Stručná příručka: Avast Small Office Protection

Pomoc s řešením problémů najdete v naší online dokumentaci:
https://businesshelp.avast.com/

Obsah

Nastavení zařízení

Nová aplikace Avast Small Office Protection se od aplikace Avast Business Antivirus liší následovně:

- maximálně 10 licencí (produkt je určený pro malé firmy s menším počtem zařízení),
- *nelze* nainstalovat na serverové operační systémy,
- lze nainstalovat na zařízeních s Androidem/iOS,
- obsahuje různé komponenty,
- k dispozici pouze pro *nespravovaná* zařízení.

Srovnání komponent aplikací Avast Business Antivirus a Avast Small Office najdete v části Přehled komponent.

Systémové požadavky

Koncová zařízení se Small Office Protection

Windows:

- 7 SP2 nebo vyšší, 8.x kromě edic RT a Starter, 10 kromě edic Mobile a IoT Core Edition

Mac:

- MacOS 10.10 (Mavericks nebo novější a alespoň 500 MB volného místa na disku)

Android:

- Android 4.1 (Jelly Bean) nebo vyšší

iPhone/iPad:

- iOS 12.0 nebo vyšší

Požadavky na nastavení firewallu

Na firewallu nebo proxy serveru je nutné povolit určité porty a webové adresy, aby konzole mohla fungovat, aby klienty Small Office Protection mohly komunikovat a aby fungovalo ověřování.

Porty

TCP a UDP:

- 53 – služby bezpečné DNS (pouze pokud používáte komponentu Ověřené weby)
- 80 – kontroly zranitelnosti na internetu a aktualizace funkcí
- 443 – vyjednávání se šifrovacím klíčem FFL (pouze pokud používáte komponentu Ověřené weby)

Webové adresy

- *.avast.com
- *.avcdn.net
- *.mailshell.net (pouze pokud používáte Antispam)

Instalace Small Office Protection na zařízení

Pracovní stanice s Windows

Instalační soubor nespravované aplikace Small Office Protection si můžete stáhnout odsud. Stažený instalační program můžete spustit na zařízení s Windows, ve kterém chcete nainstalovat antivirus.

Přizpůsobení instalace

1. Instalační soubor zkopírujte do umístění, které je přístupné z koncového zařízení.
2. Dvojím kliknutím instalační soubor spusťte.
3. Když se zobrazí dotaz, zda smí aplikace provádět změny v zařízení, klikněte na možnost **Ano**.
4. Klikněte na možnost **Přizpůsobit** a proveďte jeden z následujících úkonů:
    - Výběrem možnosti **Doporučená ochrana** nainstalujte všechny komponenty.
    - Výběrem možnosti **Minimální ochrana** nainstalujte jen Souborový štít, Webový štít a E-mailový štít.
    - Po výběru možnosti **Vlastní ochrana** můžete zvolit komponenty, které chcete nainstalovat.

5. Klikněte na tlačítko **Nainstalovat** a počkejte, než se Small Office Protection nainstaluje na zařízení.
6. Na výzvu restartujte zařízení.

Doporučené komponenty pro servery a pracovní stanice

Firmy mají jiné potřeby než běžní uživatelé, a proto některé komponenty Small Office Protection nedoporučujeme ve firemních sítích používat.

Doporučeno pro firmy

Následující komponenty je třeba zcela odinstalovat nebo pomocí příslušného posuvníku **vypnout**:

- Ověřené weby
- Inspektor Wi-Fi

Pokud je neodeberete, můžete se potýkat s nestabilitou připojení k síti, pomalejším fungováním počítače nebo chybami.

Zařízení s MacOS X

Instalační soubor nespravované aplikace Small Office Protection si můžete stáhnout odsud. Stažený instalační program můžete spustit na zařízení s MacOS X, ve kterém chcete nainstalovat antivirus.

1. Zkopírujte instalační soubor (.dmg) do umístění, které je ze zařízení přístupné, a zkontrolujte, zda na zařízení neběží žádná jiná aplikace ani antivirový software.
2. Dvakrát klikněte na stažený instalační soubor.
3. Dvakrát klikněte na ikonu Small Office Protection a zavřete okno.
4. Ve vyskakovacím okně klikněte na tlačítko **Pokračovat**, přečtěte si zásady ochrany soukromí a klikněte na tlačítko **Pokračovat**.
5. Kliknutím na tlačítko **Pokračovat** potvrďte, že máte přečtenou *licenční smlouvu s koncovým uživatelem*, a poté kliknutím na tlačítko **Souhlasím** potvrďte přijetí podmínek.
6. Chcete-li případně změnit výchozí nastavení instalace, klikněte na možnost **Přizpůsobit**. Jinak klikněte na tlačítko **Nainstalovat**.
7. Na výzvu použijte své Touch ID nebo zadejte heslo správce a udělte tak svolení k instalaci. Pak klikněte na tlačítko **Nainstalovat software**.

8. Kliknutím na tlačítko OK povolte aplikaci Small Office Protection přístup ke složce se staženými soubory.
9. Pokud se zobrazí oznámení *Bylo zablokováno rozšíření systému*, klikněte na možnost **Otevřít předvolby zabezpečení** a postupujte následovně:
    1. Klikněte na ikonu zámku, zadejte heslo správce, klikněte na tlačítko **Odemknout** a poté na tlačítko **Povolit**.
    2. Vyberte možnost **Soukromí** a pro Small Office Protection zapněte *úplný přístup k disku*. Na výzvu klikněte na tlačítko **Ukončit** a poté zavřete okno **Zabezpečení a soukromí**.
10. Pokud nechcete nainstalovat Google Chrome jako výchozí prohlížeč, zrušte zaškrtnutí příslušného pole a pak klikněte na tlačítko **Pokračovat**.
11. Po dokončení instalace klikněte na tlačítko **Zavřít**. Pak klikněte na možnost **Přesunout do koše**.
12. Kliknutím na tlačítko **OK** povolte instalačnímu programu aplikace Small Office Protection přístup ke složce se staženými soubory.

Zařízení s Androidem

Small Office Protection pro telefon s Androidem si můžete stáhnout z Obchodu Google Play.

1. Otevřete aplikaci Obchod Play.
2. Vyhledejte „Avast".
3. Ze seznamu vyberte položku **Avast Antivirus – ochrana mobilu a čištění virů**.
4. Klikněte na tlačítko **Nainstalovat**.
5. V případě potřeby klikněte na tlačítko **Ano** a spusťte tak stahování.

Zařízení s iOS

Small Office Protection pro telefon s iOS si můžete stáhnout z App Storu.

1. Otevřete App Store.
2. Vyhledejte „Avast Mobile Security".
3. Ze seznamu vyberte možnost **Avast Security & Privacy**.
4. Klepněte na ikonu stažení.
5. Po stažení aplikace klepněte na tlačítko **Otevřít**.

6. Na výzvu klepněte na možnost **Povolit** a povolte aplikaci Avast Security & Privacy zobrazovat oznámení.

Aktivace licencí na zařízení

Předplatné Small Office Protection můžete aktivovat po nainstalování aplikace na zařízení. K nákupu aplikace Small Office Protection byste měli dostat kód předplatného, který slouží k aktivaci aplikace na zařízeních a který je provázaný s vaším účtem Avast. Počet zařízení, ve kterých je možné produkt aktivovat, závisí na zakoupeném předplatném.

Pracovní stanice s Windows

1. Na zařízení otevřete aplikaci Small Office Protection.
2. Klikněte na ikonu **Menu**.
3. Klikněte na možnost **Zadat aktivační kód**.
4. Zadejte aktivační kód a poté klikněte na tlačítko **Zadat**.
5. V případě potřeby potvrďte předplatné a jeho komponenty.

Zařízení s Androidem

Aktivace aktivačním kódem

1. Otevřete aplikaci *Avast Mobile Security* klepnutím na její ikonu na zařízení.
2. Klepněte na možnosti **Menu** ▸ **Odstranit reklamy**.
3. V pravém horním rohu klepněte na ikonu **tří teček** a vyberte možnost **Již zakoupeno**.
4. Vyberte možnost **Uplatnit aktivační kód**.
5. Aktivační kód zadejte nebo vložte do textového pole (včetně pomlček).
6. Aktivaci dokončete klepnutím na tlačítko **Použít tento kód**.

Aktivace účtem Avast

1. Otevřete aplikaci *Avast Mobile Security* klepnutím na její ikonu na zařízení.
2. Klepněte na možnosti **Menu** ▸ **Odstranit reklamy**.
3. V pravém horním rohu klepněte na ikonu **tří teček** a vyberte možnost **Již zakoupeno**.

4. Vyberte možnost **Obnovit z účtu Avast**.
5. Vyberte možnost **E-mail**.
6. Zadejte přihlašovací údaje k účtu Avast.
7. Klepněte na možnost **Přihlásit k účtu Avast**.

Zařízení s iOS

1. Otevřete aplikaci *Avast Security & Privacy* klepnutím na její ikonu na zařízení.
2. Klepněte na tlačítko Upgradovat.
3. Klepněte na možnost **Již zakoupeno**.
4. Vyberte možnost **Zadejte kód předplatného Avastu**.
5. Aktivační kód zadejte nebo vložte do textového pole (včetně pomlček).
6. Aktivaci dokončete klepnutím na tlačítko **OK**.

Konfigurace nastavení a komponenty

Small Office Protection pro pracovní stanice a mobilní zařízení nabízí spoustu komponent.

Komponenty podle operačního systému

Komponenta	Pracovní stanice s Windows	MacOS X	Android	iOS
Souborový štít	X	X		
Webový štít	X	X	X	
E-mailový štít	X	X		
Behaviorální štít	X			
Štít proti ransomwaru	X	X		
Štít vzdáleného přístupu	X			
Inspektor Wi-Fi	X	X		
Ověřené weby	X			
Firewall	X			
Sandbox	X			
Antispam				
Exchange				
Sharepoint				
Štít webové kamery	X			
Štít citlivých dat	X			
SecureLine VPN				
Skartovač dat	X			
Passwords	X			
Ochrana hesel	X			
Aktualizace aplikací	X			
Čištění prohlížečů	X			
Režim Nerušit	X			
Záchranný disk	X			
Testování souborů			X	
Foto trezor			X	X
Ochrana identity				X
Zámek aplikací			X	
Anti-Theft			X	

Komponenta	Pracovní stanice s Windows	MacOS X	Android	iOS
Fotopast			X	
Poslední známá poloha			X	
Zabezpečení SIM			X	
Blokování hovorů			X	
Spořič energie			X	
Optimalizace paměti			X	
Čištění nepotřebných souborů			X	
Test rychlosti Wi-Fi sítě			X	
Wi-Fi test			X	X
Informace o aplikacích			X	
Samostatná VPN aplikace			X	X

Zapnutí a vypnutí komponent

Spoustu štítů a nástrojů v aplikaci Small Office Protection lze v zařízení zapnout či vypnout. To se hodí zejména v případě, kdy instalujete na server jen několik komponent nebo kdy chcete nainstalovat jen minimum nástrojů. Některé nástroje ale lze pouze nainstalovat nebo zcela odinstalovat – například Sandbox nebo Záchranný disk.

1. Otevřete klienta Small Office Protection.
2. Klikněte na kartu komponenty, kterou chcete zapnout nebo vypnout:
   - **Ochrana:** Souborový štít, Webový štít, E-mailový štít, Behaviorální štít, Sandbox, Inspektor Wi-Fi, Ověřené weby, Firewall
   - **Soukromí:** Passwords, Antispam, Skartovač dat, Štít webové kamery
   - **Výkon:** Aktualizace aplikací
3. Klikněte na tlačítko komponenty
4. U komponenty, kterou chcete změnit, proveďte jeden z následujících kroků:
   - Chcete-li komponentu zapnout, přepněte příslušný posuvník do polohy **Zapnuto**.

- Chcete-li komponentu vypnout, přepněte příslušný posuvník do polohy **Vypnuto**.

5. V případě potřeby potvrďte volbu.

Instalace a odinstalace komponent

Většina funkcí aktivní ochrany je instalována s aplikací Small Office Protection. Přes nabídku Řešení problémů je ale můžete podle potřeby odinstalovat či znovu nainstalovat. Komponenty pro ochranu systému MacOS X nelze nainstalovat ani odinstalovat, ale můžete je vypnout.

1. Otevřete klienta Small Office Protection.
2. Přejděte do části **Menu ▸ Nastavení ▸ Obecné ▸ Řešení problémů**.
3. Klikněte na možnost **Přidat/změnit komponenty**.
4. U komponent, které chcete změnit, proveďte jeden z následujících kroků:
   - Pokud komponenta ještě není nainstalovaná, zaškrtněte její pole.
   - Pokud komponenta už je nainstalovaná, zrušte zaškrtnutí jejího pole.
5. Až změny dokončíte, potvrďte je kliknutím na tlačítko **Změnit**.

Podrobnosti o konfiguraci jednotlivých komponent, které jsou k dispozici v nastaveních Small Office Protection, najdete v článku Konfigurace nastavení ve Small Office Protection.

Konfigurace výjimek

Zástupné znaky

Řada štítů a dalších komponent v aplikaci Small Office Protection (včetně hlavní antivirové komponenty) vám umožňuje nastavovat výjimky či blokovat konkrétní cesty. Zástupné znaky vám pomohou, když neznáte přesnou cestu či název souboru, který chcete zahrnout nebo vyloučit. Také vám pomohou označit více souborů v jedné cestě. Některé cesty k souborům ale používání zástupných znaků neumožňují.

Znak	Význam
?	Nahrazuje jeden znak **Příklad:** `ab?.html` odpovídá souborům `abc.html`, `abd.html`, `abe.html` atd. a **neodpovídá** souboru `abc.htm`.

Znak	Význam
*	Nahrazuje nula nebo více znaků **Příklad:** `*mtl` odpovídá souborům `abc.html` a `d.html`. `*txt` odpovídá souborům `abc.txt`, `x.txt` a `xyztxt`.

Výjimky

Můžete nastavit výjimky, které budou uplatněny v jednotlivých štítech a komponentách Small Office Protection. Stačí na stránce **Nastavení** ▸ **Obecné** přejít na kartu *Výjimky*.

Přidávání výjimek

1. Otevřete klienta Small Office Protection.
2. Vpravo nahoře klikněte na **Menu** a poté na možnost **Nastavení**.
3. V části **Obecné** ▸ **Výjimky** klikněte na možnost **Přidat výjimku** a proveďte jeden z následujících úkonů:
   - Zadejte nebo najděte cestu k souboru, který chcete vyloučit.
   - Zadejte nebo najděte cestu ke složce, kterou chcete vyloučit.
   - Zadejte webovou adresu, kterou chcete vyloučit.
4. Až budete hotoví, klikněte na možnost **Přidat výjimku**.

Konfigurace automatických aktualizací

Na svých zařízeních můžete automaticky aktualizovat virové definice i verzi aplikace Small Office Protection, když jsou k dispozici nové aktualizace. Také můžete nastavit, aby byla zařízení aktualizována ručně. Další informace najdete v tématu Aktualizace Small Office Protection.

Konfigurace automatických aktualizací

1. Vpravo nahoře klikněte na **Menu**.
2. Klikněte na možnost **Nastavení**.
3. V části *Obecné* vyberte kartu **Aktualizace**.
4. U dvou tlačítek **Vyhledat aktualizace** klikněte na položku **Více možností**.
5. Vyberte možnost **Automatická aktualizace**.

Vytváření a konfigurace testů

Pracovní stanice s Windows

V nastaveních virových testů můžete nastavit typy souborů a programy, které má Small Office Protection testovat. Proto jsou hlavní nastavení testování konfigurována v nastaveních testů, zatímco výjimky jsou nastavovány v části Obecné.

Typy testů

- **Úplný virový test –** Provádí podrobný test systému, který kontroluje všechny pevné disky, rootkity a automaticky spouštěné programy.
- **Cílený test –** Otestuje pouze složky vybrané při zahájení testu.
- **Test z Průzkumníku –** Otestuje vybrané složky nebo jednotky, ale je k dispozici jen z kontextové nabídky Windows, když kliknete pravým tlačítkem na soubor, složku nebo jednotku.
- **Test po restartu (pouze MS Windows) –** Otestuje zařízení po spuštění.

Nastavení jednotlivých typů testů můžete otevřít tím, že kliknete na možnosti Menu ▸ Nastavení a pak přejdete na možnosti Ochrana ▸ Testy na viry.

Přizpůsobení úplných virových testů

Citlivost

V nastavení citlivosti testů můžete určit, jak mají být testy citlivé. Čím je citlivost vyšší, tím je ochrana lepší, ale také tím vyšší je možnost výskytu falešných poplachů na malware. Když citlivost snížíte, falešných poplachů bude méně, avšak účinnost testů bude nižší. Posuvník Citlivost testu lze nastavit do polohy střední, vysoké nebo nízké citlivosti.

Hledat potenciálně nežádoucí programy (PUP): umožňuje Avastu hledat programy, které jsou tajně stahovány s jinými programy a provádějí nežádoucí činnost.

Během testu následovat odkazy: umožňuje Avastu testovat také ostatní soubory používané testovanými soubory, jestli neobsahují potenciálně škodlivý obsah.

Testovat celé soubory (u velkých souborů velmi pomalé): umožňuje Avastu testovat celé soubory, nikoli pouze jejich části, jež jsou obvykle postiženy škodlivým kódem.

Priorita testu: určuje množství systémových prostředků, které smí Avast při testování používat. Vyšší priorita znamená rychlejší testování a zároveň může zpomalovat ostatní procesy na zařízení.

Testované oblasti

Výběrem příslušných polí můžete oblasti uvedené v seznamu zahrnout do testování. Hlavní možnosti oblastí jsou následující:

- **Všechny pevné disky:** umožňuje Avastu otestovat všechny pevné disky v počítači.
- **Systémová jednotka:** možnosti v této části se týkají dat uložených na fyzických zařízeních, jako jsou pevné disky nebo jednotky USB.

Při testování oblasti určené výše budou použity následující možnosti.

Všechna vyměnitelná média: umožňuje Avastu testovat aplikace, které se spouštějí automaticky, když k počítači připojíte jednotku USB nebo když do něj vložíte jiné výměnné médium.

Rootkity: umožňuje Avastu hledat hrozby ukryté v systému.

UEFI BIOS: umožňuje Avastu při spouštění počítače testovat hlavní firmwarová rozhraní.

Disky CD a DVD: umožňuje Avastu hledat škodlivý obsah na discích CD a DVD.

Moduly načtené v paměti: umožňuje Avastu testovat aplikace a procesy spouštěné po startu systému nebo běžící na pozadí.

Archivy

V části Archivy můžete určit typy komprimovaných souborů, které má Avast při testování rozbalovat.

- **Testovat jen běžné instalační programy:** testuje pouze obsah spustitelných souborů, které slouží k instalaci aplikací.
- **Testovat všechny archivy:** testuje veškerý obsah souborů archivů (testy kvůli tomu potrvají výrazně déle).
- **Netestovat archivy:** vypne testování archivů Avastem.

Typy souborů

Určete typy souborů, které při testování počítače na přítomnost malwaru mají být testovány přednostně:

- **Typy založené na obsahu (pomalé):** testuje soubory, které jsou obvykle nejzranitelnější vůči útokům malwaru.
- **Typy podle přípony (rychlé):** testuje pouze soubory s rizikovými příponami, jako jsou .exe, .com, .bat.
- **Testovat všechny soubory (velmi pomalé):** testuje všechny soubory v počítači na přítomnost malwaru.

Během testu provádět automatické akce: když povolíte tuto možnost, můžete určit automatickou akci při nálezu infikovaného souboru:

- **Automaticky vyčistit:** Avast se pokusí o opravu infikovaného souboru. Pokud se mu to nepovede, přesune soubor do Virové truhly. A pokud se mu ani to nepovede, soubor smaže.
- **Přesunout soubor do Virové truhly:** infikovaný soubor nebude automaticky opraven a místo toho bude přesunut do Virové truhly.
- **Smazat soubor:** Avast se infikovaný soubor nepokusí opravit ani přesunout do Virové truhly, ale automaticky jej smaže.

Po dokončení testu vypnout počítač: umožňuje Avastu po dokončení testu vypnout počítač.

Generovat report: umožňuje Avastu automaticky vytvářet a ukládat report. Umístění souboru reportu je uvedené pod touto možností.

Výjimky

Ačkoli se vylučování souborů či složek z testů nedoporučuje, můžete pro účely řešení problémů pro určité soubory či složky dočasně nastavit výjimky z testování. Ve spodní části stránky s nastaveními testů klikněte na možnost **Zobrazit výjimky**. Pak se řiďte pokyny v části **Konfigurace výjimek**.

Přizpůsobení cílených testů

Citlivost

V nastavení citlivosti testů můžete určit, jak mají být testy citlivé. Čím je citlivost vyšší, tím je ochrana lepší, ale také tím vyšší je možnost výskytu falešných poplachů na

malware. Když citlivost snížíte, falešných poplachů bude méně, avšak účinnost testů bude nižší. Posuvník Citlivost testu lze nastavit do polohy střední, vysoké nebo nízké citlivosti.

Hledat potenciálně nežádoucí programy (PUP): umožňuje Avastu hledat programy, které jsou tajně stahovány s jinými programy a provádějí nežádoucí činnost.

Během testu následovat odkazy: umožňuje Avastu testovat také ostatní soubory používané testovanými soubory, jestli neobsahují potenciálně škodlivý obsah.

Testovat celé soubory (u velkých souborů velmi pomalé): umožňuje Avastu testovat celé soubory, nikoli pouze jejich části, jež jsou obvykle postiženy škodlivým kódem.

Priorita testu: určuje množství systémových prostředků, které smí Avast při testování používat. Vyšší priorita znamená rychlejší testování a zároveň může zpomalovat ostatní procesy na zařízení.

Archivy

V části Archivy můžete určit typy komprimovaných souborů, které má Avast při testování rozbalovat.

- **Testovat jen běžné instalační programy:** testuje pouze obsah spustitelných souborů, které slouží k instalaci aplikací.
- **Testovat všechny archivy:** testuje veškerý obsah souborů archivů (testy kvůli tomu potrvají výrazně déle).
- **Netestovat archivy:** vypne testování archivů Avastem.

Typy souborů

Určete typy souborů, které při testování počítače na přítomnost malwaru mají být testovány přednostně:

- **Typy založené na obsahu (pomalé):** testuje soubory, které jsou obvykle nejzranitelnější vůči útokům malwaru.
- **Typy podle přípony (rychlé):** testuje pouze soubory s rizikovými příponami, jako jsou .exe, .com, .bat.
- **Testovat všechny soubory (velmi pomalé):** testuje všechny soubory v počítači na přítomnost malwaru.

Během testu provádět automatické akce: když povolíte tuto možnost, můžete určit automatickou akci při nálezu infikovaného souboru:

- **Automaticky vyčistit:** Avast se pokusí o opravu infikovaného souboru. Pokud se mu to nepovede, přesune soubor do Virové truhly. A pokud se mu ani to nepovede, soubor smaže.
- **Přesunout soubor do Virové truhly:** infikovaný soubor nebude automaticky opraven a místo toho bude přesunut do Virové truhly.
- **Smazat soubor:** Avast se infikovaný soubor nepokusí opravit ani přesunout do Virové truhly, ale automaticky jej smaže.

Po dokončení testu vypnout počítač: umožňuje Avastu po dokončení testu vypnout počítač.

Generovat report: umožňuje Avastu automaticky vytvářet a ukládat report. Umístění souboru reportu je uvedené pod touto možností.

Přizpůsobení testů z Průzkumníku

Citlivost

V nastavení citlivosti testů můžete určit, jak mají být testy citlivé. Čím je citlivost vyšší, tím je ochrana lepší, ale také tím vyšší je možnost výskytu falešných poplachů na malware. Když citlivost snížíte, falešných poplachů bude méně, avšak účinnost testů bude nižší. Posuvník Citlivost testu lze nastavit do polohy střední, vysoké nebo nízké citlivosti.

Hledat potenciálně nežádoucí programy (PUP): umožňuje Avastu hledat programy, které jsou tajně stahovány s jinými programy a provádějí nežádoucí činnost.

Během testu následovat odkazy: umožňuje Avastu testovat také ostatní soubory používané testovanými soubory, jestli neobsahují potenciálně škodlivý obsah.

Testovat celé soubory (u velkých souborů velmi pomalé): umožňuje Avastu testovat celé soubory, nikoli pouze jejich části, jež jsou obvykle postiženy škodlivým kódem.

Priorita testu: určuje množství systémových prostředků, které smí Avast při testování používat. Vyšší priorita znamená rychlejší testování a zároveň může zpomalovat ostatní procesy na zařízení.

Archivy

V části Archivy můžete určit typy komprimovaných souborů, které má Avast při testování rozbalovat.

- **Testovat jen běžné instalační programy:** testuje pouze obsah spustitelných souborů, které slouží k instalaci aplikací.
- **Testovat všechny archivy:** testuje veškerý obsah souborů archivů (testy kvůli tomu potrvají výrazně déle).
- **Netestovat archivy:** vypne testování archivů Avastem.

Typy souborů

Určete typy souborů, které při testování počítače na přítomnost malwaru mají být testovány přednostně:

- **Typy založené na obsahu (pomalé):** testuje soubory, které jsou obvykle nejzranitelnější vůči útokům malwaru.
- **Typy podle přípony (rychlé):** testuje pouze soubory s rizikovými příponami, jako jsou .exe, .com, .bat.
- **Testovat všechny soubory (velmi pomalé):** testuje všechny soubory v počítači na přítomnost malwaru.

Během testu provádět automatické akce: když povolíte tuto možnost, můžete určit automatickou akci při nálezu infikovaného souboru:

- **Automaticky vyčistit:** Avast se pokusí o opravu infikovaného souboru. Pokud se mu to nepovede, přesune soubor do Virové truhly. A pokud se mu ani to nepovede, soubor smaže.
- **Přesunout soubor do Virové truhly:** infikovaný soubor nebude automaticky opraven a místo toho bude přesunut do Virové truhly.
- **Smazat soubor:** Avast se infikovaný soubor nepokusí opravit ani přesunout do Virové truhly, ale automaticky jej smaže.

Po dokončení testu vypnout počítač: umožňuje Avastu po dokončení testu vypnout počítač.

Generovat report: umožňuje Avastu automaticky vytvářet a ukládat report. Umístění souboru reportu je uvedené pod touto možností.

Přizpůsobení testů po restartu

Citlivost

V nastavení citlivosti testů můžete určit, jak mají být testy citlivé. Čím je citlivost vyšší, tím je ochrana lepší, ale také tím vyšší je možnost výskytu falešných poplachů na

malware. Když citlivost snížíte, falešných poplachů bude méně, avšak účinnost testů bude nižší. Posuvník Citlivost testu lze nastavit do polohy střední, vysoké nebo nízké citlivosti.

Hledat potenciálně nežádoucí programy (PUP): umožňuje Avastu hledat programy, které jsou tajně stahovány s jinými programy a provádějí nežádoucí činnost.

Rozbalovat archivy: umožňuje Avastu rozbalovat soubory a složky v archivech, aby je bylo možné otestovat.

Testované oblasti

Výběrem příslušných polí můžete oblasti uvedené v seznamu zahrnout do testování. Hlavní možnosti oblastí jsou následující:

- **Všechny pevné disky:** umožňuje Avastu otestovat všechny pevné disky v počítači.
- **Systémová jednotka:** možnosti v této části se týkají dat uložených na fyzických zařízeních, jako jsou pevné disky nebo jednotky USB.

Při testování oblasti určené výše budou použity následující možnosti.

Automaticky spouštěné programy: umožňuje Avastu kontrolovat všechny automaticky spouštěné programy.

Během testu provádět automatické akce: když povolíte tuto možnost, můžete určit automatickou akci při nálezu infikovaného souboru:

- **Automaticky vyčistit:** Avast se pokusí o opravu infikovaného souboru. Pokud se mu to nepovede, přesune soubor do Virové truhly. A pokud se mu ani to nepovede, soubor smaže.
- **Přesunout soubor do Virové truhly:** infikovaný soubor nebude automaticky opraven a místo toho bude přesunut do Virové truhly.
- **Smazat soubor:** Avast se infikovaný soubor nepokusí opravit ani přesunout do Virové truhly, ale automaticky jej smaže.

Zařízení s Androidem

Pomocí možnosti Otestovat lze otestovat všechny aplikace nainstalované v zařízení a zjistit tamní bezpečnostní rizika způsobená změnami ve výchozích nastaveních Androidu. Virové definice používané testem jsou automaticky aktualizovány.

1. Otevřete aplikaci *Avast Mobile Security* klepnutím na její ikonu na zařízení.
2. Na hlavní obrazovce aplikace klepněte na možnost **Otestovat**.

Aplikace po dokončení testu buď zobrazí zprávu, že je vše v pořádku, nebo zobrazí seznam nalezených problémů společně s možnostmi jejich vyřešení. Pokud jsou takové možnosti k dispozici, můžete klepnout na tlačítko **Vyřešit** nebo **Povolit**.

Test interní paměti

Ve výchozím stavu je test interní paměti vypnutý. Pokud chcete testovat i interní úložiště zařízení, můžete toto testování zapnout v části Nastavení.

1. Otevřete aplikaci *Avast Mobile Security* klepnutím na její ikonu na zařízení.
2. Klepněte na možnosti **Menu** ▸ **Nastavení**.
3. Klepněte na možnost **Ochrana**.
4. Klepnutím na posuvník povolte *Testování interního úložiště*.

Zařízení s iOS

Pomocí možnosti Otestovat lze otestovat všechny aplikace nainstalované v zařízení a zjistit tamní bezpečnostní rizika způsobená změnami ve výchozích nastaveních iOS. Virové definice používané testem jsou automaticky aktualizovány.

1. Otevřete aplikaci *Avast Security & Privacy* klepnutím na její ikonu na zařízení.
2. Na hlavní obrazovce aplikace klepněte na možnost **Otestovat**.

Aplikace po dokončení testu buď zobrazí zprávu, že je vše v pořádku, nebo zobrazí seznam nalezených problémů společně s možnostmi jejich vyřešení. Pokud jsou takové možnosti k dispozici, můžete klepnout na tlačítko **Vyřešit** nebo **Povolit**.

Small Office Protection nabízí spoustu dalších funkcí a možností. Další informace najdete v naší znalostní databázi na https://businesshelp.avast.com/.