijatí zmluvy alebo pozvánok, upozornení alebo inej právnej komunikácie. Takáto elektronická komunikácia sa bude považovať za prijatú v písomnej forme, pokiaľ príslušné právne predpisy osobitne nevyžadujú inú formu komunikácie.

21. **Rozhodujúce právo**. Táto Dohoda sa riadi a musí byť vykladaná v súlade so zákonmi Slovenskej republiky.

Koncový používateľ a Poskytovateľ sa dohodli, že kolízne ustanovenia rozhodujúceho právneho poriadku a Dohovor OSN o zmluvách pri medzinárodnej kúpe tovarov sa nepoužijú. Výslovne súhlasíte, že riešenie akýkoľvek sporov alebo nárokov z tejto Dohody voči Poskytovateľovi alebo spory a nároky súvisiace s používaním softvéru je príslušný Okresný súd Bratislava I a výslovne súhlasíte s výkonom jurisdikcie týmto súdom.

22. **Všeobecné ustanovenia**. V prípade, že akákoľvek ustanovenie tejto Dohody je neplatné alebo nevykonateľné, neovplyvní to platnosť ostatných ustanovení Dohody. Tie zostanú platné a vykonateľné podľa podmienok v nej stanovených. Táto Dohoda bola vyhotovená v angličtine. V prípade, že je z praktických dôvodov alebo na akýkoľvek iný účel vypracovaný akýkoľvek preklad Dohody, alebo v prípade akýchkoľvek nezrovnalostí medzi jazykovými verziami tejto Dohody platí verzia v angličtine.

Spoločnosť ESET si vyhradzuje právo kedykoľvek vykonať zmeny v Softvéri, ako aj kedykoľvek upraviť podmienky tejto Dohody, jej prílohy, dodatky, Zásady ochrany osobných údajov, Zásady Ukončenia životného cyklu a dokumentáciu, prípadne ich ľubovoľnú časť tak, že aktualizuje príslušný dokument: (i) aby zohľadňoval zmeny v Softvéri alebo v tom, ako spoločnosť ESET vykonáva podnikateľskú činnosť, (ii) z právnych, regulačných alebo bezpečnostných dôvodov alebo (iii) na zabránenie zneužitiu alebo ublíženiu. O každej úprave Dohody vás informujeme prostredníctvom e-mailu, oznámenia v aplikácii alebo iným spôsobom elektronickej komunikácie. Ak s navrhovanými zmenami Dohody nebudete súhlasiť, môžete ju v súlade s článkom 10 ukončiť do 30 dní od prijatia oznámenia o zmene. Ak Dohodu v tejto časovej lehote neukončíte, navrhované zmeny sa budú považovať za prijaté a nadobudnú voči vám účinnosť k dátumu prijatia oznámenia o zmene.

Táto Zmluva medzi Vami a Poskytovateľom predstavuje jedinú a úplnú Zmluvu vzťahujúcu sa na Softvér, a plne nahrádza akékoľvek predchádzajúce vyhlásenia, rokovania, záväzky, správy alebo reklamné informácie, týkajúce sa Softvéru.

DODATOK K DOHODE

Vyhodnotenie bezpečnosti zariadení pripojených k sieti. Na vyhodnotenie bezpečnosti zariadení pripojených k sieti sa vzťahujú ďalšie ustanovenia, ako je uvedené nižšie:

Softvér obsahuje funkciu pre kontrolu bezpečnosti lokálnej siete koncového používateľa a bezpečnosti zariadení pripojených k lokálnej sieti, ktorá si vyžaduje názov lokálnej siete a informácie o zariadeniach pripojených k lokálnej sieti, ako je prítomnosť, typ, názov, IP adresa a MAC adresa zariadenia na lokálnej sieti v spojitosti s licenčnými informáciami. Informácie zahŕňajú typ bezdrôtového zabezpečenia a typ bezdrôtového šifrovania pre sieťové smerovače. Táto funkcia môže taktiež poskytovať informácie ohľadom dostupnosti bezpečnostného softvérového riešenia pre zabezpečenie zariadení na lokálnej sieti.

Ochrana proti zneužitiu údajov. Na ochranu proti zneužitiu údajov sa vzťahujú ďalšie ustanovenia, ako je uvedené nižšie:

Softvér obsahuje funkciu, ktorá zabraňuje strate alebo zneužitiu kritických údajov v priamej súvislosti s krádežou počítača. Táto funkcia je podľa predvolených nastavení softvéru vypnutá. Na aktiváciu funkcie sa vyžaduje vytvorenie účtu ESET HOME, prostredníctvom ktorého funkcia aktivuje zhromažďovanie údajov v prípade krádeže počítača. Ak sa rozhodnete aktivovať túto funkciu Softvéru, údaje o ukradnutom počítači sa budú zhromažďovať a odosielať Poskytovateľovi, pričom tieto údaje môžu obsahovať údaje o sieťovej polohe počítača, údaje o obsahu zobrazenom na obrazovke počítača, údaje o konfigurácii počítača a/alebo údaje nahraté kamerou pripojenou k počítaču (ďalej len „Údaje“). Koncový používateľ má nárok na použitie údajov získaných touto funkciou a poskytnutých prostredníctvom účtu ESET HOME výlučne na vyriešenie nepriaznivej situácie spôsobenej krádežou počítača. Na účely tejto funkcie poskytovateľ spracúva údaje v súlade so zásadami ochrany osobných údajov a príslušnými právnymi predpismi. Poskytovateľ umožní Koncovému používateľovi prístup k Údajom na obdobie potrebné na dosiahnutie účelu, na ktorý boli údaje získané, pričom toto obdobie neprekročí obdobie uchovávania určené v zásadách ochrany osobných údajov. Funkcia ochrany proti zneužitiu údajov sa môže používať výlučne v počítačoch a účtoch, ku ktorým má Koncový používateľ legitímny prístup. Akékoľvek

nezákonné použitie bude nahlásené príslušnému orgánu. Poskytovateľ bude v prípade zneužitia postupovať v súlade s príslušnými zákonmi a bude pomáhať orgánom činným v trestnom konaní. Beriete na vedomie a súhlasíte s tým, že ste zodpovední za ochranu hesla na prístup k účtu ESET HOME, a súhlasíte s tým, že heslo nezverejníte žiadnej tretej strane. Koncový používateľ je zodpovedný za všetky činnosti súvisiace s používaním funkcie ochrany proti zneužitiu údajov a účtu ESET HOME bez ohľadu na to, či sú oprávnené. Ak dôjde k neoprávnenému použitiu Účtu ESET HOME, okamžite informujte Poskytovateľa. Ďalšie ustanovenia o Ochrane proti zneužitiu údajov sa vzťahujú výlučne na Koncových používateľov softvérov ESET Internet Security a ESET Smart Security Premium.

ESET Secure Data. Na funkciu ESET Secure Data sa vzťahujú ďalšie ustanovenia, ako je uvedené nižšie:

1. Definície. V týchto ďalších ustanoveniach o softvéri ESET Secure Data majú nasledujúce slová tieto zodpovedajúce významy:

a) „Informácie“ – akékoľvek informácie alebo údaje šifrované alebo dešifrované pomocou softvéru;

b) „Produkty“ – softvér ESET Secure Data a dokumentácia k nemu;

c) „ESET Secure Data“ – softvér používaný na šifrovanie a dešifrovanie elektronických údajov;

Všetky odkazy na plurál zahŕňajú singulár a všetky odkazy na mužský rod zahŕňajú ženský a stredný rod a naopak. Slová bez osobitnej definície sa používajú v súlade s definíciami uvedenými v Dohode.

2. Dodatočné vyhlásenie Koncového používateľa. Beriete na vedomie a súhlasíte s tým, že:

a) je vašou povinnosťou chrániť, udržiavať a zálohovať Informácie;

b) by ste mali pred inštaláciou softvéru ESET Secure Data plne zálohovať všetky Informácie a údaje (vrátane, nie však výhradne, všetkých dôležitých informácií a údajov) vo svojom počítači;

c) musíte udržiavať bezpečné záznamy všetkých hesiel alebo iných informácií použitých na nastavenie a používanie softvéru ESET Secure Data licenčných kódov, súborov kľúčov a ďalších údajov generovaných na samostatné ukladacie médiá;

d) ste zodpovední za používanie Produktov. Poskytovateľ nenesie zodpovednosť za žiadne straty, nároky ani škody vzniknuté v dôsledku neoprávneného alebo chybného šifrovania alebo dešifrovania informácií alebo iných údajov, akokoľvek a kdekoľvek sú tieto informácie alebo iné údaje ukladané;

e) aj keď Poskytovateľ prijal všetky primerané opatrenia na zabezpečenie integrity a bezpečnosti softvéru ESET Secure Data, Produkty (alebo ktorýkoľvek z nich) nesmú byť použité v žiadnej oblasti, ktorá je závislá od úrovne zabezpečenia typu Fail-Safe alebo je potenciálne riskantná alebo nebezpečná vrátane, nie však výhradne, jadrových zariadení, leteckej navigácie, riadiacich alebo komunikačných systémov, zbraňových a obranných systémov a systémov na podporu života a sledovanie životných funkcií;

f) je zodpovednosťou Koncového používateľa zabezpečiť, aby úroveň zabezpečenia a šifrovania poskytovaná produktmi bola adekvátna vzhľadom na vaše požiadavky;

g) ste zodpovední za používanie Produktov (alebo ktoréhokoľvek z nich) vrátane, nie však výhradne, za zaistenie toho, aby sa používali v súlade so všetkými platnými zákonmi a predpismi Slovenskej republiky alebo inej krajiny, oblasti alebo štátu, kde sa Produkt používa. Pred použitím Produktov sa musíte uistiť, že nie sú v rozpore so žiadnym vládnym embargom (v Slovenskej republike alebo inak);

h) softvér ESET Secure Data môže občas kontaktovať servery Poskytovateľa s cieľom overiť informácie o licencii, dostupnosti opráv, balíkoch Service Pack a ďalších aktualizáciách, ktoré môžu zlepšovať, udržiavať alebo

upravovať fungovanie softvéru ESET Secure Data, a môže odosielať všeobecné systémové informácie týkajúce sa svojho fungovania v súlade so zásadami ochrany osobných údajov.

i) Poskytovateľ nenesie zodpovednosť za žiadne straty, škody, výdavky ani nároky vyplývajúce zo straty, odcudzenia, nesprávneho použitia, poškodenia, zničenia alebo deštrukcie hesiel, nastavenia informácií, šifrovacích kľúčov, licenčných aktivačných kódov a ďalších údajov generovaných alebo ukladaných počas používania softvéru.

Ďalšie ustanovenia o funkcii ESET Secure Data sa vzťahujú výlučne na Koncových používateľov softvéru ESET Smart Security Premium.

Password Manager Software. Na Password Manager Software sa vzťahujú ďalšie ustanovenia, ako je uvedené nižšie:

1. Dodatočné vyhlásenie Koncového používateľa. Beriete na vedomie a súhlasíte s tým, že nesmiete:

a) používať Password Manager Software na prevádzkovanie žiadnych kritických aplikácií v situáciách, kedy je v stávke ľudský život alebo majetok. Beriete na vedomie, že Password Manager Software nie je určený na také účely a že jeho zlyhanie by v takýchto prípadoch mohlo viesť k smrti, zraneniam či závažnému poškodeniu majetku alebo životného prostredia, za ktoré Poskytovateľ nenesie žiadnu zodpovednosť.

PASSWORD MANAGER SOFTWARE NIE JE NAVRHNUTÝ, URČENÝ ANI LICENCOVANÝ NA POUŽITIE V RIZIKOVÝCH PROSTREDIACH VYŽADUJÚCICH BEZPORUCHOVÚ PREVÁDZKU S KONTROLNÝMI MECHANIZMAMI TYPU FAIL-SAFE VRÁTANE, NIE VŠAK VÝHRADNE, PROJEKTOVANIA, VÝSTAVBY, ÚDRŽBY ALEBO PREVÁDZKY JADROVÝCH ZARIADENÍ, LETECKÝCH NAVIGAČNÝCH ALEBO KOMUNIKAČNÝCH SYSTÉMOV, RIADENIA LETOVEJ PREVÁDZKY A PODPORY ŽIVOTNÝCH FUNKCIÍ ALEBO ZBRAŇOVÝCH SYSTÉMOV. POSKYTOVATEĽ ZVLÁŠŤ ODMIETA VÝSLOVNE UVEDENÉ ČI PREDPOKLADANÉ ZÁRUKY VHODNOSTI PRE TIETO ÚČELY.

b) používať softvér Password Manager Software spôsobom, ktorý je v rozpore s touto Dohodou alebo zákonmi Slovenskej republiky alebo vašej jurisdikcie. Osobitne nesmiete softvér Password Manager Software používať na vykonávanie alebo propagovanie akýchkoľvek nelegálnych činností vrátane nahrávania údajov so škodlivým obsahom alebo obsahom, ktorý sa môže použiť na akékoľvek nelegálne činnosti alebo ktorý akýmkoľvek spôsobom porušuje právne predpisy alebo práva akejkoľvek tretej strany (vrátane akýchkoľvek práv duševného vlastníctva), vrátane, nie však výlučne, akýchkoľvek pokusov o získanie prístupu k účtom v Úložisku (na účely týchto ďalších ustanovení o softvéri Password Manager Software Úložisko znamená priestor na ukladanie údajov spravovaný Poskytovateľom alebo treťou stranou inou ako Poskytovateľ a používateľom na účely umožnenia synchronizácie a zálohovania údajov používateľa) alebo k akýmkoľvek účtom a údajom iných používateľov softvéru Password Manager Software alebo Úložiska. Ak porušíte ktorékoľvek z týchto ustanovení, Poskytovateľ je oprávnený okamžite ukončiť túto Dohodu a požadovať od vás úhradu nákladov na prípadné potrebné nápravné opatrenia, ako aj prijať akékoľvek potrebné kroky na to, aby vám zabránil v ďalšom používaní softvéru Password Manager Software, a to bez možnosti vrátenia peňazí.

2. OBMEDZENIE ZODPOVEDNOSTI. PASSWORD MANAGER SOFTWARE SA POSKYTUJE „TAK, AKO JE“. ŽIADNA ZÁRUKA AKÉHOKOĽVEK DRUHU NIE JE VYJADRENÁ ANI PREDPOKLADANÁ. SOFTVÉR POUŽÍVATE NA VLASTNÉ NEBEZPEČENSTVO. VÝROBCA NIE JE ZODPOVEDNÝ ZA STRATU ÚDAJOV, ŠKODY, OBMEDZENIE DOSTUPNOSTI SLUŽIEB VRÁTANE VŠETKÝCH ÚDAJOV ODOSLANÝ SOFTVÉROM PASSWORD MANAGER SOFTWARE NA EXTERNÝ UKLADACÍ PRIESTOR S CIEĽOM SYNCHRONIZÁCIE A ZÁLOHOVANIA ÚDAJOV. ŠIFROVANIE ÚDAJOV POMOCOU SOFTVÉRU PASSWORD MANAGER SOFTWARE NEIMPLIKUJE ŽIADNU ZODPOVEDNOSŤ POSKYTOVATEĽA S OHĽADOM NA BEZPEČNOSŤ TÝCHTO ÚDAJOV. VÝSLOVNE SÚHLASÍTE S TÝM, ŽE ÚDAJE ZÍSKANÉ, POUŽÍVANÉ, ŠIFROVANÉ, UKLADANÉ, SYNCHRONIZOVANÉ ALEBO ODOSIELANÉ POMOCOU SOFTVÉRU PASSWORD MANAGER SOFTWARE MÔŽU BYŤ TIEŽ ULOŽENÉ NA SERVEROCH TRETÍCH STRÁN (PLATÍ LEN NA POUŽÍVANIE SOFTVÉRU PASSWORD MANAGER SOFTWARE, PRI KTOROM BOLA POVOLENÁ SYNCHRONIZÁCIA A ZÁLOHOVANIE SLUŽIEB). AK SA POSKYTOVATEĽ PODĽA VLASTNÉHO UVÁŽENIA ROZHODNE POUŽÍVAŤ TAKÝTO UKLADACÍ PRIESTOR TRETEJ STRANY, WEBOVÉ STRÁNKY, WEBOVÝ PORTÁL, SERVER ALEBO SLUŽBU, POSKYTOVATEĽ NENESIE ZODPOVEDNOSŤ

ZA KVALITU, BEZPEČNOSŤ ALEBO DOSTUPNOSŤ TAKEJTO SLUŽBY TRETEJ STRANY A V ŽIADNOM ROZSAHU NIE JE POSKYTOVATEĽ ZODPOVEDNÝ ZA PORUŠENIE ZMLUVNÝCH ALEBO ZÁKONNÝCH POVINNOSTÍ TRETEJ STRANY, ANI ZA ŠKODY, UŠLÝ ZISK, FINANČNÉ ALEBO NEFINANČNÉ ŠKODY, ALEBO AKÝKOĽVEK INÝ DRUH STRATY, KU KTOREJ DOŠLO PRI POUŽÍVANÍ TOHTO SOFTVÉRU. POSKYTOVATEĽ NENESIE ZODPOVEDNOSŤ ZA OBSAH AKÝCHKOĽVEK ÚDAJOV ZÍSKANÝCH, POUŽÍVANÝCH, ŠIFROVANÝCH, UKLADANÝCH, SYNCHRONIZOVANÝCH ALEBO ODOSIELANÝCH POUŽITÍM SOFTVÉRU PASSWORD MANAGER SOFTWARE ALEBO UKLADACIEHO PRIESTORU. BERIETE NA VEDOMIE, ŽE POSKYTOVATEĽ NEMÁ PRÍSTUP K OBSAHU ULOŽENÝCH ÚDAJOV A NIE JE SCHOPNÝ SLEDOVAŤ ANI ODSTRÁNIŤ OBSAH PORUŠUJÚCI ZÁKONY.

Poskytovateľ vlastní všetky práva na vylepšenia, inovácie a opravy súvisiace so softvérom Password Manager Software (ďalej len „Vylepšenia“), a to aj v prípade, že ľubovoľné z týchto vylepšení boli vytvorené na základe spätnej väzby, nápadov alebo návrhov predložených vami v akejkoľvek forme. Nebudete mať nárok na žiadnu náhradu vrátane akýchkoľvek licenčných poplatkov súvisiacich s takýmito Vylepšeniami.

SUBJEKTY A POSKYTOVATELIA LICENCIÍ POSKYTOVATEĽA NEBUDÚ ZODPOVEDNÍ ZA POHĽADÁVKY A ZÁVÄZKY AKÉHOKOĽVEK DRUHU VYPLÝVAJÚCE Z POUŽÍVANIA SOFTVÉRU PASSWORD MANAGER SOFTWARE VAMI ALEBO TRETÍMI STRANAMI, ANI AKOKOĽVEK SPOJENÉ S TAKÝMTO POUŽÍVANÍM, ANI ZA POUŽÍVANIE ALEBO NEPOUŽÍVANIE AKEJKOĽVEK MAKLÉRSKEJ FIRMY ALEBO PREDAJCU, ANI ZA PREDAJ ALEBO KÚPU AKÉHOKOĽVEK CENNÉHO PAPIERA, A TO BEZ OHĽADU NA TO, ČI SÚ TIETO POHĽADÁVKY A ZÁVÄZKY ZALOŽENÉ NA ZÁKONNEJ ALEBO SPRAVODLIVEJ TEÓRII.

SUBJEKTY A POSKYTOVATELIA LICENCIÍ POSKYTOVATEĽA NIE SÚ ZODPOVEDNÍ ZA ŽIADNE ANI VŠETKY PRIAME, NÁHODNÉ, ZVLÁŠTNE, NEPRIAME ALEBO NÁSLEDNÉ ŠKODY VYPLÝVAJÚCE Z AKÉHOKOĽVEK SOFTVÉRU TRETÍCH STRÁN, PRÍSTUPU K ÚDAJOM PROSTREDNÍCTVOM SOFTVÉRU PASSWORD MANAGER SOFTWARE, VÁŠHO POUŽÍVANIA ALEBO NEMOŽNOSTI POUŽÍVAŤ ALEBO ZÍSKAŤ PRÍSTUP K SOFTVÉRU PASSWORD MANAGER SOFTWARE ALEBO AKÝMKOĽVEK ÚDAJOM POSKYTOVANÝM SOFTVÉROM PASSWORD MANAGER SOFTWARE ANI ZA TAKÉ ŠKODY SÚVISIACE SO SPOMÍNANÝM, ČI SÚ TIETO NÁROKY NA NÁHRADU ŠKODY UPLATŇOVANÉ NA ZÁKLADE AKEJKOĽVEK TEÓRIE PRÁVA, ALEBO SPRAVODLIVOSTI. ŠKODY VYLÚČENÉ TOUTO KLAUZULOU BEZ OBMEDZENIA ZAHŔŇAJÚ ŠKODY VYPLÝVAJÚCE ZO STRATY ZISKU, ZRANENIA OSÔB ALEBO POŠKODENIA MAJETKU, PRERUŠENIA PODNIKANIA, STRATY OBCHODNÝCH ALEBO OSOBNÝCH INFORMÁCIÍ. NIEKTORÉ PRÁVNE PORIADKY NEPOVOĽUJÚ OBMEDZENIA NÁHODNÝCH ALEBO NÁSLEDNÝCH ŠKÔD, TAKŽE TOTO OBMEDZENIE SA NA VÁS NEMUSÍ VZŤAHOVAŤ. V TAKOM PRÍPADE BUDE MINIMÁLNA POVOLENÁ MIERA ZODPOVEDNOSTI POSKYTOVATEĽA STANOVENÁ PODĽA PLATNÝCH PRÁVNYCH PREDPISOV.

INFORMÁCIE POSKYTOVANÉ PROSTREDNÍCTVOM SOFTVÉRU PASSWORD MANAGER SOFTWARE VRÁTANE INFORMÁCIÍ A AKCIÁCH, ANALÝZ, INFORMÁCIÍ O TRHU, SPRÁV A FINANČNÝCH ÚDAJOV MÔŽU BYŤ ONESKORENÉ, NEPRESNÉ ALEBO MÔŽU OBSAHOVAŤ CHYBY ALEBO OPOMENUTIA A SUBJEKTY A POSKYTOVATELIA LICENCIÍ POSKYTOVATEĽA NEBUDE NIESŤ V SÚVISLOSTI S NIMI ŽIADNU ZODPOVEDNOSŤ. POSKYTOVATEĽ MÔŽE ZMENIŤ ALEBO PRERUŠIŤ AKÝKOĽVEK ASPEKT ALEBO FUNKCIU SOFTVÉRU PASSWORD MANANGER SOFTWARE ALEBO POUŽÍVANIE VŠETKÝCH ALEBO NIEKTORÝCH FUNKCIÍ ALEBO TECHNOLÓGIÍ SOFTVÉRU PASSWORD MANANGER SOFTWARE KEDYKOĽVEK A BEZ PREDCHÁDZAJÚCEHO UPOZORNENIA.

V PRÍPADE, ŽE SÚ USTANOVENIA V TOMTO ČLÁNKU Z AKÉHOKOĽVEK DÔVODU NEPLATNÉ ALEBO JE POSKYTOVATEĽ POVAŽOVANÝ ZA ZODPOVEDNÉHO ZA STRATY, ŠKODY ATĎ. V SÚLADE S PLATNÝMI ZÁKONMI, V TAKOM PRÍPADE SA STRANY DOHODLI, ŽE ZODPOVEDNOSŤ POSKYTOVATEĽA BUDE VO VZŤAHU K VÁM OBMEDZENÁ NA CELKOVÚ VÝŠKU LICENČNÝCH POPLATKOV, KTORÉ STE UHRADILI.

SÚHLASÍTE S TÝM, ŽE ODŠKODNÍTE, BUDETE CHRÁNIŤ A BRÁNIŤ POSKYTOVATEĽA A JEHO ZAMESTNANCOV, DCÉRSKE SPOLOČNOSTI, PRIDRUŽENÉ SPOLOČNOSTI, REBRANDINGOVÉ SUBJEKTY A ĎALŠÍCH PARTNEROV V PRÍPADE AKÝCHKOĽVEK POHĽADÁVOK, ZÁVÄZKOV, ŠKÔD, STRÁT, NÁKLADOV, VÝDAVKOV A POPLATKOV NÁROKOVANÝCH TRETÍMI STRANAMI (VRÁTANE VLASTNÍKOV ZARIADENÍ ALEBO SUBJEKTOV, KTORÝCH PRÁVA BOLI OVPLYVNENÉ ÚDAJMI POUŽITÝMI V SOFTVÉRI ALEBO V UKLADACÍCH PRIESTOROCH), KTORÉ MOHLI TÝMTO STRANÁM VZNIKNÚŤ V DÔSLEDKU VÁŠHO POUŽÍVANIA SOFTVÉRU PASSWORD MANAGER SOFTWARE.

3. Údaje v softvéri Password Manager Software. Ak nie je inak a výslovne vybraté vami, všetky údaje zadané vami, ktoré sa ukladajú do databázy softvéru Password Manager Software, sa ukladajú v šifrovanom formáte vo vašom počítači alebo inom pamäťovom zariadení, ktoré definujete. Beriete na vedomie, že v prípade odstránenia alebo poškodenia ľubovoľnej databázy alebo iných súborov softvéru Password Manager Software, budú všetky údaje v nich obsiahnuté nenávratne stratené a chápete a akceptujete riziko takejto straty. Skutočnosť, že sú Vaše osobné údaje uložené v šifrovanom formáte v počítači neznamená, že informácie nemôžu byť odcudzené alebo zneužité niekým, kto získa hlavné heslo alebo získa prístup k aktivačnému zariadeniu definovanému zákazníkom na otvorenie databázy. Ste zodpovední za udržiavanie bezpečnosti všetkých spôsobov prístupu.

4. Prenos osobných údajov poskytovateľovi alebo do ukladacieho priestoru. Password Manager Software prenáša alebo odosiela osobné údaje z databázy softvéru Password Manager Software – menovite heslá, prihlasovacie údaje, účty a identity – do ukladacieho priestoru cez internet, ak si vyberiete takú možnosť a vykonáva to výhradne za účelom zaistenia včasnej synchronizácie a zálohovania údajov. Údaje sa prenášajú výhradne v šifrovanej podobe. Používanie softvéru Password Manager Software na vypĺňanie online formulárov zadávaním hesiel, prihlasovacích údajov alebo iných údajov môže vyžadovať, aby sa tieto informácie odoslali cez internet na webovú stránku, ktorú identifikujete. Tento prenos údajov nie je iniciovaný softvérom Password Manager Software, preto Poskytovateľ nemôže byť zodpovedný za bezpečnosť takýchto interakcií s ľubovoľnou webovou stránkou, ktorú podporujú rôzni poskytovatelia. Všetky transakcie cez internet, či už v spojitosti alebo bez spojitosti so softvérom Password Manager Software, vykonávate podľa vlastného uváženia a na vlastné riziko a budete mať výhradnú zodpovednosť za všetky poškodenie svojho počítačového systému alebo stratu údajov vyplývajúcich zo sťahovanie a/alebo používania niektorého takéhoto materiálu alebo služby. Na minimalizovanie rizika straty cenných údajov Poskytovateľ odporúča, aby zákazníci vykonávali pravidelné zálohovanie databázy a ďalších citlivých súborov na externé disky. Poskytovateľ nie je schopný poskytnúť vám všetku pomoc pri obnove stratených alebo poškodených údajov. Ak Poskytovateľ poskytuje služby zálohovania pre databázové súbory používateľov, v prípade poškodenia alebo odstránenia súborov z počítačov používateľov, takáto služba zálohovania sa poskytuje bez akejkoľvek záruky a neimplikuje vo vzťahu k vám žiadnu zodpovednosť Poskytovateľa.

Používaním softvéru Password Manager Software súhlasíte s tým, že softvér môže občas kontaktovať servery Poskytovateľa s cieľom overiť informácie o licencii, dostupnosti opráv, balíkoch Service Pack a ďalších aktualizáciách, ktoré môžu zlepšovať, udržiavať alebo upravovať fungovanie softvéru Password Manager Software. Softvér môže odosielať všeobecné systémové informácie týkajúce sa fungovania softvéru Password Manager Software v súlade so zásadami ochrany osobných údajov.

5. Informácie o odinštalovaní a pokyny na odinštalovanie. Všetky informácie v databáze, ktoré by ste chceli zachovať, musíte pred odinštalovaním softvéru Password Manager Software vyexportovať.

Ďalšie ustanovenia o softvéri Password Manager Software sa vzťahujú výlučne na Koncových používateľov softvéru ESET Smart Security Premium.

ESET LiveGuard. Na funkciu ESET LiveGuard sa vzťahujú ďalšie ustanovenia, ako je uvedené nižšie:

Softvér obsahuje funkciu ďalšej analýzy súborov odoslaných Koncovým používateľom. Poskytovateľ použije súbory odoslané Koncovým používateľom a výsledky analýzy len v súlade so Zásadami ochrany osobných údajov a v súlade s príslušnými právnymi predpismi.

Ďalšie ustanovenia o funkcii ESET LiveGuard sa vzťahujú výlučne na Koncových používateľov softvéru ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Zásady ochrany osobných údajov

Spoločnosť ESET, spol. s r. o. so sídlom na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka číslo 3586/B, IČO: 31333532, ako prevádzkovateľ údajov (ďalej len „ESET“ alebo „my“) kladie veľký dôraz na ochranu osobných údajov. Chceme splniť požiadavku transparentnosti, ktorá je právne štandardizovaná vo všeobecnom nariadení EÚ o ochrane údajov (ďalej len „GDPR“). S týmto cieľom zverejňujeme tieto zásady ochrany osobných údajov, ktorých jediným účelom je informovať nášho zákazníka (ďalej len „koncový používateľ“ alebo „vy“) ako dotknutú osobu o týchto témach ochrany osobných údajov:

- právny základ spracúvania osobných údajov;
- zdieľanie a dôvernosť údajov;
- bezpečnosť údajov;
- práva, ktoré máte ako dotknutá osoba;
- spracúvanie osobných údajov;
- Kontaktné informácie.

Právny základ spracúvania osobných údajov

Existuje len niekoľko právnych základov spracovania údajov, ktoré využívame v súlade s príslušným právnym rámcom týkajúcim sa ochrany osobných údajov. Spracúvanie osobných údajov spoločnosťou ESET je potrebné najmä preto, aby sa mohla plniť Licenčná dohoda s koncovým používateľom (ďalej len „EULA“) (článok 6 ods. 1 písm. b) nariadenia GDPR), ktorá sa vzťahuje na poskytovanie produktov alebo služieb spoločnosti ESET, pokiaľ nie je výslovne uvedené inak, napríklad:

- Právny základ oprávneného záujmu (článok 6 ods. 1 písm. f) nariadenia GDPR), ktorý nám umožňuje spracúvať údaje o tom, ako naši zákazníci používajú naše služby a ako sú s nimi spokojní, aby sme používateľom poskytli čo najlepšiu ochranu, podporu a skúsenosti. Príslušné právne predpisy uznávajú ako oprávnený záujem dokonca aj marketing, a preto sa naň spoliehame pri marketingovej komunikácii s našimi zákazníkmi.

- Súhlas (článok 6 ods. 1 písm. a) nariadenia GDPR), o ktorý vás môžeme požiadať v špecifických situáciách, keď tento právny základ považujeme za najvhodnejší, alebo ak to vyžaduje zákon.

- Splnenie zákonnej povinnosti (článok 6 ods. 1 písm. c) nariadenia GDPR), napríklad pokiaľ ide o stanovenie požiadaviek týkajúcich sa elektronickej komunikácie alebo uchovávania fakturačných a účtovných dokumentov.

Zdieľanie a dôvernosť údajov

Vaše údaje nezdieľame s tretími stranami. Spoločnosť ESET však pôsobí globálne prostredníctvom pridružených spoločností alebo partnerov v rámci svojej siete predaja, služieb a podpory. Informácie o správe licencií, účtovaní a technickej podpore spracúvané spoločnosťou ESET sa môžu prenášať medzi pridruženými subjektmi alebo partnermi na účely plnenia dohody EULA, ako je napríklad poskytovanie služieb alebo podpory.

Spoločnosť ESET uprednostňuje spracúvanie údajov v krajinách Európskej únie (EÚ). V závislosti od vašej polohy (používanie našich produktov a/alebo služieb mimo EÚ) a/alebo vami vybratej služby však môže byť nevyhnutné preniesť vaše údaje do krajiny mimo EÚ. Využívame napríklad služby tretích strán spojené s cloudovou

výpočtovou technikou. V týchto prípadoch si dôkladne vyberáme poskytovateľov služieb a dbáme na ochranu údajov na primeranej úrovni prostredníctvom zmluvných, ale tiež technických a organizačných opatrení. V prípade potreby sa spravidla dohodneme na štandardných zmluvných doložkách EÚ s doplnkovými zmluvnými pravidlami.

Pri niektorých krajinách mimo EÚ, ako je napríklad Spojené kráľovstvo a Švajčiarsko, už EÚ určila porovnateľnú úroveň ochrany údajov. Z dôvodu porovnateľnej úrovne ochrany údajov sa pri prenose údajov do týchto krajín nevyžaduje žiadne osobitné oprávnenie ani dohoda.

Bezpečnosť údajov

Spoločnosť ESET realizuje vhodné technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti, ktorá zodpovedá potenciálnym rizikám. Čo najlepšie sa snažíme zabezpečiť neustálu dôvernosť, integritu, dostupnosť a odolnosť systémov a služieb spracovania údajov. V prípade úniku údajov, ktorý má za následok ohrozenie vašich práv a slobôd, sme však pripravení informovať príslušný dozorný orgán, ako aj koncových používateľov ako dotknuté osoby.

Práva dotknutej osoby

Práva každého koncového používateľa sú dôležité a chceme vás informovať, že všetci koncoví používatelia (z ktorejkoľvek krajiny EÚ aj mimo EÚ) majú práva uvedené nižšie zaručené spoločnosťou ESET. Ak chcete uplatniť svoje práva dotknutej osoby, môžete nás kontaktovať prostredníctvom formulára podpory alebo e-mailom na adrese dpo@eset.sk. Na účely identifikácie vás požiadame o tieto informácie: meno, e-mailovú adresu a (ak sú tieto informácie k dispozícii) licenčný kľúč alebo číslo zákazníka a pridruženú spoločnosť. Neodosielajte nám žiadne iné osobné údaje, napríklad dátum narodenia. Chceme zdôrazniť, že na účely spracovania vašej žiadosti, ako aj na účely identifikácie, budeme spracúvať vaše osobné údaje.

Právo na odvolanie súhlasu. Právo na odvolanie súhlasu sa uplatňuje v prípade spracúvania, ktoré je založené len na súhlase. Ak vaše osobné údaje spracúvame na základe vášho súhlasu, máte právo súhlas kedykoľvek odvolať aj bez uvedenia dôvodu. Odvolanie súhlasu je účinné len pre budúcnosť a nemá vplyv na zákonnosť spracúvania údajov pred odvolaním.

Právo namietať. Právo namietať voči spracúvaniu sa uplatňuje v prípade spracúvania na základe oprávneného záujmu spoločnosti ESET alebo tretej strany. Ak vaše osobné údaje spracúvame na ochranu oprávneného záujmu, ako dotknutá osoba máte právo kedykoľvek namietať voči nami uvedenému oprávnenému záujmu a spracúvaniu vašich osobných údajov. Vaša námietka je účinná len pre budúcnosť a nemá vplyv na zákonnosť spracúvania údajov pred námietkou. Ak vaše osobné údaje spracúvame na účely priameho marketingu, nie je potrebné uvádzať dôvody námietky. Platí to aj pre profilovanie, pokiaľ je spojené s takýmto priamym marketingom. Vo všetkých ostatných prípadoch vás požiadame, aby ste nás stručne informovali o svojich sťažnostiach týkajúcich sa oprávneného záujmu spoločnosti ESET spracúvať vaše osobné údaje.

V niektorých prípadoch máme oprávnenie napriek vášmu odvolaniu súhlasu ďalej spracúvať vaše osobné údaje na inom právnom základe, napríklad na účely plnenia zmluvy.

Právo prístupu. Ako dotknutá osoba máte právo kedykoľvek bezplatne získať informácie o svojich údajoch, ktoré uchováva spoločnosť ESET.

Právo na opravu. Ak neúmyselne spracúvame vaše nesprávne osobné údaje, máte právo na ich opravu.

Právo na vymazanie a právo na obmedzenie spracúvania. Ako dotknutá osoba máte právo požiadať o vymazanie alebo obmedzenie spracúvania svojich osobných údajov. Ak napríklad vaše osobné údaje spracúvame s vaším súhlasom, odvoláte ho a neexistuje žiadny iný právny základ, ako je napríklad zmluva, vaše osobné údaje vymažeme okamžite. Vaše osobné údaje tiež budú vymazané, keď už nebudú potrebné na účely, ktoré sú pre ne

uvedené, na konci nášho obdobia uchovávania.

Ak vaše osobné údaje používame výhradne na účely priameho marketingu a odvoláte súhlas alebo budete namietať voči existujúcemu oprávnenému záujmu spoločnosti ESET, spracúvanie vašich osobných údajov obmedzíme tak, že pridáme vaše kontaktné údaje do svojho interného blacklistu, aby nedošlo k nevyžiadanému kontaktu. V opačnom prípade sa vaše osobné údaje vymažú.

Upozorňujeme, že sa od nás môže žiadať, aby sme vaše údaje uchovávali až do uplynutia povinností a období uchovávania stanovených zákonodarcom alebo dozornými orgánmi. Povinnosti a obdobia uchovávania tiež môžu vyplývať z právnych predpisov Slovenskej republiky. Po ich uplynutí sa príslušné údaje vymažú zvyčajným spôsobom.

Právo na prenosnosť údajov. Ako dotknutej osobe vám radi poskytneme osobné údaje spracúvané spoločnosťou ESET vo formáte XLS.

Právo podať sťažnosť. Ako dotknutá osoba máte právo kedykoľvek podať sťažnosť dozornému orgánu. Spoločnosť ESET podlieha slovenským zákonom a je viazaná právnymi predpismi Európskej únie o ochrane údajov. Príslušným dozorným orgánom na ochranu údajov je Úrad na ochranu osobných údajov Slovenskej republiky so sídlom na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Spracúvanie osobných údajov

Služby poskytované spoločnosťou ESET a realizované v rámci nášho produktu sa poskytujú v súlade s podmienkami dohody LICENČNÁ DOHODA (EULA), ale niektoré z nich si môžu vyžadovať osobitnú pozornosť. Chceme vám poskytnúť podrobnejšie informácie o zhromažďovaní údajov, ktoré súvisí s poskytovaním našich služieb. Poskytujeme rôzne služby, ktoré sú opísané v zmluve EULA, ako aj v produktovej dokumentácii. Poskytujeme rôzne služby opísané v dohode EULA a produktovej dokumentácii. Nato, aby všetko fungovalo, ako má, musíme zhromažďovať tieto informácie:

Licenčné a účtovné údaje. Spoločnosť ESET zhromažďuje a spracúva meno, e-mailovú adresu, licenčný kľúč a (v prípade potreby) adresu, pridruženú spoločnosť a platobné údaje, aby mohla zabezpečiť aktiváciu licencie, poskytnutie licenčného kľúča, pripomenutia uplynutia platnosti, plnenie žiadostí o podporu, overenie pravosti licencií, poskytovanie svojej služby a iné upozornenia vrátane marketingových oznámení v súlade s príslušnými právnymi predpismi alebo vaším súhlasom. Spoločnosť ESET má zákonnú povinnosť uchovávať účtovné informácie počas obdobia 10 rokov, licenčné informácie sa však najneskôr 12 mesiacov od uplynutia platnosti licencie anonymizujú.

Informácie o aktualizáciách a ďalšie štatistické informácie. Spracúvané informácie zahŕňajú informácie týkajúce sa procesu inštalácie a počítača vrátane informácií o platforme, na ktorej je nainštalovaný náš produkt, a informácií o operáciách a funkčnosti našich produktov, napríklad informácií o operačnom systéme, hardvéri, identifikátoroch inštalácie, identifikátoroch licencie, IP adrese, MAC adrese a nastaveniach konfigurácie produktu. Spracúvajú sa na účely poskytovania služieb aktualizácie a inovácie a na účely údržby, zabezpečenia a vylepšenia našej infraštruktúry koncových serverov.

Tieto informácie sa uchovávajú oddelene od identifikačných informácií potrebných na účely správy licencií a účtovania, pretože nevyžadujú identifikáciu koncového používateľa. Obdobie uchovávania je najviac 4 roky.

Reputačný systém **ESET LiveGrid®.** Jednosmerné hashe súvisiace s infiltráciou sa spracúvajú na účely reputačného systému ESET LiveGrid®, ktorý zlepšuje účinnosť našich antimalvérových riešení na základe porovnávania kontrolovaných súborov s databázou položiek zaradených na whitelist a blacklist v cloude. Počas tohto procesu sa koncový používateľ neidentifikuje.

Systém spätnej väzby **ESET LiveGrid®.** Prijaté podozrivé vzorky a metadáta zhromažďované v rámci systému spätnej väzby ESET LiveGrid®, ktoré umožňujú spoločnosti ESET okamžite reagovať na potreby svojich koncových používateľov, ako aj na najnovšie hrozby. Spoliehame sa na to, že nám zašlete

- Infiltrácie, ako napríklad vzorky potenciálnych vírusov a iných škodlivých a podozrivých programov; problematické, potenciálne neželané alebo potenciálne nebezpečné objekty, ako napríklad spustiteľné súbory, e-mailové správy, ktoré ste nahlásili ako spam alebo ktoré takto označil váš produkt;

- Informácie o používaní internetu, ako napríklad IP adresu, geografické informácie, IP pakety, URL adresy a ethernetové rámce;

- Súbory výpisov pri zlyhaní a informácie, ktoré obsahujú.

Nemáme v úmysle zhromažďovať vaše údaje mimo tohto rozsahu, niekedy sa tomu však nedá zabrániť. Náhodne zhromaždené údaje môžu byť obsiahnuté v samotnom malvéri (zhromaždené bez vášho vedomia alebo súhlasu) alebo môžu byť súčasťou názvov súborov či URL adries a my nemáme v úmysle začleniť ich do našich systémov ani ich spracovať na účely uvedené v týchto zásadách ochrany osobných údajov.

Všetky informácie získané a spracúvané prostredníctvom systému spätnej väzby ESET LiveGrid® sú určené na používanie bez identifikácie koncového používateľa.

Vyhodnotenie bezpečnosti zariadení pripojených k sieti. Na účely poskytovania funkcie vyhodnotenia bezpečnosti spracúvame názov lokálnej siete a informácie o zariadeniach pripojených k lokálnej sieti, ako je prítomnosť, typ, názov, IP adresa a MAC adresa zariadenia v lokálnej sieti v spojitosti s licenčnými informáciami. Informácie zahŕňajú typ bezdrôtového zabezpečenia a typ bezdrôtového šifrovania pre sieťové smerovače. Informácie o licencii identifikujúce koncového používateľa sa najneskôr 12 mesiacov od uplynutia platnosti licencie anonymizujú.

Technická podpora. Kontaktné a licenčné informácie a údaje obsiahnuté vo vašich žiadostiach o podporu sa môžu vyžadovať na poskytnutie podpory. Podľa toho, akým spôsobom sa nás rozhodnete kontaktovať, môžeme zhromažďovať informácie, ako sú napríklad vaša e-mailová adresa, telefónne číslo, licenčné informácie, podrobnosti o produkte a popis vášho konkrétneho prípadu podpory. Na zjednodušenie poskytnutia služby podpory vás môžeme požiadať o poskytnutie ďalších informácií. Údaje spracúvané na účely technickej podpory sa uchovávajú 4 roky.

Ochrana proti zneužitiu údajov. V prípade vytvorenia účtu ESET HOME na stránke https://home.eset.com a aktivácie funkcie koncovým používateľom v súvislosti s krádežou počítača sa budú zhromažďovať a spracúvať tieto informácie: údaje o polohe, snímky obrazovky, údaje o konfigurácii počítača a údaje zaznamenané kamerou počítača. Zhromaždené údaje sú uložené na našich serveroch alebo na serveroch našich poskytovateľov služieb, pričom obdobie uchovávania je 3 mesiace.

Password Manager. Ak sa rozhodnete aktivovať funkciu Password Manager, údaje súvisiace s vaším prihlásením budú uložené v zašifrovanej podobe iba vo vašom počítači alebo inom určenom zariadení. Ak aktivujete synchronizačnú službu, šifrované údaje sa uložia na našich serveroch alebo na serveroch našich poskytovateľov služieb. Spoločnosť ESET ani poskytovateľ služieb nemajú prístup k šifrovaným údajom. Iba vy máte kľúč na dešifrovanie údajov. Pri deaktivácii funkcie sa údaje odstránia.

ESET LiveGuard. Ak sa rozhodnete aktivovať funkciu ESET LiveGuard, bude sa vyžadovať odosielanie vzoriek, napríklad súborov preddefinovaných a vybratých koncovým používateľom. Vzorky, ktoré vyberiete na vzdialenú analýzu, sa nahrajú do služby spoločnosti ESET, pričom výsledok analýzy sa odošle späť do vášho počítača. Všetky podozrivé vzorky sa spracujú rovnako ako informácie zhromaždené systémom spätnej väzby ESET LiveGrid®.

Program zvyšovania spokojnosti zákazníkov Ak sa rozhodnete aktivovať Program zvyšovania spokojnosti

zákazníkov , anonymné telemetrické informácie týkajúce sa použitia našich produktov budú získavané a používané na základe vášho súhlasu.

Ak osoba, ktorá používa naše produkty a služby, nie je koncovým používateľom, ktorý si príslušný produkt alebo službu zakúpil a uzatvoril s nami dohodu EULA (napríklad zamestnanec koncového používateľa, jeho rodinný príslušník alebo osoba inak oprávnená koncovým používateľom používať produkt alebo službu v súlade s dohodou EULA), spracúvanie údajov sa uskutočňuje v oprávnenom záujme spoločnosti ESET v zmysle článku 6 ods. 1 písm. f) nariadenia GDPR, aby používateľ oprávnený koncovým používateľom mohol používať nami poskytované produkty a služby v súlade s dohodou EULA.

Kontaktné informácie

Ak chcete využiť svoje právo dotknutej osoby alebo chcete položiť otázku či vyjadriť obavu, obráťte sa na nás na adrese:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk