Bitdefender INTERNET SECURITY

UŽIVATELSKÁ PŘÍRUČKA

Bitdefender Internet Security
Uživatelská příručka

Datum vydání 20. července 2020

Právní oznámení

Bitdefender

Obsah

INSTALACE

1. PŘÍPRAVA NA INSTALACI

Před instalací produktu Bitdefender Internet Security proveďte následující přípravy, abyste zajistili hladký průběh instalace:

- Ujistěte se, že zařízení, do kterého chcete instalovat Bitdefender, splňuje systémové požadavky. Pokud zařízení nesplňuje všechny systémové požadavky, Bitdefender nebude nainstalován nebo, pokud je nainstalován, nebude správně fungovat a způsobí zpomalení systému a nestabilitu. Úplný seznam požadavků na systém najdete zde *„Požadavky na systém“* (str. 3).
- Přihlaste se k zařízení pomocí účtu správce.
- Odstraňte ze zařízení veškerý podobný software. Pokud bude jakákoli podobná aplikace zaznamenána během instalačního procesu Bitdefender, budete upozorněni na nutnost odinstalace. Současný běh dvou zabezpečovacích aplikací může ovlivnit jejich provoz a způsobit zásadní problémy se systémem. Nástroj Windows Defender bude během instalace vypnutý.
- Vypněte nebo odeberte jakýkoli program brány firewall, který může být na zařízení spuštěn. Současný provoz dvou firewallových programů může ovlivnit jejich činnost a způsobit zásadní problémy se systémem. Brána firewall systému Windows bude během instalace vypnutá.
- Během instalace se doporučuje připojit zařízení k internetu, i když instalujete z CD/DVD. Pokud jsou k dispozici novější verze aplikačních souborů obsažených v instalačním balíčku, produkt Bitdefender je může stáhnout a nainstalovat.

2. POŽADAVKY NA SYSTÉM

Bitdefender Internet Security můžete nainstalovat pouze na zařízení, která používají následující operační systémy:

- Windows 7 s aktualizací Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

- 2,5 GB volného místa na pevném disku (nejméně 800 MB na systémové jednotce)
- 2 GB paměti (RAM)

Důležité
Výkon zařízení může být ovlivněn na zařízeních, která mají CPU staré generace.

Poznámka
Chcete-li zjistit operační systém Windows, ve kterém je zařízení spuštěno, a informace o hardwaru:

- V systému **Windows 7** klikněte pravým tlačítkem na ikonu **Počítač** na ploše a poté v nabídce vyberte položku **Vlastnosti**.
- V systémech **Windows 8** na úvodní obrazovce vyhledejte položku **Počítač** (například můžete začít psát „Počítač“, přímo na úvodní obrazovce) a poté klikněte pravým tlačítkem na její ikonu. Ve **Windows 8.1**, nalezněte **Tento Počítač**.

  Dole v nabídce vyberte položku **Vlastnosti**. V oblasti **Systém** vyhledejte informace o typu systému počítače.
- V systému **Windows 10** zadejte „**Systém**“ do vyhledávacího pole na hlavním panelu a klikněte na nalezenou ikonu. V oblasti **Systém** vyhledejte informace o typu systému počítače.

2.1. Softwarové požadavky

Aby bylo možné zařízení Bitdefender a všechny jeho funkce používat, musí splňovat následující softwarové požadavky:

- Microsoft Edge verze 40 a vyšší
- Internet Explorer 10 a vyšší
- Mozilla Firefox verze 51 a vyšší

- Google Chrome verze 34 a vyšší
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 nebo vyšší

3. INSTALACE PRODUKTU BITDEFENDER

Bitdefender můžete nainstalovat z instalačního disku nebo pomocí webového instalátoru staženého na vaše zařízení z Bitdefender Central .

Pokud váš nákup zahrnuje více než jedno zařízení (například jste zakoupili produkt Bitdefender Internet Security pro 3 počítače), opakujte proces instalace a aktivujte svůj produkt se stejným účtem na každém zařízení. Účet, který je třeba použít, je tentýž, který obsahuje vaše aktivní předplatné produktu Bitdefender.

3.1. Instaluj z Bitdefender Central

Z účtu Bitdefender Central můžete stáhnout instalační sadu odpovídající zakoupenému předplatnému. Po dokončení instalace bude produkt Bitdefender Internet Security aktivován.

Pro stáhnutí Bitdefender Internet Security z Bitdefender Central:

1. Přihlaš se na Bitdefender Central.
2. Vyberte menu **Moje Zařízení** a klikněte na **INSTALOVAT OCHRANU**.
3. Prosím vyberte jednu z následujících variant
   - **Chránit toto zařízení**
     a. Vyberte tuto možnost a vyberte vlastníka zařízení. Pokud zařízení patří někomu jinému, klepněte na odpovídající tlačítko.
     b. Uložte instalační soubor.
   - **Chránit další zařízení**
     a. Vyberte tuto možnost a vyberte vlastníka zařízení. Pokud zařízení patří někomu jinému, klepněte na odpovídající tlačítko.
     b. Klikněte na **ODESLAT ODKAZ NA STAŽENÍ**.
     c. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**.

        Pamatujte, že vygenerovaný odkaz ke stažení je platný pouze 24 hodin. Pokud doba platnosti odkazu vyprší, musíte vygenerovat nový pomocí stejných kroků.

d. Na zařízení, kde chcete nainstalovat váš Bitdefender produkt Bitdefender, zkontrolujte emailový účet, který jste zadali a poté klikněte na příslušné tlačítko stáhnout

4. Počkejte na dokončení stahování a poté spusťte instalační soubor.

Ověření instalace

Bitdefender nejprve zkontroluje systém z důvodu ověření instalace.

Pokud systém nesplňuje minimální požadavky na instalaci Bitdefender, budete informováni o oblastech, které je třeba vylepšit, abyste mohli pokračovat.

Jestliže bude nalezen nekompatibilní antivirový program nebo starší verze produktu Bitdefender, budete vyzváni k jejich odebrání ze systému. Podle pokynů proveďte odebrání softwaru ze systému, abyste předešli pozdějším problémům. Možná budete muset restartovat zařízení, abyste dokončili odebrání detekovaných bezpečnostních řešení.

Instalační balíček produktu Bitdefender Internet Security je neustále aktualizován.

Poznámka
Stažení instalačních souborů může trvat dlouho, zejména v případě pomalejšího připojení k internetu.

Po ověření instalace se zobrazí průvodce instalací. Při instalaci produktu Bitdefender Internet Security postupujte podle pokynů.

1. krok - instalace produktu Bitdefender

Předtím než přejdete k instalaci, musíte souhlasit s Podmínkami Předplatného. Přečtěte si, prosím, smlouvu o předplatném, neboť obsahuje smluvní podmínky, podle kterých můžete použít Bitdefender Internet Security.

Pokud s těmito podmínkami nesouhlasíte, zavřete toto okno. Instalační proces bude přerušen a instalace se ukončí.

V tomto kroku lze provést dva další úkony:

- Nechte povolenou možnost **Send product reports**. Při povolení této možnosti budou zprávy obsahující informace o používání produktu odesílány na servery produktu Bitdefender. Tyto informace jsou nezbytné pro zlepšování produktu a mohou nám pomoci poskytovat v budoucnosti

lepší komfort. Tyto zprávy neobsahují žádná důvěrná data, jako vaše jméno nebo IP adresa, a nebudou použity ke komerčním účelům.

- Nastavte jazyk, ve kterém chcete nainstalovat program.

Klikněte na **INSTALOVAT** pro spuštění instalace produktu Bitdefender.

2. krok - průběh instalace

Počkejte na dokončení instalace. Zobrazují se podrobné informace o průběhu.

3. krok - dokončení instalace

Produkt Bitdefender je úspěšně nainstalován.

Zobrazí se shrnutí instalace. Pokud byla během instalace nalezena a odstraněna aktivní hrozba, může být nutný restart systému.

Krok 4 - Analýza zařízení

Nyní budete dotázáni, zda si přejete provést analýzu vašeho zařízení, abyste se ujistili, že je bezpečné. Během tohoto kroku bude Bitdefender prověřovat kritické systémové oblasti. Spusťte jej kliknutím na **Spustit analýzu zařízení** .

Rozhraní skenování můžete skrýt kliknutím na **Spustit skenování na pozadí** . Poté vyberte, zda chcete být informováni o dokončení skenování nebo ne.

Po dokončení skenování klikněte na **Otevřít rozhraní Bitdefenderu** .

Poznámka
Pokud nechcete provést skenování, můžete jednoduše kliknout na **Přeskočit** .

5. krok - začínáme

V okně **Začínáme** se zobrazují detaily o Vašem aktivním předplatném.

Klikněte na tlačítko **Dokončit** a přejdete do rozhraní produktu Bitdefender Internet Security.

3.2. Instalace z instalačního disku

Pokud chcete produkt Bitdefender nainstalovat z instalačního disku, vložte disk do optické jednotky.

Po krátké chvíli by se měla zobrazit instalační obrazovka. Zahajte instalaci podle pokynů.

Pokud se instalační obrazovka neobjeví, pomocí nástroje Průzkumník Windows přejděte do kořenového adresáře disku a dvakrát klikněte na soubor autorun.exe.

Klikněte na tlačítko **Instaluj z CD/DVD** pokud je vaše internetové spojení pomalé, nebo není systém připojen k internetu. V tomto případě Bitdefender dostupný na disku bude nainstalován a novější verze bude stažena z Bitdefender serverů přes produktový update.

Ověření instalace

Bitdefender nejprve zkontroluje systém z důvodu ověření instalace.

Pokud systém nesplňuje minimální požadavky na instalaci Bitdefender, budete informováni o oblastech, které je třeba vylepšit, abyste mohli pokračovat.

Jestliže bude nalezen nekompatibilní antivirový program nebo starší verze produktu Bitdefender, budete vyzváni k jejich odebrání ze systému. Podle pokynů proveďte odebrání softwaru ze systému, abyste předešli pozdějším problémům. Možná budete muset restartovat zařízení, abyste dokončili odebrání detekovaných bezpečnostních řešení.

Poznámka

Stažení instalačních souborů může trvat dlouho, zejména v případě pomalejšího připojení k internetu.

Po ověření instalace se zobrazí průvodce instalací. Při instalaci produktu Bitdefender Internet Security postupujte podle pokynů.

1. krok - instalace produktu Bitdefender

Předtím než přejdete k instalaci, musíte souhlasit s Podmínkami Předplatného. Přečtěte si, prosím, smlouvu o předplatném, neboť obsahuje smluvní podmínky, podle kterých můžete použít Bitdefender Internet Security.

Pokud s těmito podmínkami nesouhlasíte, zavřete toto okno. Instalační proces bude přerušen a instalace se ukončí.

V tomto kroku lze provést dva další úkony:

- Nechte povolenou možnost **Send product reports**. Při povolení této možnosti budou zprávy obsahující informace o používání produktu odesílány na servery produktu Bitdefender. Tyto informace jsou nezbytné pro zlepšování produktu a mohou nám pomoci poskytovat v budoucnosti lepší komfort. Tyto zprávy neobsahují žádná důvěrná data, jako vaše jméno nebo IP adresa, a nebudou použity ke komerčním účelům.
- Nastavte jazyk, ve kterém chcete nainstalovat program.

Klikněte na **INSTALOVAT** pro spuštění instalace produktu Bitdefender.

2. krok - průběh instalace

Počkejte na dokončení instalace. Zobrazují se podrobné informace o průběhu.

3. krok - dokončení instalace

Zobrazí se shrnutí instalace. Pokud byla během instalace nalezena a odstraněna aktivní hrozba, může být nutný restart systému.

Krok 4 - Analýza zařízení

Nyní budete dotázáni, zda si přejete provést analýzu vašeho zařízení, abyste se ujistili, že je bezpečné. Během tohoto kroku bude Bitdefender prověřovat kritické systémové oblasti. Spusťte jej kliknutím na **Spustit analýzu zařízení** .

Rozhraní skenování můžete skrýt kliknutím na **Spustit skenování na pozadí** . Poté vyberte, zda chcete být informováni o dokončení skenování nebo ne.

Po dokončení skenování klikněte na **Pokračovat s vytvořením účtu** .

Poznámka

Pokud nechcete provést skenování, můžete jednoduše kliknout na **Přeskočit** .

Krok 5 - Bitdefender účet

Po dokončení počátečního nastavení se zobrazí okno účtu Bitdefender. Účet Bitdefender je vyžadován k aktivaci produktu a použití jeho online funkcí. Další informace viz *„Bitdefender Central“* (str. 30).

Pokračuje dle příslušné situace.

- **Chci vytvořit účet Bitdefender**

1. Zadejte požadované informace do příslušných polí. Data, která zde uvedete, zůstanou utajená. Heslo musí mít délku nejméně 8 znaků, musí obsahovat alespoň jedno číslo nebo symbol a musí obsahovat malá a velká písmena.
2. Než budete postupovat dále, musíte souhlasit s Podmínkami použití. Přečtěte si Smluvní podmínky pečlivě, protože obsahují podmínky, za kterých můžete používat Bitdefender.

   Dále si můžete přečíst zásady ochrany osobních údajů.
3. Klikněte na **VYTVOŘIT ÚČET** .

> **Poznámka**
> Jakmile je účet vytvořen, můžete se pomocí e-mailové adresy zadané při registraci a hesla přihlásit k účtu na adrese https://central.bitdefender.com nebo v aplikaci Bitdefender Central za předpokladu, že je nainstalován na jednom z vašich zařízení Android nebo iOS zařízení. Chcete-li nainstalovat aplikaci Bitdefender Central v zařízení s Androidem, musíte mít přístup k službě Google Play, vyhledat Bitdefender Central a potom zvolit odpovídající možnost instalace. Chcete-li nainstalovat aplikaci Bitdefender Central v systému iOS, musíte se dostat do aplikace App Store, vyhledat Bitdefender Central a potom zvolit odpovídající možnost instalace.

- **Již mám účet Bitdefender**

1. Klikněte na **Přihlásit se**.
2. Zadejte svou emailovou adresu do příslušného pole a klikněte na tlačítko **Další**.
3. Zadejte heslo a poté klikněte na tlačítko **PŘIHLÁSIT SE**.

   Pokud jste zapomněli heslo, které jste si nastavili nebo ho chcete pouze resetovat:

   a. Klikněte na tlačítko **Zapomenuté heslo**.

   b. Zadejte svou emailovou adresu, poté klikněte na **DALŠÍ**.

   c. Zkontrolujte svůj e-mailový účet, zadejte bezpečnostní kód, který jste obdrželi a klepněte na tlačítko **DALŠÍ**.

      Můžete také kliknout na **Změnit heslo** v e-mailu, který jsme vám poslali.

d. Napište nové heslo a poté ho napište ještě jednou Klikněte na tlačítko **Save**.

> **Poznámka**
> Pokud máte již MyBitdefender účet, můžete ho nadále používat pro přihlašování do Bitdefender účtu. Jestliže jste zapomněli heslo, musíte jít na https://my.bitdefender.com pro jeho obnovení. Poté použijte aktualizované údaje pro přihlášení do Bitdefender účtu.

- **Chci se přihlásit pomocí svého účtu Microsoft, Facebook nebo Google**

  Pro přihlášení pomocí svého účtu Microsoft, Facebook nebo Google:

  1. Vyberte službu, kterou chcete použít. Budete přesměrováni na přihlašovací stránku příslušné služby.
  2. Podle pokynů poskytnutých vybranou službou propojte svůj účet s produktem Bitdefender.

> **Poznámka**
> Produkt Bitdefender nepřistupuje k žádným důvěrným informacím, jako je heslo účtu, který používáte k přihlášení, ani osobní údaje o vašich přátelích a kontaktech.

Krok 6 - Aktivovat váš produkt

> **Poznámka**
> Tento krok se objeví, pokud jste vybrali vytvoření nového Bitdefender účtu během předešlého kroku, nebo pokud jste přihlášeni na účet, kde předplatné již vypršelo.

Je nutné mít aktivní internetové připojení pro kompletní aktivaci produktu.

Pokračuje dle příslušné situace:

- Mám aktivační kód

  V tomto případě, aktivujte produkt dle následujících pokynů:

  1. Zadejte aktivační kód do pole **Mám aktivační kód** a poté klikněte na **POKRAČOVAT**.

> **Poznámka**
> Můžete najít váš aktivační kód:

- na obalu CD/DVD.
- na registrační kartě produktu.
- v emailu doručeném po nákupu.

2. **Chci ohodnotit produkt Bitdefender**

   V tomto případě můžete využít 30-denní zkušební doby. Pro začátek trialu vyberte **Nemám předplatné, chci testovat produkt zdarma**, a poté klikněte na **POKRAČOVAT**.

7. krok - začínáme

V okně **Začínáme** se zobrazují detaily o Vašem aktivním předplatném.

Klikněte na tlačítko **Dokončit** a přejdete do rozhraní produktu Bitdefender Internet Security.

ZAČÍNÁME

4. ZÁKLADY

Po instalaci produktu Bitdefender Internet Security je vaše zařízení chráněno před všemi druhy hrozeb (jako je malware, spyware, ransomware, exploity, botnety a trojské koně) a internetovými hrozbami (například hackery, Phishing a spam).

Aplikace používá technologii Photon ke zvýšení rychlosti a výkonu průběhu skenování na přítomnost hrozeb. Ta funguje tím způsobem, že se učí návykům používání vašich systémových aplikací, a tím určuje, co a kdy má skenovat, aby byl dopad na výkon systému minimální.

Nechráněné připojení se k veřejným nezabezpečeným sítím na letištích, v obchodech, kavárnách nebo hotelech může ohrozit vaše zařízení a data. Hlavně proto, že podvodníci mohou sledovat vaši činnost a vysledovat tu nejlepší příležitost ke krádeži vašich osobních údajů, ale také proto, že každý může vidět vaši IP adresu; což činí z vašeho zařízení možnou oběť budoucích kyberútoků. Abyste takovým nešťastným situacím zabránili, nainstalujte a používejte aplikaci *„VPN“* (str. 145).

Můžete mít přehled o svých heslech a online uživatelských účtech tak, že je uložíte *„Ochrana vašich osobních dat správcem hesel“* (str. 135) do peněženky. Používáním jediného hlavního hesla máte možnost chránit své soukromí před vetřelci, kteří by se mohli pokusit Vás okrást o peníze.

„Ochrana webových kamer“ (str. 128)zabraňuje nedůvěryhodným aplikacím v přístupu k Vaší videokameře, tudíž brání všem hackerským útokům. Dle rozhodnutí uživatele produktu Bitdefender bude přístup oblíbených aplikací k Vaší webkameře buď povolen, nebo zakázán.

Aby jste byli chráněni proti případným špionům a slídilům, když je Vaše zařízení připojeno k nezabezpečené bezdrátové síti, Bitdefender analyzuje její úroveň zabezpečení a v případě potřeby, navrhne doporučené možnosti pro zvýšení bezpečnosti Vašich online aktivit. Pro pokyny, jak udržet svá soukromá data v bezpečí, se prosím odkažte na *„Wi-Fi Bezpečnostní Poradce“* (str. 124).

Soubory zašifrované ransomwarem můžeme teď obnovit bez nutnosti zaplatit výkupné. Pro informace jak obnovit zašifrované soubory se obraťte na *„Zotavení po infekci Ransomware“* (str. 132).

Když pracujete, hrajete hry nebo sledujete filmy, produkt Bitdefender vám může nabídnout nepřerušovaný uživatelský komfort tím, že odkládá úlohy

údržby, zabraňuje přerušení a upravuje vizuální efekty systému. Všech těchto možností a jejich výhod můžete využít aktivací a konfigurací *„Profily“* (str. 168).

Produkt Bitdefender bude činit většinu rozhodnutí souvisejících se zabezpečením za vás a vyskakovací upozornění bude zobrazovat jen zřídka. Detaily ohledně provedených akcích a informace o operacích programu jsou dostupné v okně Událostí. Další informace viz *„Upozornění“* (str. 16).

Čas od času je třeba otevřít Bitdefender a vyřešit jakékoliv existující problémy. Možná budete muset nakonfigurovat konkrétní součásti Bitdefender nebo podniknout preventivní kroky k ochraně zařízení a vašich dat.

Pokud chcete používat online funkce produktu Bitdefender Internet Security a spravovat předplatná a zařízení, přejděte do vašeho účtu Bitdefender. Další informace viz *„Bitdefender Central“* (str. 30).

V části „Doporučené postupy“ (str. 43) najdete postupy k provádění běžných úkonů. Pokud se během používání produktu Bitdefender setkáte s problémy, nahlédněte do části *„Řešení běžných problémů“* (str. 177), kde můžete najít případná řešení nejčastějších problémů.

4.1. Otevření okna produktu Bitdefender

Chcete-li získat přístup k hlavnímu rozhraní produktu Bitdefender Internet Security, klikněte na ploše na ikonu .

V případě potřeby můžete také postupovat podle následujících kroků:

- V systému **Windows 7**:
  1. Klikněte na nabídku **Start** a přejděte do nabídky **Všechny programy**.
  2. Klikněte na položku **Bitdefender**.
  3. Klikněte na položku **Bitdefender Internet Security** nebo použijte rychlejší postup a dvakrát klikněte na ikonu Bitdefender v oznamovací oblasti.
- V systémech **Windows 8 a Windows 8.1**:

  Na úvodní obrazovce systému Windows najděte položku Bitdefender (můžete například začít psát "Bitdefender" přímo na úvodní obrazovce) a poté klikněte na její ikonu. Alternativně otevřete aplikaci pro pracovní plochu a poté dvakrát klikněte na ikonu Bitdefender v oznamovací oblasti.
- V systému **Windows 10**:

Do vyhledávacího pole na hlavním panelu zadejte "Bitdefender" a poté klikněte na příslušnou ikonu. Alternativně dvakrát klikněte na ikonu Bitdefender v oznamovací oblasti.

Další informace o okně produktu Bitdefender a ikoně v oznamovací oblasti najdete zde *„Rozhraní produktu Bitdefender“* (str. 20).

4.2. Upozornění

Bitdefender uchovává podrobný protokol událostí týkajících se jeho činnosti ve vašem zařízení. Kdykoli nastane důležitá událost související se zabezpečením vašeho systému, do událostí produktu Bitdefender se přidá nová zpráva podobně, jako když se v přijaté poště objeví nový email.

Události představují velmi důležitý nástroj pro sledování a správu ochrany produktu Bitdefender. Můžete například snadno zkontrolovat, zda byla aktualizace úspěšně provedena, zda byly v zařízení nalezeny hrozby nebo zranitelnosti atd. Dále můžete v případě potřeby učinit další opatření nebo změnit opatření prováděná produktem Bitdefender.

Chcete-li získat přístup k protokolu o oznámení, klikněte na**Notifications** na navigačním panelu na Bitdefender rozhraní. Kdykoliv se objeví kritická událost, na ikoně se zobrazí počítadlo.

V závislosti na závažnosti, události jsou seskupeny v:

- **Kritické** události označují kritické problémy. Měli byste je ihned prověřit.
- **Výstražné** události označují nekritické problémy. Až budete mít čas, měli byste je zkontrolovat a odstranit.
- **Informační** události označují úspěšné činnosti.

Klikněte na každý panel pro zobrazení detailů o generovaných událostech. Stručné informace jsou zobrazeny po jediném kliknutí na každý titulek, jmenovitě: krátký popis; akce, kterou Bitdefender provedl; a datum a čas provedení. K dispozici mohou být možnosti k provedení další činnosti v případě potřeby.

Abyste mohli snáze spravovat zaprotokolované události, každá část okna Události nabízí možnosti k odstranění nebo označení všech událostí v dané části jako přečtené.

4.3. Profily

Některé počítačové aktivity, jako online hry nebo video prezentace, vyžadují rychlejší odezvu systému, vysoký výkon a žádné rušení. Pokud váš notebook běží na baterie, je nejlepší odložit nedůležité operace, které spotřebovávají další energii, na dobu, kdy znovu připojíte napájení.

Profily produktu Bitdefender přidělují více systémových prostředků spuštěným aplikacím tím, že dočasně mění nastavení ochrany a upravují konfiguraci systému. Tím se minimalizuje dopad systému na vaši činnost.

Produkt Bitdefender je vybaven následujícími profily, které umožňují přizpůsobit se různým činnostem:

Pracovní profil
: Optimalizuje efektivitu vaší práce tím, že identifikuje a upravuje nastavení produktu a systému.

Filmový profil
: Vylepšuje vizuální efekty a eliminuje rušení během sledování filmů.

Herní profil
: Vylepšuje vizuální efekty a eliminuje rušení během hraní her.

Profil Veřejná Wi-Fi
: Aplikuje nastavení produktu pro využití maximální ochrany, zatímco jste připojeni na nezabezpečenou wi-fi.

Profil režimu baterie
: Aplikuje nastavení produktu a pozdrží aktivitu v pozadí pro úsporu baterie.

4.3.1. Nastavte automatickou aktivaci profilů

Pro usnadnění ovládání můžete nakonfigurovat Bitdefender, aby spravoval váš pracovní profil. V tomto režimu Bitdefender automaticky detekuje činnost, kterou provádíte, a aplikuje nastavení pro optimalizaci systému a produktu.

Při prvním přístupu k **Profily** budete vyzváni k aktivaci automatických profilů. Stačí kliknout na **ZAPNOUT** v zobrazeném okně.

Chcete-li funkci zapnout později, můžete kliknout na **NE TEĎ** .

Povolení automatické aktivace profilů Bitdefender:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. Na kartě **Profily** klikněte na **Nastavení** .

3. Klikněte na příslušný přepínač pro zapnutí **Automatické aktivace profilů**.

Pokud nechcete, aby byly profily automaticky aktivované, vypněte přepínač.

Pro ruční aktivaci profilu klikněte na odpovídající přepínač. Z prvních tří profilů lze ručně aktivovat pouze jeden.

Pro více informací o Profilech, obraťte se na„*Profily*“ (str. 168)

4.4. Ochrana nastavení produktu Bitdefender heslem

Pokud nejste jediným uživatelem s právy správce pomocí tohoto zařízení, doporučujeme vám chránit nastavení Bitdefender heslem.

Nastavit ochranu heslem pro Bitdefender nastavení:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. V okně **Obecné** zapněte **Zabezpečení heslem**.
3. Zadejte heslo do dvou zobrazených polí a poté klikněte na tlačítko **OK**. Heslo musí být dlouhé alespoň 8 znaků.

Po nastavení hesla musí každý, kdo chce změnit nastavení produktu Bitdefender, nejprve zadat heslo.

Důležité

Heslo si zapamatujte nebo si záznam o něm uschovejte na bezpečném místě. Pokud heslo zapomenete, bude nutné program přeinstalovat nebo kontaktovat podporu produktu Bitdefender.

Pro odstranění ochrany heslem:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. V okně **Obecné** vypněte **Zabezpečení heslem**.
3. Zadejte heslo a poté klikněte na tlačítko **OK**.

Poznámka

Pokud chcete změnit heslo pro váš produkt, klikněte na odkaz **Změna hesla**. Zadejte své současné heslo a poté klikněte na **OK**. V novém okně, které se objeví, zadejte nové heslo, které si odteď přejete využívat k omezení přístupu k Vašemu Bitdefender nastavení.

4.5. Produktová hlášení

Přehledy produktů obsahují informace o tom, jak používat produkt Bitdefender, který jste nainstalovali. Tyto informace jsou nezbytné pro zlepšování produktu a mohou nám pomoci poskytovat vám v budoucnosti lepší komfort.

Upozorňujeme, že tyto přehledy neobsahují žádné důvěrné údaje, jako je vaše jméno nebo IP adresa, a že nebudou použity k obchodním účelům.

Pokud jste během procesu instalace zvolili odeslání takových zpráv na servery Bitdefender a nyní byste chtěli proces zastavit:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte **Pokročilou** kartu.
3. Vypnout **Produktová hlášení**.

4.6. Oznámení o speciálních nabídkách

Když jsou k dispozici zvláštní nabídky, produkt Bitdefender vás na ně upozorní pomocí vyskakovacího okna. To vám umožňuje využít výhodných cen a chránit vaše zařízení delší dobu.

Pro zapnutí/vypnutí oznámení o speciálních nabídkách:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. V okně **Obecné** zapněte příslušný přepínač.

Možnost zvláštních nabídek a produktových zpráv je ve výchozím stavu povolena.

5. ROZHRANÍ PRODUKTU BITDEFENDER

Produkt Bitdefender Internet Security splňuje potřeby počítačových začátečníků, stejně jako technicky zkušených uživatelů. Jeho grafické uživatelské rozhraní je navrženo tak, aby vyhovovalo každé kategorii uživatelů.

Pro průchod uživatelského rozhraní Bitdefender využijte úvodního průvodce obsahujícího detaily o tom, jak produkt ovládat a nastavit, zobrazeného v horní části na levé straně. Vyberte pravou položku, aby jste byly naváděni nebo **Přeskočit**, pro ukončení průvodce.

Bitdefender ikona oznamovací oblasti je vám stále k dispozici nehledě na to, jestli chcete otevřít hlavní okno, spustit aktualizaci produktu, nebo prohlížet informace o nainstalované verzi.

Hlavní okno poskytuje informace o stavu zabezpečení. Na základě použití a vašich potřeb Autopilot zobrazuje různé typy doporučení, které vám pomohou zlepšit zabezpečení a výkon zařízení. Kromě toho můžete přidávat rychlé akce, které nejvíce využíváte, takže je máte po ruce, kdykoliv je potřebuje.

Z navigační nabídky na levé straně se dostanete do oblasti nastavení, oznámení a sekcí Bitdefender, kde najdete podrobnou konfiguraci a pokročilé administrativní úkoly.

Z horní části hlavního rozhraní máte přístup ke svému účtu Bitdefender. Také nás můžete kontaktovat, v případě, že máte nějaké dotazy.

5.1. Ikona oznamovací oblasti

Pro rychlejší správu celého produktu můete použít ikonu produktu Bitdefender v oznamovací oblasti.

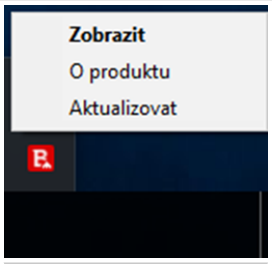
Poznámka

Ikona produktu Bitdefender nemusí být vždy vidět. Pro zobrazení ikony permanentně:

- V systémech **Windows 7, Windows 8 a Windows 8.1**:
  1. Klikněte na šipku v pravém dolním rohu obrazovky.
  2. Klikněte na položku **Přizpůsobit...** a otevře se okno ikon oznamovací oblasti.
  3. Vyberte položku **Zobrazovat ikony a upozornění** u ikony **Bitdefender Agent**.

- V systému **Windows 10**:
  1. Klepněte pravým tlačítkem myši na hlavní panel a vyberte **Nastavení hlavního panelu**.
  2. Přejděte dolů a klikněte na **Vybrat ikony, které se zobrazí na hlavním panelu** v části **Oblast oznámení**.
  3. Zapněte přepínač vedle položky **Bitdefender Agent**.

Když dvakrát kliknete na tuto ikonu, otevře se okno produktu Bitdefender. Po kliknutí na ikonu pravým tlačítkem se zobrazí kontextová nabídka umožňující rychlou správu produktu Bitdefender.



Tray Icon

- **Zobrazit** - otevře hlavní okno produktu Bitdefender.
- **O produktu** - otevře okno, kde můžete vidět informace o Bitdefender, kde hledat pomoc v případě, že se objeví něco neočekávaného, kde si přečtete smlouvu o předplatném a zobrazíte komponenty třetích stran a zásady ochrany osobních údajů.
- **Aktualizovat** - spustí okamžitou aktualizaci. Stav aktualizace můžete sledovat v panelu Aktualizace hlavního okna produktu Bitdefender.

Ikona systémové lišty Bitdefender vás informuje o problémech, které se týkají vašeho zařízení nebo jak produkt funguje, a to zobrazením speciálního symbolu takto:

Žádné problémy neovlivňují zabezpečení vašeho systému.
Kritické problémy ovlivňují bezpečnost vašeho systému. Požadují vaši akutní pozornost a musí být spraveny co nejdříve.

Pokud produkt Bitdefender nepracuje, ikona oznamovací oblasti se zobrazuje na šedém pozadí: . K tomu obvykle dojde, když vyprší vaše předplatné. Rovněž k tomu může dojít, když služby produktu Bitdefender nereagují, nebo pokud normální provoz produktu Bitdefender ovlivňují jiné chyby.

5.2. Navigační menu

Na levé straně rozhraní Bitdefender je navigační nabídka, která vám umožňuje rychlý přístup k funkcím a nástrojům Bitdefender, které potřebujete k práci s vaším produktem. Karty dostupné v této oblasti jsou:

- **Kontrolní panel**. Odsud můžete rychle opravovat bezpečnostní problémy, prohlížet doporučení podle potřeb vašeho systému a způsobů užívání a provádět rychlé akce.
-
- **Ochrana**. Odtud můžete spouštět a konfigurovat antivirové kontroly, obnovovat data v případě, že jsou šifrována ransowmwarem, a nakonfigurovat ochranu při surfování na internetu.
- **Soukromí**. Odsud můžete vytvářet správce hesel pro vaše online účty, chránit přístup k vaší webové kameře před nežádanýma očima, provádět online platby v bezpečném prostředí, otevřít aplikaci VPN a chránit vaše děti prohlížením a omezením jejich činnosti online.
- **Nástroje**. Odtud můžete spravovat profily a přistupovat k funkci ochrany dat.
- **Události**. Odtud máte přístup ke generovaným událostem.
- **Nastavení**. Odtud máte přístup k obecným nastavením.

V horní části hlavního rozhraní najdete funkce **Můj účet** a **Podpora** .

- **Podpora**. Odteď, kdykoliv budete potřebovat pomoc pří řešení problému s Bitdefender Internet Security, můžete kontaktovat Bitdefender oddělení technické podpory.
- **Můj účet**. Odsud můžete přistupovat k vašemu účtu Bitdefender pro ověření předplatných a provádění bezpečnostních činností na vašich spravovaných zařízeních. Jsou dostupné také detaily ohledně Bitdefender účtu a používaném předplatném.

5.3. Řídicí panel

Kontrolní panel vám umožňuje provádět běžné úkony, rychle opravovat bezpečnostní problémy, zobrazovat informace o činnosti produktu a mít přístup k panelům, ze kterých lze konfigurovat nastavení produktu.

Na vše stačí jen pár kliknutí.

Okno sestává ze tří hlavních oblastí:

Oblast stavu zabezpečení
: Zde můžete zkontrolovat stav zabezpečení vašeho zařízení.

Autopilot
: Zde můžete kontrolovat doporučení Autopilota pro zajištění správného fungování systému.

Rychlé akce
: Odtud můžete spouštět různé úkony pro udržení vašeho systému v bezpečí.

5.3.1. Oblast stavu zabezpečení

Bitdefender používá systém pro sledování problémů k detekci a informování o problémech, které mohou mít vliv na zabezpečení vašeho zařízení a dat. Zjištěné problémy zahrnují důležitá nastavení ochrany, která byla vypnuta, a jiné podmínky, které představují bezpečnostní riziko.

Kdykoli problémy ovlivňují zabezpečení vašeho zařízení, změní se stav, který se objeví v horní části rozhraní Bitdefender , na červenou. Zobrazený stav značí povahu problémů, které ovlivňují váš systém. Navíc, ikona v oznamovací oblasti se změní na a pokud umístíte kurzor myši na ikonu, vyskakovací okno potvrdí existenci nevyřešených problémů.

Protože zjištěné problémy mohou bránit produktu Bitdefender, aby vás chránil před hrozbami, nebo představovat zásadní bezpečnostní riziko, doporučujeme vám věnovat jim pozornost a opravit je co možná nejdříve. Pro opravení problému klikněte na tlačítko vedle zjištěného problému.

5.3.2. Autopilot

Pro efektivní provoz a zvýšenou ochranu během provádění různých akcí, Bitdefender Autopilot bude hrát roli vašeho soukromého bezpečnostního poradce. Podle činnosti, kterou se zabýváte, ať už pracujete, provádíte online platby, sledujete filmy, nebo hrajete hry, Bitdefender Autopilot navrhne kontextová doporučení na základě vašeho užívání zařízení a vašich potřeb. Navržená doporučení se mohou týkat také akcí, které je nutné provést pro zajištění činnosti vašeho produktu na plný výkon.

Abyste začali používat doporučenou funkci nebo zavedli vylepšení na váš produkt, klikněte na odpovídající tlačítko.

Vypnutí doporučení Autopilota

Aby upoutal vaši pozornost na doporučení Autopilota, produkt Bitdefender je nastaven tak, aby vás upozornil prostřednictvím vyskakovacího okna.

Pro vypnutí upozornění Autopilota:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. V okně **Obecné** vypněte **Upozornění na doporučení**.

5.3.3. Rychlé akce

Pomocí rychlých akcí můžete rychle spouštět úkoly, které považujete za důležité pro udržení vašeho systému v bezpečí, a pro zlepšení vaší práce.

Ve výchozím stavu Bitdefender zahrnuje rychlé akce, které lze nahradit těmi, které nejčastěji používáte. Pro nahrazení rychlé akce:

1. Klikněte na ikonu v pravém horním rohu karty, kterou chcete odstranit.
2. Ukažte kurzorem na úlohu, kterou chcete přidat do hlavního rozhraní, a poté klikněte na **PŘIDAT**.

Úlohy, které můžete přidat do hlavního rozhraní, jsou:

- **Rychlý sken**. Spusťte rychlou kontrolu a okamžitě zjistěte možné hrozby, které mohou na vašem zařízení existovat.
- **Systémový sken**. Spusťte kontrolu systému, abyste se ujistili, že vaše zařízení neobsahuje hrozby.
- **Sken zranitelností**. Prohledejte zranitelnost svého zařízení a ujistěte se, že všechny nainstalované aplikace spolu s operačním systémem jsou aktualizovány a správně fungují.
- **Wi-Fi Bezpečnostní Poradce**. Otevřete okno Poradce zabezpečení Wi-Fi uvnitř modulu zranitelnosti.
- **Portmonky**. Prohlížejte a spravujte své portmonky.
- **Otevřít Safepay**. Spuštěním funkce Bitdefender Safepay™ ochráníte citlivá data při provádění online transakcí.
- **Otevřít VPN**. Otevřete Bitdefender VPN, čímž přidáte ochrannou vrstvu navíc, zatímco jste připojeni k internetu.
- **Likvidátor souborů**. Spusťte nástroj File Shredder a odstraňte ze zařízení stopy citlivých dat.

Pro zahájení ochrany přidaných zařízení s Bitdefender:

1. Klikněte na **Instalovat na další zařízení**.

Na obrazovce se objeví nové okno.

2. Klikněte na **ODESLAT ODKAZ NA STAŽENÍ**.
3. Při instalaci produktu Bitdefender postupujte podle pokynů.

V závislosti na Vaší volbě, následující produkty Bitdefender budou nainstalovány:

- Bitdefender Internet Security na zařízeních s operačním systémem Windows.
- Bitdefender Antivirus pro Mac na zařízeních s operačním systémem macOS.
- Bitdefender zabezpečení pro mobilní zařízení s operačním systémem Android.
- Bitdefender zabezpečení pro mobilní zařízení s operačním systémem iOS.

5.4. Sekce Bitdefender

Produkt Bitdefender je dodáván se třemi sekcemi rozdělenými do užitečných modulů, které vám pomohou být chráněni při práci, procházení webu nebo provádění online plateb, zlepšují rychlost vašeho systému a provádějí mnoho dalších činností.

Kdykoli se chcete dostat k funkcím konkrétní sekce nebo začít s nastavováním vašeho produktu, můžete tak učinit pomocí následujících ikon v rozhraní Bitdefender:

-  Ochrana
-  Soukromí
-  Služby

5.4.1. **Ochrana**

V části Ochrana můžete nakonfigurovat pokročilá nastavení zabezpečení, spravovat přátele a spammery, prohlížet a upravovat nastavení síťového připojení, nastavovat funkce prevence online hrozeb, kontrolovat a opravovat potenciální zranitelnosti systému a posuzovat zabezpečení bezdrátového připojení sítě, ke kterým se připojujete.

Na panelu Ochrana lze spravovat následující moduly:

ANTIVIRUS

Antivirová ochrana je základem vašeho zabezpečení. Produkt Bitdefender vás v reálném čase a na požádání chrání před všemi druhy hrozeb, jako je malware, trojské koně, spyware, adware atd.

Z antivirového modulu můžete snadno provádět následující činnosti skenování:

- Rychlý sken
- Kompletní sken
- Spravovat skeny
- Rescue Environment

Další informace o činnostech skenování a konfiguraci antivirové ochrany viz *„Antivirová ochrana“* (str. 79).

PREVENCE ONLINE HROZEB

Prevence online hrozeb vás chrání před phishingovými útoky, podvodnými pokusy a úniky soukromých dat při surfování na Internetu.

Další informace o konfiguraci produktu Bitdefender pro ochranu vašich webových aktivit viz *„Prevence online hrozeb“* (str. 102).

FIREWALL

Brána firewall vás chrání, když jste připojeni k sítím a Internetu, filtrováním všech pokusů o připojení.

Další informace o konfiguraci brány firewall najdete v části *„Firewall“* (str. 114).

Pokročilá ochrana před hrozbami

Pokročilá ochrana před hrozbami aktivně chrání systém proti druhům hrozeb jako je ransomware, spyware a trojské koně tím, že kontroluje chování všech nainstalovaných aplikací. Podezřelé procesy jsou identifikovány a, když je to nezbytné, blokovány.

Další informace o tom, jak zajistit, aby byl Váš systém chráněný před malwarem, najdete v části *„Pokročilá Ochrana“* (str. 99).

ANTISPAM

Antispamový modul produktu Bitdefender filtruje poštovní provoz na protokolu POP3 a tak zajišťuje, aby vaše složka přijaté pošty neobsahovala nevyžádané emaily.

Další informace o antispamové ochraně viz *„Antispam“* (str. 105).

ZRANITELNOST

Modul Vulnerability vám pomáhá udržovat operační systém a aplikace, které pravidelně používáte, a identifikovat nezabezpečené bezdrátové sítě, ke kterým se připojujete. Kliknutím na **Otevřít** v modulu Zranitelnost získáte přístup k jeho funkcím.

Funkce **Sken zranitelností** vám umožňuje identifikovat kritické aktualizace systému Windows, aktualizace aplikací, slabá hesla patřící k účtům Windows a bezdrátové sítě, které nejsou zabezpečené. Klepnutím na **Spustit skenování** provedete skenování v zařízení.

Kliknutím na **Wi-Fi Bezpečnostní poradce** zobrazíte seznam bezdrátových sítí, ke kterým se připojujete, spolu s naším hodnocením reputace pro každou z nich a opatřeními, která můžete podniknout, abyste zůstali v bezpečí z potenciálních sledování.

Další informace o konfiguraci ochrany před zranitelnostmi viz *„Zranitelnosti“* (str. 120).

Náprava Ransomware

Funkce Náprava Ransomware vám pomáhá obnovit soubory v případě, že ransomware nějaké zašifruje.

Pro více informací o tom jak obnovit zašifrované soubory, obraťte se na *„Zotavení po infekci Ransomware“* (str. 132).

5.4.2. Soukromí

V sekci Soukromí můžete otevřít aplikaci Bitdefender VPN, šifrovat své osobní údaje, zabezpečit své online transakce, udržet svou webovou kameru a prohlížení internetu v bezpečí a chránit své děti sledováním a omezováním jejich činnosti online.

Moduly, které můžete spravovat v sekci Soukromí, jsou:

VPN

VPN chrání vaši online činnost a skryje vaši IP adresu pokaždé, když se připojujete k nezabezpečené bezdrátové síti na letištích, v obchodech, kavárnách nebo hotelech. Navíc získáte přístup k obsahu, který je běžně v určitých lokalitách nepřístupný.

Další informace o této funkci naleznete na *„VPN“* (str. 145).

OCHRANA VIDEO & AUDIO

Ochrana videa & zvuku chrání webovou kameru před nebezpečím zablokováním přístupu nedůvěryhodných aplikací a upozorní vás, když se aplikace pokusí získat přístup k mikrofonu.

Více informací o tom, jak chránit webovou kameru před nechtěným přístupem a jak nastavit Bitdefender, aby vás upozornil na aktivitu mikrofonu, naleznete v části *„Ochrana video & Audio“* (str. 128).

PASSWORD MANAGER

Správce hesel produktu Bitdefender vám pomáhá sledovat vaše hesla, chrání vaše soukromí a zajišťuje bezpečné procházení webu.

Další informace o konfiguraci modulu Správce hesel viz *„Ochrana vašich osobních dat správcem hesel“* (str. 135).

SAFEPAY

Prohlížeč Bitdefender Safepay™ vám umožňuje zachovat soukromí a bezpečí při online bankovnictví, nakupování v e-shopech a dalších druzích online transakcí.

Další informace o funkci Bitdefender Safepay™ viz *„Zabezpečení Safepay pro online transakce“* (str. 149).

RODIČOVSKÁ KONTROLA

Bitdefender Rodičovská kontrola umožňuje sledovat, co vaše děti na svém zařízení dělají. V případě nevhodného obsahu můžete omezit přístup k Internetu nebo určitým aplikacím.

Kliknutím na tlačítko **Konfigurace** v okně Rodičovské kontroly můžete začít konfigurovat zařízení Vašich dětí a sledovat jejich činnosti odkudkoli.

Další informace o konfiguraci modulu Správce hesel viz *„Rodičovská kontrola“* (str. 154).

ANTI-TRACKER

Funkce Anti-tracker vám pomůže vyhnout se sledování, takže vaše data zůstanou při surfování soukromá a zároveň zkrátí dobu načítání webových stránek.

Další informace o funkci Anti-tracker naleznete v části *„Anti-tracker“* (str. 142).

5.4.3. Služby

Ochrana dat

Likvidátor souborů produktu Bitdefender vám pomůže trvale odstranit data fyzickým smazáním z pevného disku.

Další informace o tom naleznete na stránce „*Ochrana dat*“ (str. 175).

Profily

Každodenní pracovní činnosti, sledování filmů nebo hraní her mohou způsobovat zpomalení systému, zejména pokud běží zároveň s procesy aktualizací a činností údržby systému Windows.

S pomocí produktu Bitdefender nyní můžete zvolit a použít upřednostňovaný profil, který provede nastavení systému vhodná pro zvýšení výkonu určitých nainstalovaných aplikací.

Další informace o této funkci naleznete na „*Profily*“ (str. 168).

5.5. Změnit jazyk produktu

Rozhraní Bitdefender je k dispozici v několika jazycích a lze jej změnit pomocí následujících kroků:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. V **Hlavním** okně, klikněte na **Změna jazyka**.
3. Vyberte ze seznamu požadovaný jazyk a poté klikněte na **ULOŽIT**.
4. Chvíli vyčkejte, než se nové nastavení projeví.

6. BITDEFENDER CENTRAL

Bitdefender Central je platforma, na které máte přístup k online funkcím a službám produktu a kde můžete vzdáleně provádět důležité činnosti na zařízeních, na nichž je produkt Bitdefender nainstalován. Ke svému účtu Bitdefender se můžete přihlásit z jakéhokoli zařízení připojeného k internetu. Přejděte na adresu https://central.bitdefender.com nebo přímo z aplikace Bitdefender Central na zařízeních Android a iOS.

Pro nainstalování aplikace Bitdefender Central na vaše zařízení:

- **Na Androidu** - hledejte na Google Play Bitdefender Central a poté stáhněte a nainstalujte aplikaci. Následujte požadované kroky pro dokončení instalace.
- **Na iOS** - hledejte v App Store Bitdefender Central a poté stáhněte a nainstalujte aplikaci. Následujte požadované kroky pro dokončení instalace.

Jakmile jste přihlášeni, můžete provádět následující činnosti:

- Stáhněte a nainstalujte Bitdefender na operačních systémech Windows, macOS, iOS a Android. Ke stažení jsou k dispozici následující produkty:
  - Bitdefender Internet Security
  - Antivirový program Bitdefender pro počítače Macintosh
  - Bitdefender Mobile Security pro Android
  - Bitdefender zabezpečení mobilních zařízení s operačním systémem iOS
  - Bitdefender Rodičovský Kontrola
- Spravovat a obnovovat předplatná produktu Bitdefender.
- Přidávat nová zařízení do vaší sítě a odkudkoli je spravovat.
- Upravujte nastavení Rodičovského poradce na zařízeních Vašich dětí a mějte dozor nad jejich aktivitami odkudkoli.

6.1. Přistupuji na Bitdefender Central

Existuje několik možností, jak jít na Bitdefender Central:

- Z hlavního rozhraní produktu Bitdefender:
  1. Klikněte na **Můj účet** v navigačním menu v rozhraní Bitdefender.
  2. Klikněte na **Přejít k Bitdefender**.

3. Přihlaste se k účtu Bitdefender pomocí Vaší emailové adresy a hesla.

- Z webového prohlížeče:
  1. Otevřít webový prohlížeč na libovolném zařízení s přístupem k Internetu.
  2. Přejděte na adresu: https://central.bitdefender.com.
  3. Přihlaste se k účtu Bitdefender pomocí Vaší emailové adresy a hesla.
- Z vašich Android nebo iOS zařízení:

  Otevřete aplikaci Bitdefender Central, kterou jste si nainstalovaly.

Poznámka
V tomto materiálu máte k dispozici možnosti a pokyny dostupné na webové platformě.

6.2. Dvoufaktorové ověření

Metoda dvoufaktorové autentifikace přidává k vašemu účtu Bitdefender dodatečnou bezpečnostní vrstvu tím, že kromě vašich přihlašovacích údajů vyžaduje ověřovací kód. Tímto způsobem zamezíte odcizení účtu a ubráníte se před kybernetickými útoky, jako jsou keyloggery, útoky hrubou silou (brute-force) atd.

Zapnout dvoufaktorové ověření

Pokud povolíte dvoufaktorové ověřování, bude váš účet Bitdefendermnohem bezpečnější a vaše identita bude ověřena pokaždé, když se přihlásíte z různých zařízení, a to buď při instalaci jednoho z Bitdefender. Zkontrolujte stav předplatného nebo spusťte úlohy vzdáleně na svých zařízeních.

Pro zapnutí dvoufaktorové ověření:

1. Přihlaš se na Bitdefender Central.
2. Klikněte na ikonu v pravém horním rohu obrazovky.
3. Klikněte na **Bitdefender Účet** v rolovacím menu.
4. Vyberte kartu **Heslo a zabezpečení**.
5. Klikněte na **Dvoufaktorové ověření**.
6. Klikněte na **ZAČÍT**.

   Vyberte jednu z následujících možností:

- **Aplikace pro autentifikaci** - pomocí aplikace pro ověřování vygenerujte kód při každém přihlášení k účtu Bitdefender.

  Pokud chcete použít aplikaci pro ověřování, ale nejste si jisti, co si vybrat, je k dispozici seznam s ověřovacími aplikacemi, které doporučujeme.

  a. Chcete-li začít, klikněte na **POUŽÍT APLIKACI PRO AUTENTIFIKACI**.

  b. Chcete-li se přihlásit na zařízení se systémem Android nebo iOS, naskenujte QR kód.

  Chcete-li se přihlásit na notebooku nebo na ploše, můžete ručně zobrazený kód přidat.

  Klikněte na tlačítko **Pokračovat**.

  c. Vložte kód poskytnutý aplikací nebo kód zobrazený v předchozím kroku a potom klepněte na tlačítko **AKTIVOVAT**.

- **E-mail** - pokaždé, když se přihlásíte ke svému účtu Bitdefender, bude do vaší e-mailové schránky odeslán ověřovací kód. Zkontrolujte svůj e-mailový účet a zadejte požadovaný kód.

  a. začněte kliknutím na **POUŽÍT EMAIL**.

  b. Zkontrolujte svůj e-mailový účet a zadejte požadovaný kód.

  Nezapomeňte, že máte pět minut na to, abyste zkontrolovali svůj e-mailový účet a zadali vygenerovaný kód. Pokud doba platnosti odkazu vyprší, musíte vygenerovat nový pomocí stejných kroků.

  c. Klikněte na **AKTIVOVAT**.

  d. Máte k dispozici deset aktivačních kódů, které můžete kopírovat, stahovat nebo tisknout a používat v případě, že ztratíte svou e-mailovou adresu nebo se nebudete moci přihlásit. Každý kód lze použít pouze jednou.

  e. Klikněte na **HOTOVO**.

V případě, že chcete ukončit dvoufaktorové ověření:

1. Klikněte na **VYPNOUT DVOUFAKTOROVÉ OVĚŘENÍ**.
2. Zkontrolujte aplikaci nebo e-mailový účet a zadejte kód, který jste obdrželi.

   V případě, že jste se rozhodli pro zaslání ověřovacího kódu e-mailem, máte pět minut na to, abyste zkontrolovali svůj e-mailový účet a zadali vygenerovaný kód. Pokud doba platnosti odkazu vyprší, musíte vygenerovat nový pomocí stejných kroků.

3. Potvrďte vaši volbu.

6.2.1. Přidat důvěryhodná zařízení

Chcete-li se ujistit, že k účtu Bitdefender máte přístup pouze vy, budeme potřebovat nejdříve bezpečnostní kód. Pokud chcete tento krok přeskočit při každém připojení ze stejného zařízení, doporučujeme jej nastavit jako důvěryhodné zařízení.

Přidání zařízení jako důvěryhodné:

1. Přihlaš se na Bitdefender Central.
2. Klikněte na ikonu v pravém horním rohu obrazovky.
3. Klikněte na **Bitdefender Účet** v rolovacím menu.
4. Vyberte kartu **Heslo a zabezpečení**.
5. Klikněte na **Důvěryhodná zařízení**.
6. Zobrazí se seznam se zařízeními, kde je nainstalovaný Bitdefender. Klikněte na požadované zařízení.

Můžete přidat tolik zařízení, kolik chcete, za předpokladu, že mají nainstalovaný Bitdefender a vaše předplatné je platné.

6.3. Moje předplatná

Platforma Bitdefender Central vám nabízí možnost snadno spravovat předplatná, která máte k dispozici pro všechna vaše zařízení.

6.3.1. Kontrola dostupných předplatných

Postup kontroly dostupných předplatných:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel **Moje předplatná**.

Zde jsou k dispozici informace o dostupnosti předplatných, která vlastníte, a počtu zařízení, která je používají.

Můžete přidat nové zařízení k předplatnému nebo ho obnovit výběrem karty předplatného.

Poznámka
Můžete mít jedno nebo více předplatných na vašem účtu za předpokladu, že jsou určeny pro různé platformy (Windows, Mac OS X, nebo Android).

6.3.2. Přidání nového zařízení

Pokud se vaše předplatné vztahuje k více než jednomu zařízení, můžete přidat nové zařízení a nainstalovat na ně produkt Bitdefender Internet Security provedením následujícího postupu:

1. Přihlaš se na Bitdefender Central.
2. Vyberte menu **Moje Zařízení** a klikněte na **INSTALOVAT OCHRANU**.
3. Prosím vyberte jednu z následujících variant

   - **Chránit toto zařízení**

     Vyberte tuto možnost a vyberte vlastníka zařízení. Pokud zařízení patří někomu jinému, klepněte na odpovídající tlačítko.

   - **Chránit další zařízení**

     Vyberte tuto možnost a vyberte vlastníka zařízení. Pokud zařízení patří někomu jinému, klepněte na odpovídající tlačítko.

     Klikněte na **ODESLAT ODKAZ NA STAŽENÍ**. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Pamatujte, že vygenerovaný odkaz ke stažení je platný pouze 24 hodin. Pokud doba platnosti odkazu vyprší, musíte vygenerovat nový pomocí stejných kroků.

     Na zařízení, kde chcete nainstalovat váš Bitdefender produkt Bitdefender, zkontrolujte emailový účet, který jste zadali a poté klikněte na příslušné tlačítko stáhnout
4. Počkejte na dokončení stahování a poté spusťte instalační soubor.

6.3.3. Obnovení předplatného

Pokud jste nezvolili automatické obnovení předplatného Bitdefender, můžete ho obnovit ručně pomocí následujícího postupu:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel **Moje předplatná**.
3. Vyberte požadovanou kartu předplatného.

4. Pokračujte kliknutím na tlačítko **Obnovit**.

Ve webovém prohlížeči se otevře webová stránka, na které můžete obnovit předplatné produktu Bitdefender.

6.3.4. Aktivace předplatného

Předplatné lze aktivovat během instalace pomocí vašeho účtu Bitdefender. Společně s procesem aktivace se začne odpočítávat její platnost.

Pokud jste zakoupili aktivační kód od některého z našich dealerů nebo jste ho obdrželi jako dárek, můžete přidat jeho dostupnost do předplatného produktu Bitdefender za předpokladu, že je určený pro tentýž produkt.

Pro aktivování předplatného s využitím aktivačního kódu:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel **Moje předplatná**.
3. Klikněte na tlačítko **AKTIVAČNÍ KÓD** a poté kód zadejte do příslušného pole.
4. Pokračujte kliknutím na tlačítko **Aktivovat**.

Předplatné je aktivováno. Přejděte do panelu **Moje zařízení** a vyberte položku **INSTALOVAT OCHRANU** pro instalaci produktu na jedno z vašich zařízení.

6.4. Moje zařízení

Oblast **Moje zařízení** ve vašem účtu Bitdefender Central vám poskytuje možnost instalovat, spravovat a vzdáleně ovládat produkt Bitdefender na libovolném zařízení, pokud je zapnuto a připojeno k Internetu. Na kartách zařízení se zobrazuje název zařízení, stav ochrany a případná rizika ovlivňující zabezpečení vašich zařízení.

Pro zobrazení seznamu vašich zařízení uspořádaných podle jejich stavu nebo uživatelů klikněte na šipku rozbalovacího menu v pravém horním rohu obrazovky.

Pro snadnou identifikaci zařízení můžete přizpůsobit jejich názvy:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel **Moje zařízení**.

3. Klikněte na požadovanou kartu zařízení a poté na ikonu ⋮ v pravé horní části obrazovky.
4. Zvolte **Nastavení**.
5. Zadejte nové jméno do pole **Název zařízení** a poté klikněte na **Uložit**.

Pro lepší správu můžete vytvořit a přiřadit vlastníka každému z vašich zařízení:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel **Moje zařízení**.
3. Klikněte na požadovanou kartu zařízení a poté na ikonu ⋮ v pravé horní části obrazovky.
4. Zvolte **Profil**.
5. Klikněte na **Přidat správce** a poté vyplňte příslušná pole. Upravte svůj profil, přidejte fotku a nastavte datum narození.
6. Kliknutím na tlačítko **ADD** profil uložíte.
7. Vyberte požadovaného vlastníka v seznamu **Device owner** a poté klikněte na tlačítko **ASSIGN**.

Pro vzdálenou aktualizaci Bitdefender na Windows zařízeních:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel **Moje zařízení**.
3. Klikněte na požadovanou kartu zařízení a poté na ikonu ⋮ v pravé horní části obrazovky.
4. Zvolte **Aktualizovat**.

Další vzdálené akce a informace ohledně produktu Bitdefender na konkrétním zařízení jsou k dispozici po kliknutí na kartu požadovaného zařízení.

Po kliknutí na kartu zařízení jsou k dispozici následující karty:

- **Ovládací panel**. V tomto okně můžete prohlížet informace o zvoleném zařízení, kontrolovat jeho stav zabezpečení, stav Bitdefender VPN a kolik hrozeb bylo zablokováno za posledních sedm dní. Stav zabezpečení může být zelený, když s vaším zařízením není žádný problém, žlutý, pokud zařízení vyžaduje pozornost nebo červený, když je zařízení ohroženo. Pokud se na

vašem zařízení vyskytnou problémy, klikněte na šipku rozbalovacího menu v horní části stavu pro více informací. Odsud můžete ručně opravovat problémy, které ovlivňují zabezpečení vašich zařízení.

- **Ochrana**. V tomto okně můžete vzdáleně spustit rychlý nebo kompletní sken na vašich zařízeních. Kliknutím na tlačítko **SKEN** proces spustíte. Rovněž můžete zjistit, kdy na zařízení proběhl poslední sken, a k dispozici je zpráva o posledním skenu s nejdůležitějšími informacemi.Další informace o uvedených dvou skenovacích procesech viz 14.2.3 – *„Provedení kompletního skenu“* a *„Provedení rychlého skenu“* (str. 84).
- **Zranitelnost**. Pokud chcete v zařízení vyhledat jakékoliv nedostatky, jako chybějící aktualizace systému Windows, zastaralé aplikace nebo slabá hesla, klikněte na tlačítko **Skenovat** na kartě Zabezpečení. Zranitelnosti nelze opravit vzdáleně. Pokud budou nalezeny jakékoliv nedostatky, spusťte znovu kontrolu svého zařízení a následně proveďte doporučené akce. Klikněte na **Více detailů** k získání detailního hlášení o nalezených problémech. Pro více informací o této možnosti se prosím podívejte na *„Zranitelnosti“* (str. 120).

6.5. Aktivita

V okně Aktivita máte přístup k informacím o zařízeních, která mají nainstalovaný Bitdefender.

Jakmile otevřete okno **Aktivita**, máte k dispozici následující karty:

- **Moje zařízení**. Zde můžete zobrazit počet připojených zařízení spolu s jejich stavem ochrany. Chcete-li na zjištěných zařízeních vzdáleně opravit problémy, klepněte na tlačítko **Opravit problémy** a poté klepněte na **SKENOVAT A OPRAVIT PROBLÉMY**.

  Chcete-li zobrazit podrobnosti o zjištěných problémech, klikněte na volbu **Zobrazit problémy**.

  Informace o zjištěných hrozbách nelze načíst ze zařízení založených na systému iOS.

- **Hrozby zablokovány**. Zde si můžete prohlédnout graf zobrazující celkovou statistiku včetně informací o hrozbách blokovaných za posledních 24 hodin a sedm dní. Zobrazované informace jsou načteny v závislosti na škodlivém chování zjištěném v přístupových souborech, aplikacích a URL adresách.

- **Uživatelé s největším počtem zablokovaných hrozeb**. Zde si můžete prohlédnout, u kterých uživatelů bylo nalezeno nejvíce hrozeb.
- **Zařízení s největším počtem blokovaných hrozeb**. Zde si můžete prohlédnout, u kterých zařízení bylo nalezeno nejvíce hrozeb.

6.6. Upozornění

Abyste měli neustálý přehled o tom, co se děje se zařízeními připojenými k Vašemu účtu, máte k dispozici ikonu 🔔. Po kliknutí získáte kompletní obrázek o všech aktivitách produktů Bitdefender, nainstalovaných na Vašich zařízeních.

7. AKTUALIZACE PRODUKTU BITDEFENDER

Každý den jsou nalezeny a identifikovány nové hrozby. Proto je velmi důležité udržovat Bitdefender aktuální s nejnovější databází s informacemi o hrozbách.

Pokud jste připojeni k Internetu pomocí vysokorychlostního připojení nebo DSL, produkt Bitdefender se o aktualizace stará sám. Ve výchozím nastavení kontroluje aktualizace po zapnutí zařízení a poté každou **hodinu** . Pokud je aktualizace detekována, je automaticky stažena a nainstalována do vašeho zařízení.

Proces aktualizace se provede za provozu, což znamená, že aktualizované soubory se nahrazují průběžně. Tímto způsobem proces aktualizace nenaruší provoz produktu a současně bude vyloučena jakákoli zranitelnost.

Důležité
Pro zajištění trvalé ochrany před nejnovějšími hrozbami nechte automatické aktualizace zapnuté.

V určitých situacích je pro zajištění aktuální ochrany produktu Bitdefender nutný váš zásah:

- Pokud se vaše zařízení připojuje k internetu přes proxy server, musíte nakonfigurovat nastavení proxy, jak je popsáno v *„Jak nakonfigurovat produkt Bitdefender, aby používal připojení k Internetu pomocí proxy?“* (str. 72).
- Pokud jste k Internetu připojeni pomocí vytáčeného připojení, doporučujeme pravidelně aktualizovat produkt Bitdefender na žádost uživatele. Další informace viz *„Provedení aktualizace“* (str. 40).

7.1. Kontrola aktuálnosti produktu Bitdefender

Pro zkontrolování poslední aktualizace vašeho Bitdefender:

1. Klikněte na **Upozornění** v navigačním menu v rozhraní Bitdefender.
2. V záložce **Vše** vyberte notifikaci týkající se posledního updatu.

Můžete zjistit, kdy byly aktualizace zahájeny, a informace o nich (zda byly úspěšné nebo ne, zda vyžadují pro dokončení instalace restart). V případě potřeby restartujte systém, jakmile to bude možné.

7.2. Provedení aktualizace

K provádění aktualizací je vyžadováno připojení k Internetu.

Pro zahájení aktualizace klikněte na ikonu produktu Bitdefender v oznamovací oblasti a vyberte položku **Aktualizovat nyní**.

Modul Aktualizace se připojí k aktualizačnímu serveru společnosti Bitdefender a vyhledá aktualizace. Pokud je nalezena aktualizace, budete vyzváni k jejímu potvrzení, nebo bude provedena automaticky, v závislostri na nastavení aktualizací.

Důležité
Po dokončení aktualizace může být nutné restartovat zařízení. Doporučujeme tak učinit co nejdříve.

Aktualizace vašich zařízení lze provádět také vzdáleně, pokud jsou zapnutá a připojená k Internetu.

Pro vzdálenou aktualizaci Bitdefender na Windows zařízeních:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel **Moje zařízení**.
3. Klikněte na požadovanou kartu zařízení a poté na ikonu v pravé horní části obrazovky.
4. Zvolte **Aktualizovat**.

7.3. Zapnutí nebo vypnutí automatických aktualizací

Zapnutí nebo vypnutí automatických aktualizací

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Aktualizace**.
3. Zapněte nebo vypněte příslušný přepínač.
4. Objeví se výstražné okno. Výběr potvrďte zvolením doby, po kterou mají být automatické aktualizace vypnut, z nabídky. Automatické aktualizace můžete vypnout na 5, 15 nebo 30 minut, na hodinu nebo do příštího restartu systému.

Varování
Jde o kritický bezpečnostní problém. Doporučujeme vypnout automatické aktualizace jen na nejkratší dobu. Pokud produkt Bitdefender není pravidelně aktualizován, nebude vás moci chránit před nejnovějšími hrozbami.

7.4. Úprava nastavení aktualizací

Aktualizace lze provádět z místní sítě nebo z internetu přímo nebo přes proxy server. Ve výchozím stavu produkt Bitdefender kontroluje aktualizace po Internetu každou hodinu a dostupné aktualizace instaluje, aniž by vás obtěžoval.

Výchozí nastavení aktualizací jsou vhodná pro většinu uživatelů a obvykle je není třeba měnit.

Pro úpravu nastavení aktualizací:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Aktualizace** a upravujte nastavení které vám nejlépe vyhovuje.

Četnost aktualizací

Produkt Bitdefender je nakonfigurován, aby aktualizace kontroloval každou hodinu. Chcete-li četnost aktualizací změnit, přemístěním posuvníku nastavte požadovanou dobu, po které má dojít k aktualizaci.

Pravidla zpracování aktualizací

Pokaždé, když je k dispozici aktualizace, Bitdefender ji automaticky stáhne a zavede, aniž by zobrazil upozornění. Pokud chcete být upozorněni pokaždé, když je nová aktualizace k dispozici, vypněte možnost **Tichá aktualizace**.

Některé aktualizace vyžadují pro dokončení instalace restart.

Pokud aktualizace vyžaduje restart, ve výchozím nastavení bude produkt Bitdefender pracovat se starými soubory, dokud uživatel zařízení dobrovolně nerestartuje. Důvodem je, aby proces aktualizací produktů Bitdefender nezasahoval do práce uživatele.

Pokud chcete být vyzváni, když aktualizace vyžaduje restartování, zapněte **Upozornění na restart**.

7.5. Průběžné aktualizace

Abyste mohli mít jistotu, že používáte nejnovější verzi produktu, Váš Bitdefender automaticky kontroluje nové aktualizace. Tyto aktualizace mohou přinést nové funkce a vylepšení, opravit nedostatky v produktu, nebo automaticky upgradovat na novou verzi. Když skrze aktualizaci přejdete na novou verzi Bitdefender, Vaše osobní nastavení jsou zachována a proces instalace a odinstalace je přeskočen.

Tyto aktualizace vyžadují restartování systému za účelem zahájení instalace nových souborů. Je-li aktualizace produktu dokončena, budete vyzváni pop-up oknem k restartování systému. Pokud neuvidíte toto upozornění, můžete buď kliknout na **RESTARTOVAT NYNÍ** v okně Upozornění, kde je zobrazena poslední provedená aktualizace, nebo ručně restartovat systém.

Poznámka

Aktualizace, zahrnující nové funkce a vylepšení, budou doručeny pouze uživatelům s nainstalovaným Bitdefender 2020.

DOPORUČENÉ POSTUPY

8. INSTALACE

8.1. Jak mohu nainstalovat produkt Bitdefender na druhé zařízení?

Pokud zakoupené předplatné zahrnuje více než jedno zařízení, můžete pomocí svého účtu Bitdefender aktivovat druhé PC.

Instalace Bitdefender na druhé zařízení:

1. Klikněte na **Instalovat na další zařízení** ve spodním levém rogu Bitdefender rozhraní.

   Na obrazovce se objeví nové okno.

2. Klikněte na **ODESLAT ODKAZ NA STAŽENÍ**.
3. Pro nainstalování Bitdefender postupujte podle pokynů.

Nové zařízení, na které jste nainstalovali produkt Bitdefender, se zobrazí na kartě Bitdefender Central.

8.2. Jak mohu přeinstalovat Bitdefender?

Mezi obvyklé situace, kdy je třeba produkt Bitdefender přeinstalovat, patří následující:

- přeinstalovali jste operační systém.
- opravit problémy, které mohou způsobovat zpomalení nebo pády
- Váš produkt Bitdefender se nespouští nebo nepracuje tak, jak má.

V případě, že je jedna ze zmíněných situací právě Vaším případem, řiďte se následujícími pokyny:

- V systému **Windows 7**:
  1. Klikněte na nabídku **Start** a přejděte do nabídky **Všechny programy**.
  2. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
  3. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
  4. K dokončení procesu je třeba restartovat zařízení.
- V systémech **Windows 8 a Windows 8.1**:

1. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
2. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
4. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
5. K dokončení procesu je třeba restartovat zařízení.

- V systému **Windows 10**:

1. Klikněte na nabídku **Start** a poté na položku Nastavení.
2. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Aplikace a funkce**.
3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
4. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.
5. Klikněte na **PŘEINSTALOVAT**.
6. K dokončení procesu je třeba restartovat zařízení.

Poznámka
Provedením tohoto přeinstalačního procesu jsou osobní nastavení uložena a k dispozici v nově nainstalovaném produktu. Ostatní nastavení mohou být vrácena zpět do svého výchozího nastavení.

8.3. Odkud mohu stáhnout produkt Bitdefender?

Můžete nainstalovat produkt Bitdefender z instalačního disku nebo pomocí webového instalátoru, který si můžete do svého zařízení stáhnout z platformy Bitdefender Central.

Poznámka
Než sadu spustíte, doporučujeme odebrat případné antivirové řešení nainstalované ve vašem počítači. Pokud na stejném zařízení používáte více než jedno řešení zabezpečení, systém se stane nestabilním.

K instalaci Bitdefender z Bitdefender Central:

1. Přihlaš se na Bitdefender Central.

2. Vyberte menu **Moje Zařízení** a klikněte na **INSTALOVAT OCHRANU**.
3. Prosím vyberte jednu z následujících variant

   - **Chránit toto zařízení**

     Vyberte tuto možnost a vyberte vlastníka zařízení. Pokud zařízení patří někomu jinému, klepněte na odpovídající tlačítko.

   - **Chránit další zařízení**

     Vyberte tuto možnost a vyberte vlastníka zařízení. Pokud zařízení patří někomu jinému, klepněte na odpovídající tlačítko.

     Klikněte na **ODESLAT ODKAZ NA STAŽENÍ**. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Pamatujte, že vygenerovaný odkaz ke stažení je platný pouze 24 hodin. Pokud doba platnosti odkazu vyprší, musíte vygenerovat nový pomocí stejných kroků.

     Na zařízení, kde chcete nainstalovat váš Bitdefender produkt Bitdefender, zkontrolujte emailový účet, který jste zadali a poté klikněte na příslušné tlačítko stáhnout

4. Spusťte produkt Bitdefender, který jste stáhli.

8.4. Jak mohu změnit jazyk mého Bitdefender produktu?

Rozhraní Bitdefender je k dispozici v několika jazycích a lze jej změnit pomocí následujících kroků:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. V **Hlavním** okně, klikněte na **Změna jazyka**.
3. Vyberte ze seznamu požadovaný jazyk a poté klikněte na **ULOŽIT**.
4. Chvíli vyčkejte, než se nové nastavení projeví.

8.5. Jak mohu použít předplatné produktu Bitdefender po upgradu systému Windows?

Tato situace nastane, když upgradujete operační systém a chcete pokračovat v předplatném produktu Bitdefender.

Pokud používáte předchozí verzi produktu Bitdefender, můžete zdarma upgradovat na nejnovější produkt Bitdefender, provedením následujícího postupu:

- Z předchozí verze antiviru Bitdefender na nejnovější dostupnou verzi antiviru Bitdefender.
- Z předchozí verze produktu Bitdefender Internet Security na nejnovější dostupnou verzi produktu Bitdefender Internet Security.
- Z předchozí verze produktu Bitdefender Total Security na nejnovější dostupnou verzi produktu Bitdefender Total Security.

Mohou nastat dva případy:

- Operační systém jste aktualizovali pomocí služby Windows Update a zjistili jste, že produkt Bitdefender již nefunguje.

  V tomto případě je nutné přeinstalovat produkt dle následujících pokynů:

  - V systému **Windows 7**:

    1. Klikněte na nabídku **Start**, přejděte do **Ovládacích panelů** a dvakrát klikněte na položku **Programy a funkce**.
    2. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
    3. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
    4. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

       Otevřete rozhraní svého nově nainstalovaného produktu Bitdefender pro přístup k jeho funkcím.

  - V systémech **Windows 8 a Windows 8.1**:

    1. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
    2. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
    3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
    4. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
    5. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

Otevřete rozhraní svého nově nainstalovaného produktu Bitdefender pro přístup k jeho funkcím.

- V systému **Windows 10**:
  1. Klikněte na nabídku **Start** a poté na položku Nastavení.
  2. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Aplikace**.
  3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
  4. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.
  5. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
  6. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

     Otevřete rozhraní svého nově nainstalovaného produktu Bitdefender pro přístup k jeho funkcím.

> **Poznámka**
> Provedením tohoto přeinstalačního procesu jsou osobní nastavení uložena a k dispozici v nově nainstalovaném produktu. Ostatní nastavení mohou být vrácena zpět do svého výchozího nastavení.

- Změnili jste systém a chcete nadále používat ochranu produktem Bitdefender. Proto je třeba přeinstalovat produkt s použitím nejnovější verze.

  Postup řešení této situace:

  1. Stažení instalačního souboru:
     a. Přihlaš se na Bitdefender Central.
     b. Vyberte menu **Moje Zařízení** a klikněte na **INSTALOVAT OCHRANU**.
     c. Prosím vyberte jednu z následujících variant
        - **Chránit toto zařízení**

          Vyberte tuto možnost a vyberte vlastníka zařízení. Pokud zařízení patří někomu jinému, klepněte na odpovídající tlačítko.
        - **Chránit další zařízení**

          Vyberte tuto možnost a vyberte vlastníka zařízení. Pokud zařízení patří někomu jinému, klepněte na odpovídající tlačítko.

Klikněte na **ODESLAT ODKAZ NA STAŽENÍ**. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Pamatujte, že vygenerovaný odkaz ke stažení je platný pouze 24 hodin. Pokud doba platnosti odkazu vyprší, musíte vygenerovat nový pomocí stejných kroků.

Na zařízení, kde chcete nainstalovat váš Bitdefender produkt Bitdefender, zkontrolujte emailový účet, který jste zadali a poté klikněte na příslušné tlačítko stáhnout

2. Spusťte produkt Bitdefender, který jste stáhli.

Další informace o průběhu instalace produktu Bitdefender viz *„Instalace produktu Bitdefender“* (str. 5).

8.6. Jak mohu aktualizovat Bitdefender na nejnovější verzi?

Od této chvíle je možná aktualizace na nejnovější verzi možná bez provádění ruční procedury odinstalace a opětovné instalace. Přesněji řečeno, nový produkt, včetně nových funkcí a zásadních zlepšení, je doručen skrze produktovou aktualizaci a, pokud máte aktivní Bitdefender předplatné, je automaticky aktivován.

Pokud používáte produkt ve verzi 2020, můžete aktualizovat na nejnovější verzi dle následujících pokynů:

1. V upozornění, které Vám bude doručeno s informacemi o aktualizaci, klikněte na **RESTARTOVAT NYNÍ**. Pokud se Vám nezobrazí, přejděte na okno Upozornění, vyberte poslední nejnovější aktualizaci a poté klikněte na tlačítko **RESTARTOVAT NYNÍ**. Počkejte, až se zařízení restartuje.

   Objeví se okno **Co je nového** s informacemi o zlepšeních a nových funkcích.

2. Kliknutím na odkazy **Více informací** budete přesměrováni na naši speciálně vyhrazenou stránku obsahující více detailních informací a užitečných článků.

3. Zavřete okno **Co je nového** pro přístup k rozhraní nově nainstalované verze produktu.

Uživatelé, kteří si přejí zdarma aktualizovat z Bitdefender 2016 nebo nižší verze na nejnovější verzi produktu Bitdefender, musí odstranit svou stávající verzi přes Ovládací panely a poté si stáhnout nejnovější instalační soubor z webové stránky Bitdefender na následující adrese:

http://www.bitdefender.com/Downloads/. Aktivace je možná pouze s platným předplatným.

9. BITDEFENDER CENTRAL

9.1. Jak se přihlásím z jiného účtu Bitdefender ?

Vytvořili jste si nový účet Bitdefender a od nynějška ho chcete používat.

Pro úspěšné přihlášení pomocí jiného Bitdefender účtu:

1. Klikněte na název účtu v horní části rozhraní Bitdefender .
2. Kliknutím na **Přepnout účet** v pravém horním rohu obrazovky změníte účet propojený se zařízením.
3. Zadejte svou emailovou adresu do příslušného pole a klikněte na tlačítko **Další**.
4. Zadejte heslo a poté klikněte na tlačítko **PŘIHLÁSIT SE**.

Poznámka

Produkt Bitdefender z vašeho zařízení se automaticky změní dle předplatného přidruženého k novému účtu Bitdefender.
POkud k novému účtu Bitdefender není přidružené žádné předplatné nebo ho chcete přenést z předchozího účtu, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

9.2. Jak vypnout pomocné zprávy Bitdefender Central?

Aby jsme vám pomohli porozumět k čemu je která možnost v Bitdefender Central, zobrazí se konzoli pomocné zprávy.

Pokud si přejete přestat zobrazovat tyto typy zpráv:

1. Přihlaš se na Bitdefender Central.
2. Klikněte na ikonu v pravém horním rohu obrazovky.
3. Klikněte na **Můj účet** v rolovacím menu.
4. Klikněte na **Nastavení** v rolovacím menu.
5. Vypnout možnost **Zapnout/Vypnout pomocné zprávy**.

9.3. Zapoměl jsem heslo, které jsem nastavil pro svůj účet Bitdefender. Jak jej resetovat?

Pro nastavení nového hesla pro váš uživatelský účet Bitdefender existují dvě možnosti:

- Z rozhraní produktu Bitdefender:
  1. Klikněte na **Můj účet** v navigačním menu v rozhraní Bitdefender.
  2. Klikněte **Přepnout Účet** ve vrchním pravém rohu obrazovky.

     Objeví se nové okno.
  3. Zadejte svou e-mailovou adresu a klikněte na **DALŠÍ** .

     Objeví se nové okno.
  4. Klikněte na tlačítko **Zapomenuté heslo**.
  5. Klikněte na **DALŠÍ**.
  6. Zkontrolujte svůj e-mailový účet, zadejte bezpečnostní kód, který jste obdrželi a klepněte na tlačítko **DALŠÍ**.

     Můžete také kliknout na **Změnit heslo** v e-mailu, který jsme vám poslali.
  7. Napište nové heslo a poté ho napište ještě jednou Klikněte na tlačítko **Save**.
- Z webového prohlížeče:
  1. Přejděte na adresu: https://central.bitdefender.com.
  2. Klikněte na **PŘIHLÁSIT SE**.
  3. Zadejte svou emailovou adresu, poté klikněte na **DALŠÍ**.
  4. Klikněte na tlačítko **Zapomenuté heslo**.
  5. Klikněte na **DALŠÍ**.
  6. Zkontrolujte váš emailový účet a řiďte se instrukcemi pro nastavení nového hesla pro váš Bitdefender účet.

Pro další přístup k účtu Bitdefender zadejte vaši emailovou adresu a nové heslo, které jste právě nastavili.

9.4. Jak mohu spravovat přihlašovací relace spojené s mým Bitdefender účtem?

Ve Vašem Bitdefender účtu můžete sledovat nejnovější aktivní i neaktivní přihlašovací relace probíhající na zařízeních propojených s Vaším účtem. Navíc se můžete odhlásit vzdáleně provedením následujících kroků:

1. Přihlaš se na Bitdefender Central.
2. Klikněte na ikonu v pravém horním rohu obrazovky.
3. Klikněte na **Relace** v rolovacím menu.
4. V oblasti **Aktivní relace** zvolte možnost **ODHLÁSIT SE** vedle zařízení, na kterém chcete ukončit přihlašovací relaci.

10. SKENOVÁNÍ POMOCÍ PRODUKTU BITDEFENDER

10.1. Jak provést sken souboru nebo složky?

Nejjednodušším způsobem, jak skenovat soubor nebo složku, je kliknout pravým tlačítkem na objekt, který chcete skenovat, vybrat položku Bitdefender a v nabídce zvolit možnost **Skenovat antivirem Bitdefender**.

Dokončete sken podle pokynů průvodce antivirovým skenem. Produkt Bitdefender automaticky provede doporučené činnosti na detekovaných souborech.

Pokud zbývají nějaké nevyřešené hrozby, budete vyzváni k výběru činností, které s nimi budou provedeny.

Mezi obvyklé situace, při kterých je vhodné použít tento způsob skenování, patří následující:

- Máte podezření na infekci určitého souboru nebo složky.
- Kdykoli stáhnete z Internetu soubory, které si myslíte že mohou být nebezpečné.
- Před kopírováním souborů do zařízení naskenujte sdílenou síťovou složku.

10.2. Jak mám provést sken systému?

Chcete-li provést úplnou kontrolu systému:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. Klikněte na tlačítko **Spustit skenování** vedle položky **Kontrola systému** .
4. S pomocí průvodce kompletním skenem dokončete sken. Produkt Bitdefender automaticky provede doporučené činnosti na detekovaných souborech.

   Pokud zbývají nějaké nevyřešené hrozby, budete vyzváni k výběru činností, které s nimi budou provedeny. Další informace viz *„Průvodce antivirovým skenem“* (str. 89).

10.3. Jak mám naplánovat sken?

Bitdefender můžete nastavit tak, aby začal skenovat důležitá umístění systému, pokud nejste v přední části zařízení.

Chcete-li naplánovat kontrolu:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. Klikněte na ••• vedle typu testu, který chcete naplánovat, System Scan nebo Quick Scan, v spodní část rozhraní, poté vyberte **Upravit** .

   Alternativně můžete vytvořit typ skenování podle svých potřeb kliknutím na **+ Vytvořit skenování** vedle **Spravovat skenování** .
4. Přizpůsobte skenování podle svých potřeb a poté klikněte na **Další** .
5. Zaškrtněte políčko vedle **Zvolte, kdy se má úkol naplánovat** .

   Vyberte jednu z odpovídajících možností a nastavte plán:

   - Při spouštění systému
   - Denně
   - Týdně
   - Měsíčně

   Pokud zvolíte možnost Denní, Měsíční nebo Týdenní, přetáhněte jezdec podél stupnice a nastavte požadované časové období, kdy má naplánované skenování začít.

Pokud se rozhodnete vytvořit nové vlastní skenování, zobrazí se okno **Skenovací úloha**. Zde můžete vybrat místa, která chcete skenovat.

10.4. Jak mám vytvořit vlastní sken?

Pokud chcete na svém zařízení skenovat konkrétní umístění nebo konfigurovat možnosti skenování, nakonfigurujte a spusťte přizpůsobenou úlohu skenování.

Vlastní sken nakonfigurujte následujícím způsobem:

1. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
2. Klikněte na **+ Vytvořit Sken** vedle **Spravovat Skeny** .

3. Do pole název úlohy zadejte název testu, vyberte umístění, která chcete prohledat, a poté klikněte na **DALŠÍ** .
4. Konfigurovat tyto možnosti:
   - **Skenovat pouze aplikace**. Můžete nastavit Bitdefender tak, aby skenoval pouze přistupované aplikace.
   - **Priorita skenovací úlohy**. Můžete si vybrat, jaký dopad by měl mít proces kontroly na výkon vašeho systému.
     - Auto - Priorita procesu skenování bude záviset na aktivitě systému. Chcete-li se ujistit, že proces skenování neovlivní aktivitu systému, Bitdefender rozhodne, zda má být proces skenování spuštěn s vysokou nebo nízkou prioritou.
     - Vysoká - priorita skenování bude vysoká. Výběrem této možnosti umožníte, aby ostatní programy běžely pomaleji a aby se zkrátil čas potřebný k dokončení procesu skenování.
     - Nízká - priorita skenování bude nízká. Výběrem této možnosti umožníte, aby ostatní programy běžely rychleji a zvýší čas potřebný pro dokončení kontroly.
   - **Akce po skenování**. Vyberte, jaká akce by měla být provedena Bitdefender v případě, že nebudou nalezeny žádné hrozby.
     - Zobrazit okno s výsledky
     - Vypnout zařízení
     - Zavřít okno skenu
5. Pokud chcete konfigurovat podrobné možnosti skenování, vyberte kartu **Pokročilé nastavení**.

   Klikněte **Další**.
6. Pokud chcete, můžete povolit možnost **Plánovat sken** a poté zvolit, kdy má začít vlastní skenování, které jste vytvořili.
   - Při spouštění systému
   - Denně
   - Měsíčně
   - Týdně

Pokud zvolíte možnost Denní, Měsíční nebo Týdenní, přetáhněte jezdec podél stupnice a nastavte požadované časové období, kdy má naplánované skenování začít.

7. Klepnutím na **Uložit** uložíte nastavení a zavřete konfigurační okno.

   V závislosti na skenovaných oblastech může sken chvíli trvat. Pokud budou během procesu skenování nalezeny hrozby, budete vyzváni k výběru akcí, které mají být provedeny na zjištěných souborech.

Pokud chcete, můžete rychle znovu spustit předchozí vlastní sken kliknutím na příslušnou položku v dostupném seznamu.

10.5. Jak mohu vyloučit složku ze skenování?

Produkt Bitdefender umožňuje vyloučit určité soubory, složky nebo přípony souborů ze skenování.

Výjimky mohou použít uživatelé s pokročilými počítačovými znalostmi a pouze v následujících situacích:

- V systému máte velkou složku, ve které uchováváte filmy a hudbu.
- Máte v systému velký archiv, ve kterém uchováváte různá data.
- Udržujete složku, do které instalujete různé druhy softwaru a aplikací pro účely testování. Skenování složek může mít za následek ztrátu některých dat.

Chcete-li přidat složku do seznamu výjimek:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. Vyberte kartu **Nastavení**.
4. Klikněte na **Spravovat výjimky** .
5. Klikněte na **+ Přidat výjimku** .
6. Do příslušného pole zadejte cestu ke složce, kterou chcete kromě skenování.

   Případně můžete přejít do složky kliknutím na tlačítko Procházet v pravé části rozhraní, vyberte ji a klikněte na **OK** .
7. Zapněte přepínač vedle funkce ochrany, která by neměla prohledávat složku. Existují tři možnosti:

- Antivirus
- Prevence online hrozeb
- Pokročilá Ochrana

8. Kliknutím na tlačítko **Uložit** uložte změny a zavřete okno.

10.6. Co dělat, když produkt Bitdefender detekuje čistý soubor jako infikovaný?

Mohou nastat případy, kdy produkt Bitdefender chybně označí neinfikovaný soubor jako hrozbu (falešná detekce). Pro nápravu této chyby přidejte soubor do oblasti Bitdefender - Výjimky:

1. Vypněte antivirovou ochranu produktu Bitdefender v reálném čase:
   a. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
   b. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
   c. V okně **Pokročilé** vypněte **Bitdefender Štít** .

      Objeví se výstražné okno. Výběr potvrďte zvolením doby, po kterou má být ochrana v reálném čase vypnuta, z nabídky. Ochranu v reálném čase můžete vypnout na 5, 15 nebo 30 minut, na hodinu, trvale nebo do příštího restartu systému.
2. Zobrazení skrytých objektů v systému Windows. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak zobrazím skryté objekty v systému Windows?“* (str. 74).
3. Obnovení souboru z oblasti Karanténa:
   a. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
   b. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
   c. Přejděte do oken **Nastavení** a klikněte na **Spravovat karanténu** .
   d. Vyberte soubor a potom klikněte na **Obnovit** .
4. Přidejte soubor do seznamu výjimek. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak mohu vyloučit složku ze skenování?“* (str. 57).

   Ve výchozím nastavení Bitdefender automaticky přidává obnovené soubory do seznamu výjimek.
5. Zapněte antivirovou ochranu produktu Bitdefender v reálném čase.

6. Kontaktujte zaše zástupce podpory, abychom mohli odstranit signaturu detekce z informační aktualizace. Pokud chcete zjistit jak to udělat, obraťte se na *„Žádost o pomoc“* (str. 206).

10.7. Jak zjistím, jaké viry produkt Bitdefender detekoval?

Při každém skenu je vytvořen protokol skenu a produkt Bitdefender zaznamená zjištěné problémy.

Protokol skenu obsahuje podrobné informace o zaprotokolovaném průběhu skenování, jako možnosti skenu, skenované objekty, nalezené hrozby a činnosti, které byly na tyto hrozby aplikovány.

Protokol skenu můžete otevřít přímo z průvodce skenem, nebo, jakmile je sken dokončen, kliknutím na položku **Zobrazit protokol**.

Chcete-li zkontrolovat záznam skenu nebo detekované infekce později:

1. Klikněte na **Upozornění** v navigačním menu v rozhraní Bitdefender.
2. V záložce **Vše** vyberte notifikaci týkající se posledního skenu.

   Zde můžete najít všechny události skenu proti hrozbám, včetně hrozeb zjištěných skenováním při přístupu, uživatelem spuštěných skenů a změn stavu pro automatické skeny.
3. V seznamu notifikací můžete zjistit, které skeny byly v nedávné době provedeny. Klikněte na notifikaci a zobrazí se podrobnosti o ní.
4. Pokud chcete otevřít protokol skenu, klikněte na položku **Zobrazit protokol**.

11. RODIČOVSKÁ KONTROLA

11.1. Jak mohu chránit své děti před online hrozbami?

Rodičovský poradce produktu Bitdefender vám umožňuje omezit přístup k Internetu a určitým aplikacím, čímž zabráníte dětem v prohlížení nevhodného obsahu, když nejste nablízku.

Pro nastavení Rodičovského Poradce:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **RODIČOVSKÝ KONTROLA** klikněte na **Konfigurovat**.

   Budete přesměrováni na webovou stránku účtu Bitdefender. Přihlaste se pomocí svých přihlašovacích údajů.
3. Dashboard Rodičovské kontroly se zobrazí. Zde můžete prohlížet a konfigurovat nastavení Rodičovské Kontroly.
4. Klikněte na **PŘIDAT DĚTSKÝ PROFIL** .
5. Nastavte konkrétní informace, jako jméno, datum narození nebo pohlaví. Chcete-li přidat obrázek do profilu vašeho dítěte, klikněte na ikonu v pravém dolním rohu možnost **Obrázek profilu**. Pro pokračování klikněte na **ULOŽIT**.

   V závislosti na standardech rozvoje dítěte se nastavením věku dítěte automaticky načtou specifická nastavení pro prohlížení internetu, která jsou pro jeho věkovou kategorii považována za patřičná.
6. Klikněte na **PŘIDAT ZAŘÍZENÍ**.
7. Pokud je na zařízení Vašeho dítěte již nainstalován Bitdefender , vyberte jeho zařízení ze seznamu a poté zvolte účet, který chcete sledovat. KLIKNĚTE NA **PŘIŘADIT**.

   Pokud vaše dítě nemá na zařízení, které používá, nainstalován žádný produkt Bitdefender, klikněte na **Instalovat na nové zařízení** a poté na **Odeslat odkaz ke stažení** . Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Pamatujte, že vygenerovaný odkaz ke stažení je platný pouze 24 hodin. Pokud doba platnosti odkazu vyprší, musíte vygenerovat nový pomocí stejných kroků.

   Na zařízení, kde chcete nainstalovat Bitdefender zkontrolujte emailový účet, který jste zadaly, a poté klikněte na příslušné tlačítko stáhnout.

Důležité
Na zařízeních se systémem Windows a MacOS, která nemají nainstalovaný Bitdefender, bude nainstalován sledovací program Bitdefender Rodičovská Kontrola, který umožní sledovat online aktivity vašich dětí.
Na zařízení se systémem Android a iOS musí být stažena a nainstalována aplikace Bitdefender Rodičovská kontrola.

11.2. Jak mohu zablokovat přístup mého dítěte k webové stránce?

Rodinný poradce produktu Bitdefender vám umožňuje regulovat obsah přístupný vašemu dítěti na jeho zařízení a můžete zablokovat přístup k webové stránce.

Abyste zablokovali přístup k webové stránce, je třeba ji přidat do seznamu výjimek pomocí následujícího postupu:

1. Přejděte na adresu: https://central.bitdefender.com.
2. Přihlaste se k účtu Bitdefender pomocí Vaší emailové adresy a hesla.
3. Kliknutím na položku **Parental Control** přejděte k ovládacímu panelu.
4. Vyberte profil svého dítěte.
5. Klikněte na kartu **MOŽNOSTI** a poté vyberte **Webové stránky** .
6. Klikněte na **SPRAVOVAT** .
7. Do příslušného pole zadejte webovou stránku, kterou chcete zablokovat.
8. Vyberte **Blokovat** .
9. Kliknutím na ikonu uložte změny a poté klikněte na **HOTOVO** .

Poznámka
Omezení mohou být nastavena pouze pro zařízení s operačním systémem Android nebo Windows.

11.3. Jak mohu předejít aby moje dítě nemohlo používat některé aplikace?

Rodičovská Kontrola Bitdefender umožňuje regulovat obsah přístupný vašemu dítěti při používání zařízení.

Pro blokování přístupu k aplikace:

1. Přejděte na adresu: https://central.bitdefender.com.
2. Přihlaste se k účtu Bitdefender pomocí Vaší emailové adresy a hesla.
3. Kliknutím na položku **Parental Control** přejděte k ovládacímu panelu.
4. Vyberte podřízený profil.
5. Klikněte na **MOŽNOSTI** a vyberte **Aplikace**.
6. Zobrazí se seznam se přiřazenými zařízeními.

   Vyberte kartu se zařízením, kterému chcete zakázat přístup k aplikaci.
7. Klikněte na **Spravovat aplikace používané ...**.

   Zobrazí se seznam s nainstalovanými aplikacemi.
8. Vyberte **Blokované** vedle aplikací, které nechcete aby vaše dítě používalo.
9. Kliknutím na tlačítko **ULOŽIT** nastavení aplikujete.

Poznámka
Omezení mohou být nastavena pouze pro zařízení s operačním systémem Android nebo Windows.

11.4. Jak mohu pro své dítě nastavit umístění jako bezpečné nebo omezené?

Rodičovský poradce produktu Bitdefender vám umožní nastavit umístění pro vaše dítě jako bezpečné nebo omezené.

Pro nastavení lokality:

1. Přejděte na adresu: https://central.bitdefender.com.
2. Přihlaste se k účtu Bitdefender pomocí Vaší emailové adresy a hesla.
3. Kliknutím na položku **Parental Control** přejděte k ovládacímu panelu.
4. Vyberte profil svého dítěte.
5. Klikněte na **MOŽNOSTI** a vyberte **Poloha Dítěte**.
6. Klikněte na položku **Zařízení** v rámečku, který vidíte v okně **Poloha dítěte**.
7. Klepněte na zařízení, které chcete konfigurovat.
8. V okně **Areas** klikněte na tlačítko **ADD AREA**.
9. Vyberte typ umístění - **Safe** (Bezpečné) nebo **Restricted** (Omezené).

10. Zadejte platné názvy pro vybrané oblasti, které má nebo nemá vaše dítě oprávnění navštívit.
11. Nastavte rádius, který by měl být sledován, pomocí posuvníku **Radius**.
12. Kliknutím na tlačítko **ADD AREA** uložte nastavení.

Kdykoli chcete nastavit omezenou oblast jako bezpečnou nebo naopak, klikněte na ni a poté klikněte na tlačítko **EDIT AREA**. Podle toho, jakou změnu chcete provést, vyberte možnost **SAFE** nebo **RESTRICTED** a poté klikněte na tlačítko **UPDATE AREA**.

11.5. Jak zablokuji mému dítěti přístup k přiřazeným zařízením v noci během denních aktivit?

Bitdefender Rodičovská Kontrola umožňuje omezit přístup dítěte k přiřazeným zařízením během každodenních aktivit, jako například v době vyučování a v čase, kdy by mělo dělat domácí úkoly a také když by vaše dítě mělo spát.

Pro přidání časového omezení:

1. Přejděte na adresu: https://central.bitdefender.com.
2. Přihlaste se k účtu Bitdefender pomocí Vaší emailové adresy a hesla.
3. Kliknutím na položku **Parental Control** přejděte k ovládacímu panelu.
4. Vyberte profil dítěte, pro které chcete nastavit omezení.
5. Klikněte na **MOŽNOSTI** a vyberte **Screentime** .
6. V oblasti **Plány** klikněte na **Přidat plán** .
7. Zadejte název omezení, které chcete vytvořit (například čas jít spát, domácí úkoly, hodiny tenisu, atd.).
8. Nastavte časový rámec a dny, kdy by měla být omezení uplatněna, a klepnutím na **PŘIDAT PLÁN** nastavení uložte.

11.6. Jak zablokuji mému dítěti přístup k přiřazeným zařízením během dne nebo noci?

Bitdefender Rodičovský Kontrola umožňuje omezit přístup Vašeho dítěte k přiřazeným zařízením během různých časů v průběhu dne.

Pro nastavení denního limitu:

1. Přejděte na adresu: https://central.bitdefender.com.
2. Přihlaste se k účtu Bitdefender pomocí Vaší emailové adresy a hesla.
3. Kliknutím na položku **Parental Control** přejděte k ovládacímu panelu.
4. Vyberte profil dítěte, pro které chcete nastavit omezení.
5. Klikněte na **MOŽNOSTI** a vyberte **Screentime** .
6. V oblasti **Denní časové limity** klikněte na **NASTAVIT DENNÍ ČASOVÉ LIMITY** .
7. Nastavte čas a dny, kdy by měla být omezení uplatněna, a kliknutím na **ULOŽIT ZMĚNY** nastavení uložte.

11.7. Jak odebrat profil dítěte

Pokud chcete odstranit stávající profil dítěte:

1. Přejděte na adresu: https://central.bitdefender.com.
2. Přihlaste se k účtu Bitdefender pomocí Vaší emailové adresy a hesla.
3. Kliknutím na položku **Parental Control** přejděte k ovládacímu panelu.
4. Vyberte podřízený profil, který chcete odstranit.
5. Klikněte na **MOŽNOSTI** a vyberte **Smazat profil** .
6. Potvrďte vaši volbu.

12. PRIVACY PROTECTION

12.1. Jak se ujistím, že jsou moje online transakce zabezpečené?

Aby vaše online peněžní operace zůstaly důvěrné, můžete použít prohlížeč vybavený produktem Bitdefender na ochranu vašich transakcí a aplikací homebankingu.

Bitdefender Safepay™ je zabezpečený internetový prohlížeč navržený pro ochranu informací o vašich kreditních kartách, čísel účtů nebo jiných citlivých dat, která zadáváte při přístupu k různým online službám.

Chcete-li udržet vaši online aktivitu bezpečnou a soukromou:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **Safepay** klikněte na **Nastavení**.
3. V **Safepay** oknech klikněte na **Spustit Safepay** .
4. Kliknutím na tlačítko  zobrazíte **virtuální klávesnici**.

   Virtuální klávesnici použijte při zadávání citlivých údajů, jako vaše hesla.

12.2. Jak s pomocí produktu Bitdefender trvale odstraním soubor?

Pokud chcete trvale odstranit nějaký soubor ze systému, je třeba fyzicky vymazat data z pevného disku.

Bitdefender File Shredder vám pomůže rychle skartovat soubory nebo složky ze zařízení pomocí kontextové nabídky systému Windows podle následujících kroků:

1. Pravým tlačítkem klikněte na soubor nebo složku, které chcete trvale odstranit, vyberte položku Bitdefender a zvolte možnost **Likvidátor souborů**.
2. Klikněte na **Smazat trvale** a potvrďte, že chcete v procesu pokračovat.

   Počkejte, dokud produkt Bitdefender nedokončí likvidaci souborů.
3. Zobrazí se výsledky. Kliknutím na tlačítko **DOKONČIT** ukončíte průvodce.

12.3. Jak mohu ochránit svou webkameru před hackingem?

Můžete nastavit svůj produkt Bitdefender aby povolil nebo blokoval přístup nainstalovaných aplikací k Vaší webkameře podle následujících kroků:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **OCHRANA VIDEO & AUDIO** klikněte na **Nastavení**.
3. Přejděte do okna **Ochrana webové kamery** a zobrazí se seznam aplikací, které požádaly o přístup k vašemu fotoaparátu.
4. Přejděte na aplikaci, kterou chcete povolit nebo zakázat přístup, a poté klikněte na přepínač představovaný videokamerou, který se nachází vedle ní.

   Pro zobrazení informací o tom, co se ostatní uživatelé produktu Bitdefender rozhodli udělat s danou aplikací, klikněte na ikonu . Budete upozorněni pokaždé, když je některá z aplikací ze seznamu zablokována uživateli Bitdefender.

Chcete-li do tohoto seznamu přidat aplikace ručně, klikněte na tlačítko **Přidat aplikaci** a vyberte jednu ze dvou možností.

- Z Windows Store
- Z vašich aplikací

12.4. Jak mohu manuálně obnovit zašifrované soubory, když procesy obnovy selže?

V případě zašifrovaných souborů, které nebylo možno automaticky obnovit, můžete je manuálně obnovit pomocí těchto kroků:

1. Klikněte na **Upozornění** v navigačním menu v rozhraní Bitdefender.
2. V záložce **Vše**, vyberte upozornění ohledně nejnovějších detekovaných chování ransomware, a poté klikněte na **Šifrované Soubory**.
3. Seznam se zašifrovanými soubory se zobrazí.

   Pokračujte kliknutím na **Obnovit soubory** .

4. V případě celého nebo části selhání obnovovacího procesu, musíte vybrat umístěného, kde se dešifrované soubory mohou uložit. Klikněte na **Obnovit polohu** a poté vyberte umístění v počítači.
5. Zobrazí se potvrzovací okno.

   Proces obnovení dokončíte kliknutím na **Dokončit** .

Soubory s následujícími příponami, mohou být obnoveny v případě že jsou zašifrovány:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

13. UŽITEČNÉ INFORMACE

13.1. Jak otestuji své řešení zabezpečení?

Abyste se přesvědčili, že váš produkt Bitdefender správně funguje, doporučujeme provést test Eicar.

Test Eicar vám umožňuje zkontrolovat antivirovou ochranu pomocí bezpečného souboru vyvinutého k tomuto účelu.

Pro otestování vašeho řešení zabezpečení:

1. Stáhněte test z oficiální webové stránky organizace EICARhttp://www.eicar.org/.
2. Klikněte na kartu **Anti-Malware Testfile**.
3. Klikněte na položku **Download** v nabídce nalevo.
4. V oblasti **Download area using the standard protocol http** klikněte na testovací soubor **eicar.com**.
5. Budete informováni, že stránka, na kterou se snažíte vstoupit, obsahuje soubor EICAR-Test-File (není hrozbou).

   Pokud kliknete na položku **I understand the risks, take me there anyway** stahování testu bude zahájeno a vyskakovací okno produktu Bitdefender vás informuje, že byl nalezen virus.

   Kliknutím na položku **Další podrobnosti** získáte další informace o této akci.

Pokud neobdržíte žádnou výstrahu produktu Bitdefender, doporučujeme kontaktovat podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“ (str. 206)*.

13.2. Jak odeberu produkt Bitdefender?

Pokud chcete odstranit váš Bitdefender Internet Security:

- V systému **Windows 7**:
  1. Klikněte na nabídku **Start**, přejděte do **Ovládacích panelů** a dvakrát klikněte na položku **Programy a funkce**.
  2. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.

3. V okně, které se zobrazí, klikněte na **ODSTRANIT**.
4. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

- V systémech **Windows 8 a Windows 8.1**:

1. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
2. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
4. V okně, které se zobrazí, klikněte na **ODSTRANIT**.
5. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

- V systému **Windows 10**:

1. Klikněte na nabídku **Start** a poté na položku Nastavení.
2. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Aplikace**.
3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
4. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.
5. V okně, které se zobrazí, klikněte na **ODSTRANIT**.
6. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

Poznámka
Tento přeinstalační proces trvale vymaže Vaše osobní nastavení.

13.3. Jak odeberu Bitdefender VPN?

Postup odebrání VPN Bitdefender je podobný postupu, který používáte k odebrání dalších programů ze zařízení:

- V systému **Windows 7**:

1. Klikněte na nabídku **Start**, přejděte do **Ovládacích panelů** a dvakrát klikněte na položku **Programy a funkce**.
2. Vyhledejte položku **Bitdefender VPN** a vyberte možnost **Odinstalovat**.

   Počkejte na dokončení odinstalace.

- V systémech **Windows 8 a Windows 8.1**:
  1. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
  2. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
  3. Vyhledejte položku **Bitdefender VPN** a vyberte možnost **Odinstalovat**.

     Počkejte na dokončení odinstalace.
- V systému **Windows 10**:
  1. Klikněte na nabídku **Start** a poté na položku Nastavení.
  2. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Nainstalované aplikace**.
  3. Vyhledejte položku **Bitdefender VPN** a vyberte možnost **Odinstalovat**.
  4. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.

     Počkejte na dokončení odinstalace.

13.4. Jak odstraním Bitdefender rozšíření Anti-tracker ?

V závislosti na používaném webovém prohlížeči postupujte podle následujících kroků, abyste odinstalovali rozšíření Anti-tracker Bitdefender:

- Internet Explorer
  1. Klikněte na tlačítko  vedle vyhledávacího panelu a poté vyberte možnost Spravovat doplňky (add-ons).

     Zobrazí se seznam s nainstalovanými rozšířeními.
  2. Klikněte na Bitdefender Anti-tracker.
  3. V pravém dolním rohu klikněte na **Zakázat**.
- Google Chrome
  1. Vedle vyhledávacího panelu klikněte na .
  2. Vyberte **Další nástroje** a poté **Rozšíření**.

     Zobrazí se seznam s nainstalovanými rozšířeními.

3. Klikněte na **Odebrat** v kartě Anti-Tracker Bitdefender.
4. V okně, které se zobrazí, klikněte na tlačítko **Odebrat**.

- Mozilla Firefox

1. Vedle vyhledávacího panelu klikněte na  .
2. Vyberte **Doplňky** a poté **Rozšíření**.

   Zobrazí se seznam s nainstalovanými rozšířeními.

3. Klikněte na  a poté vyberte **Odebrat**.

13.5. Jak automaticky vypnu zařízení po skončení skenování?

Produkt Bitdefender nabízí více skenů, které můžete použít, abyste zajistili, že váš systém nebude infikovaný hrozbami. V závislosti na hardwarové a softwarové konfiguraci vašeho systému může dokončení skenování celého zařízení trvat delší dobu.

Z tohoto důvodu můžete produkt Bitdefender nakonfigurovat tak, abyvypnul systém, jakmile skončí sken.

Zvažte tento příklad: dokončili jste práci a chcete jít spát. Rádi byste nechali produktem Bitdefender zkontrolovat systém na přítomnost hrozeb.

Vypnutí zařízení po skončení rychlého skenování nebo skenování systému:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít**.
3. V okně **Skeny** klikněte na vedle Rychlé kontroly nebo Kontrola systému a vyberte **Upravit**.
4. Upravte skenování podle svých potřeb a klikněte na **Další**.
5. Zaškrtněte políčko vedle položky **Zvolte, kdy se má úkol naplánovat**, a potom vyberte, kdy se má úloha spustit.

   Pokud zvolíte možnost Denní, Měsíční nebo Týdenní, přetáhněte jezdec podél stupnice a nastavte požadované časové období, kdy má naplánované skenování začít.

6. Klikněte na tlačítko **Save**.

Vypnutí zařízení po skončení vlastního skenování:

1. Klikněte na ••• vedle vlastního skenování, které jste vytvořili.
2. Klikněte na **Další** a poté znovu na **Další**.
3. Zaškrtněte políčko vedle položky **Zvolte, kdy se má úkol naplánovat**, a potom vyberte, kdy se má úloha spustit.
4. Klikněte na tlačítko **Save**.

Pokud nebudou nalezeny žádné hrozby, zařízení se vypne.

Pokud zbývají nějaké nevyřešené hrozby, budete vyzváni k výběru činností, které s nimi budou provedeny. Další informace viz *„Průvodce antivirovým skenem“ (str. 89)*.

13.6. Jak nakonfigurovat produkt Bitdefender, aby používal připojení k Internetu pomocí proxy?

Pokud se vaše zařízení připojuje k internetu přes proxy server, musíte nakonfigurovat Bitdefender s nastavením proxy. Produkt Bitdefender obvykle detekuje a naimportuje nastavení proxy serveru z vašeho systému.

Důležité
Pro domácí připojení k Internetu se obvykle proxy server nepoužívá. Nastavení připojení proxy produktu Bitdefender je zpravidla třeba zkontrolovat a nakonfigurovat, pokud nefungují aktualizace. Pokud se produkt Bitdefender může aktualizovat, konfigurace připojení k Internetu je funkční.

Chcete-li spravovat nastavení proxy:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte **Pokročilou** kartu.
3. Zapněte **Proxy server**.
4. Klikněte na **Změnit proxy**.
5. V nastavení proxy jsou k dispozici dvě možnosti:
   - **Importovat nastavení proxy z výchozího prohlížeče** - nastavení proxy aktuálního uživatele, získaná z výchozího prohlížeče. Pokud proxy server

vyžaduje uživatelské jméno a heslo, musíte je specifikovat v příslušných polích.

> **Poznámka**
> Produkt Bitdefender může importovat nastavení proxy z nejrozšířenějších prohlížečů, včetně nejnovějších verzí prohlížečů Microsoft Edge, Internet Explorer, Mozilla Firefox a Google Chrome.

- **Ruční nastavení proxy** - nastavení proxy, které můžete nakonfigurovat sami. Musí být specifikována následující nastavení:
  - **Adresa** - zadejte IP adresu proxy serveru.
  - **Port** - zadejte port, který produkt Bitdefender použije pro připojení k proxy serveru.
  - **Uživatelské jméno** - zadejte uživatelské jméno rozpoznávané proxy serverem.
  - **Heslo** - zadejte platné heslo pro předtím specifikovaného uživatele.

6. Kliknutím na tlačítko **OK** uložte změny a zavřete okno.

Produkt Bitdefender bude používat dostupná nastavení proxy, dokud se mu nepodaří připojit k Internetu.

13.7. Používám 32bitovou, nebo 64bitovou verzi systému Windows?

Chcete-li zjistit zda máte 32 bit nebo 64 bit operační systém:

- V systému **Windows 7**:
  1. Klikněte na nabídku **Start**.
  2. V nabídce **Start** vyhledejte položku **Počítač**.
  3. Klikněte pravým tlačítkem na položku **Počítač** a vyberte **Vlastnosti**.
  4. V oblasti **Systém** zjistíte informace o vašem systému.
- V systému **Windows 8**:
  1. Na úvodní obrazovce systému Windows vyhledejte položku **Počítač** (můžete např. začít psát „počítač“ přímo na úvodní obrazovce) a poté klikněte pravým tlačítkem na její ikonu.

     Ve **Windows 8.1**, nalezněte **Tento Počítač**.
  2. Dole v nabídce vyberte položku **Vlastnosti**.

3. V ovládacím panelu Systém získáte informace o typu systému.

- V systému **Windows 10**:

  1. Do vyhledávacího pole na hlavním panelu zadejte „Systém“ a klikněte na příslušnou ikonu.
  2. V ovládacím panelu vyhledejte položku Systém pro informace o vašem systému.

13.8. Jak zobrazím skryté objekty v systému Windows?

Tento postup je užitečný v případech, kdy řešíte situaci ohrožení a potřebujete najít a odstranit infikované soubory, které mohou být skryté.

Pomocí následujícího postupu zobrazíte skryté objekty v systému Windows:

1. Klikněte na nabídku **Start** a přejděte do **Ovládacích panelů**.

   V systémech **Windows 8 a Windows 8.1** na úvodní obrazovce vyhledejte položku **Ovládací panely** (například můžete začít psát „ovládací panely“, přímo na úvodní obrazovce) a poté klikněte na její ikonu.
2. Vyberte položku **Možnosti složky**.
3. Přejděte na kartu **Zobrazení**.
4. Vyberte možnost **Zobrazovat skryté soubory a složky**.
5. Zrušte zaškrtnutí políčka **Skrýt příponu souborů známých typů**.
6. Zrušte zaškrtnutí políčka **Skrýt chráněné soubory operačního systému**.
7. Klikněte na tlačítko **Použít** a poté na tlačítko **OK**.

V systému **Windows 10**:

1. Do vyhledávacího pole na hlavním panelu zadejte „zobrazovat skryté soubory a složky“ a klikněte na příslušnou ikonu.
2. Vyberte možnost **Zobrazovat skryté soubory, složky a jednotky**.
3. Zrušte zaškrtnutí políčka **Skrýt příponu souborů známých typů**.
4. Zrušte zaškrtnutí políčka **Skrýt chráněné soubory operačního systému**.
5. Klikněte na tlačítko **Použít** a poté na tlačítko **OK**.

13.9. Jak odinstalovat jiná řešení zabezpečení?

Hlavním účelem používání řešení zabezpečení je poskytovat ochranu a bezpečí vašim datům. Co se však stane, když na stejném systému používáte více než jeden zabezpečovací produkt?

Pokud na stejném zařízení používáte více než jedno řešení zabezpečení, systém se stane nestabilním. Instalační program produktu Bitdefender Internet Security automaticky detekuje jiné zabezpečovací programy a nabídne vám možnost je odinstalovat.

Pokud jste jiná řešení zabezpečení neodebrali během úvodní instalace:

- V systému **Windows 7**:
  1. Klikněte na nabídku **Start**, přejděte do **Ovládacích panelů** a dvakrát klikněte na položku **Programy a funkce**.
  2. Chvíli počkejte, než se zobrazí seznam nainstalovaného softwaru.
  3. Najděte název programu, který chcete odebrat, a vyberte položku **Odinstalovat**.
  4. Počkejte na dokončení procesu odinstalace a poté restartujte systém.
- V systémech **Windows 8 a Windows 8.1**:
  1. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
  2. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
  3. Chvíli počkejte, než se zobrazí seznam nainstalovaného softwaru.
  4. Najděte název programu, který chcete odebrat, a vyberte položku **Odinstalovat**.
  5. Počkejte na dokončení procesu odinstalace a poté restartujte systém.
- V systému **Windows 10**:
  1. Klikněte na nabídku **Start** a poté na položku Nastavení.
  2. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Aplikace**.
  3. Najděte název programu, který chcete odebrat, a vyberte položku **Odinstalovat**.

4. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.
5. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

Pokud se vám nepodaří ze systému odebrat jiné řešení zabezpečení, získejte nástroj pro odinstalace z webových stránek výrobce nebo jej přímo kontaktujte, aby vám poskytl pokyny k odinstalaci.

13.10. Jak mám restartovat do nouzového režimu?

Nouzový režim je diagnostický provozní režim, sloužící zejména k řešení potíží ovlivňujících normální provoz systému Windows. Takové problémy sahají od konfliktu ovladačů po viry znemožňující systému Windows normální start. V nouzovém režimu funguje jenom několik aplikací a systém Windows načte pouze základní ovladače a minimum součástí operačního systému. Proto je většina virů při použití systému Windows v nouzovém režimu neaktivní a lze je snadno odstranit.

Postup spuštění systému Windows v nouzovém režimu:

- V systému **Windows 7**:
  1. Restartujte zařízení.
  2. Před spuštěním systému Windows několikrát stiskněte klávesu **F8**, aby se zobrazila spouštěcí nabídka.
  3. Ve spouštěcí nabídce vyberte položku **Nouzový režim** nebo **Nouzový režim s prací v síti**, pokud chcete mít přístup k Internetu.
  4. Stiskněte klávesu **Enter** a čekejte, dokud se nenačte systém Windows v nouzovém režimu.
  5. Tento postup končí potvrzovací zprávou. Potvrďte souhlas kliknutím na tlačítko **OK**.
  6. Aby se systém Windows spustil normálně, jednoduše ho restartujte.
- V systémech **Windows 8, Windows 8.1 a Windows 10**:
  1. Spusťte **Konfigurace systému** ve Windows současným stisknutím kláves **Windows + R** na klávesnici.
  2. Napište **msconfig** do dialogového okna **Spustit** a poté klikněte na **OK**.
  3. Vyberte kartu **Boot**.
  4. V **Nastavení Boot** vyberte **Bezpečný Boot**.

5. Klikněte na **Sítě** a poté **OK**.
6. Klikněte na **OK** v okně **Konfigurace systému** které vás informuje, že systém musí být restartován, aby bylo možné provést změny, které jste nastavili.

   Váš systém se restartuje v Bezpečném módu se sítí.

Chcete-li restartovat v normálním módu, přepněte se zpět opětovným spuštěním **Systémových operací** a zrušením možnosti **Bezpečný Boot**. Klikněte na **OK** a poté **Restart**. Vyčkejte než se nové nastavení projeví.

SPRÁVA VAŠEHO ZABEZPEČENÍ

14. ANTIVIROVÁ OCHRANA

Bitdefender chrání vaše zařízení před všemi druhy hrozeb (malware, trojské koně, spyware, rootkity atd.). Ochrana, kterou produkt Bitdefender nabízí, je rozdělena do dvou kategorií:

- Skenování při přístupu - brání vstupu nových hrozeb do systému. Produkt Bitdefender např. skenuje v dokumentu aplikace Word známé hrozby, když ho otevřete, a emailovou zprávu při jejím doručení.

  Skenování při přístupu zajišťuje ochranu před hrozbami v reálném čase, a představuje stěžejní součást každého programu pro zabezpečení počítače.

  Důležité
  Chcete-li zabránit napadení zařízení hrozbami, nechte zapnuté **on-access skenování** .

- Manuální skenování - umožňuje detekci a odstranění hrozby, která se již nachází v systému. Jedná se o klasický sken spouštěný uživatelem - vyberete, kterou jednotku, složku nebo soubor má produkt Bitdefender skenovat, a produkt Bitdefender ji na požádání oskenuje.

Bitdefender automaticky naskenuje veškerá vyměnitelná média, která jsou připojena k zařízení, aby bylo zajištěno, že k němu lze bezpečně přistupovat. Další informace viz *„Automatický sken vyjímatelných médií“* (str. 92).

Pokročilí uživatelé mohou nakonfigurovat výjimky ze skenování, pokud nechtějí skenovat konkrétní soubory nebo typy souborů. Další informace viz *„Konfigurace výjimek skenování“* (str. 94).

Když produkt Bitdefender nalezne hrozbu, automaticky se pokusí odstranit škodlivý kód z infikovaného souboru a rekonstruovat původní soubor. Tato operace se označuje jako dezinfekce. Soubory, které nelze dezinfikovat, budou přesunuty do karantény, která bude infekci zadržovat. Další informace viz *„Správa souborů v karanténě“* (str. 96).

Pokud bylo zařízení infikováno hrozbami, přejděte na stránku *„Odstranění hrozeb z vašeho systému“* (str. 198). Aby vám zařízení pomohlo vyčistit hrozby, které nelze odstranit z operačního systému Windows, poskytuje produkt Bitdefender *„Rescue Environment“* (str. 198). Toto je důvěryhodné prostředí, speciálně navržené pro odstraňování hrozeb, které vám umožní spustit

zařízení nezávisle na systému Windows. Když zařízení běží v Rescue Environment, hrozby Windows jsou neaktivní, což usnadňuje jejich odstranění.

14.1. Skenování při přístupu (ochrana v reálném čase)

Bitdefender zajišťuje ochranu před širokou škálou hrozeb v reálném čase prostřednictvím skenování všech souborů a emailových zpráv, ke kterým přistupujete.

14.1.1. Zapnutí nebo vypnutí ochrany v reálném čase

Chcete-li zapnout nebo vypnout ochranu proti malware v reálném čase:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. V okně **Pokročilé** zapněte nebo vypněte **Bitdefender Štít** .
4. Pokud chcete ochranu v reálném čase vypnout, objeví se výstražné okno. Výběr potvrďte zvolením doby, po kterou má být ochrana v reálném čase vypnuta, z nabídky. Ochranu v reálném čase můžete vypnout na 5, 15 nebo 30 minut, na hodinu, trvale nebo do příštího restartu systému. Ochrana v reálném čase se automaticky zapne, když uplyne zvolený čas.

Varování
Jde o kritický bezpečnostní problém. Doporučujeme nevypínat ochranu v reálném čase na delší než nutnou dobu. Když je ochrana v reálném čase vypnutá, nebudete chráněni před hrozbami.

14.1.2. Rozšířená nastavení konfigurace ochrany v reálném čase

Pokročilí uživatelé mohou využít výhody nastavení skenování, kterou produkt Bitdefender nabízí. Nastavení ochrany v reálném čase můžete podrobně nastavit vytvořením vlastní úrovně ochrany.

Chcete-li konfigurovat nastavení ochrany v reálném čase:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. V okně **Pokročilé** můžete podle potřeby konfigurovat nastavení skenování.

Informace o možnostech skenu

Tyto informace pro vás mohou být užitečné:

- **Skenovat pouze aplikace.** Můžete nastavit Bitdefender tak, aby skenoval pouze přistupované aplikace.
- **Skenovat pro potenciálně nežádoucí aplikace.** Vyberte tuto možnost pro skenování na nežádoucí aplikace. Potenciálně nežádoucí aplikace (PUA) nebo potenciálně nežádoucí program (PUP) je software, který je obvykle součástí freewarového softwaru, a bude spouštět vyskakovací okna nebo nainstaluje panel nástrojů do výchozího prohlížeče. Některé změní domovskou stránku nebo vyhledávač, jiné spustí několik procesů na pozadí, zpomalujících tak výkon PC, nebo zobrazují početné reklamy. Tyto programy se mohou nainstalovat bez vašeho souhlasu (jsou známé také jako adware), nebo mohou být obsaženy v původní expresní instalační sadě (podporované reklamou).
- **Skenování skriptů.** Funkce Skenování skriptů umožňuje Bitdefender skenovat skripty powershell a kancelářské dokumenty, které by mohly obsahovat malware založený na skriptech.
- **Skenovat síťové složky.** Chcete-li ze zařízení bezpečně přistupovat ke vzdálené síti, doporučujeme ponechat možnost Skenovat síťové sdílené položky povolenou.
- **Testovat archivy.** Skenování uvnitř archivů je pomalý proces náročný na prostředky, který proto není doporučen pro ochranu v reálném čase. Archivy obsahující infikované soubory nepředstavují pro zabezpečení vašeho systému bezprostřední hrozbu. Hrozba může ovlivňovat váš systém, pouze pokud je infikovaný soubor z archivu extrahován a spuštěn bez zapnuté ochrany v reálném čase.

  Pokud se rozhodnete použít tuto možnost, zapněte ji a přetáhněte jezdec podél měřítka, abyste vyloučili skenování archivů, které jsou VĚTŠÍ než zadaná hodnota v MB (megabajtech).
- **Skenovat spouštěcí sektory.** Produkt Bitdefender lze nastavit, aby skenoval spouštěcí sektory pevného disku. Tento sektor pevného disku obsahuje počítačový kód nezbytný k zahájení spouštěcího procesu. Když virus infikuje spouštěcí sektor, jednotka se může stát nepřístupnou a nemusí být možné spustit systém a přistupovat k datům.

- **Skenovat pouze nové a změněné soubory.** Skenováním pouze nových a změněných souborů výrazně zlepšíte celkovou reakci systému s minimálními ústupky v oblasti zabezpečení.
- **Skenování keyloggerů.** Tuto možnost vyberte, pokud chcete v systému skenovat přítomnost aplikací typu keylogger. Keyloggery zaznamenávají, co píšete na klávesnici, a odesílají po Internetu zprávy osobě se zlými úmysly (hackerovi). Hacker může ze zcizených dat získat citlivé informace, jako čísla účtů a hesla, a použít je k vlastnímu prospěchu.
- **Rychlý bootovací sken.** Vyberte **Kontrola při Bootu** ke kontrole vašeho systému před tím než se načtou kritické služby. Cílem této funkce je zlepšit detekci virů při startu systému a dobu spouštění systému.

Činnosti prováděné s nalezenými hrozbami

Můžete nastavit činnosti prováděné ochranou v reálném čase pomocí následujících pokynů:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. V okně **Pokročilé** přejděte v okně dolů, dokud neuvidíte možnost **Akce ohrožení** .
4. Nakonfigurujte nastavení skenu dle potřeby.

Ochrana produktu Bitdefender v reálném čase může provádět následující činnosti:

Provést vhodné akce

Produkt Bitdefender provede doporučené činnosti v závislosti na typu detekovaného souboru:

- **Počet infikovaných souborů.** Soubory detekované jako infikované shodující se s informacemi o ohrožení, které se nacházejí v databázi informací o hrozbách produktu Bitdefender Bitdefender se automaticky pokusí odstranit škodlivý kód z infikovaného souboru a rekonstruovat původní soubor. Tato operace se označuje jako dezinfekce.

  Soubory, které nelze dezinfikovat, budou přesunuty do karantény, která bude infekci zadržovat. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Další informace viz *„Správa souborů v karanténě“* (str. 96).

Důležité
V případě některých druhů hrozeb není dezinfekce možná, protože detekovaný soubor je celý škodlivý. V takových případech bude infikovaný soubor z disku odstraněn.

- **Podezřelé soubory.** Soubory detekuje jako podezřelé heuristická analýza. Podezřelé soubory nelze dezinfikovat, protože není k dispozici žádná dezinfekční rutina. Budou přesunuty do karantény, aby bylo zamezeno potenciální infekci.

  Ve výchozím stavu jsou soubory z karantény automaticky odesílány do laboratoří společnosti Bitdefender, aby je analyzovali pracovníci výzkumu malwaru společnosti Bitdefender. Jakmile je potvrzena přítomnost hrozby, následuje vydání aktualizace informací o hrozbě pro umožnění jejího odstranění.

- **Archivy obsahující infikované soubory.**
  - Archivy, které obsahují pouze infikované soubory, jsou automaticky odstraněny.
  - Pokud archiv obsahuje infikované i čisté soubory, produkt Bitdefender se pokusí odstranit infikované soubory, za předpokladu, že může rekonstruovat archiv s čistými soubory. Jestliže rekonstrukce archivu není možná, budete informováni, že nelze provést žádnou akci, aby nedošlo ke ztrátě čistých souborů.

Přesunout do karantény
Přesune nalezené soubory do karantény. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Další informace viz *„Správa souborů v karanténě“* (str. 96).

Odepřít přístup
V případě, že je zjištěn infikovaný soubor, přístup k němu bude odepřen.

14.1.3. Obnovení výchozích nastavení

Ve výchozím stavu zajišťují nastavení ochrany v reálném čase dobrou ochranu před hrozbami, s minimálním dopadem na výkon systému.

Chcete-li obnovit nastavení ochrany v reálném čase:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .

3. V okně **Pokročilé** přejděte v okně dolů, dokud neuvidíte možnost **Obnovit pokročilá nastavení** . Vyberte tuto možnost pro obnovení antivirových nastavení do výchozího stavu.

14.2. Manuální skenování

Hlavním cílem služby Bitdefender je udržovat zařízení v čistotě před hrozbami. To se provádí tak, že se na vašem zařízení nevyskytují nové hrozby a skenují se vaše e-mailové zprávy a všechny nové soubory stažené nebo zkopírované do vašeho systému.

Existuje riziko, že v systému je usazený virus už předtím, než vůbec nainstalujete produkt Bitdefender. Z tohoto důvodu je po instalaci Bitdefender vhodné zkontrolovat, zda se v zařízení nevyskytují rezidentní hrozby. A je to určitě dobrý nápad často kontrolovat zařízení, zda neobsahuje hrozby.

Manuální skenování je založeno na skenovacích úlohách. Skenovací úlohy specifikují možnosti skenování a skenované objekty. Zařízení můžete prohledávat kdykoli chcete spuštěním výchozích úkolů nebo vlastních úkolů skenování (uživatelem definované úlohy). Pokud chcete na svém zařízení skenovat konkrétní umístění nebo konfigurovat možnosti skenování, nakonfigurujte a spusťte vlastní skenování.

14.2.1. Skenování na hrozby v souboru nebo složce

Soubory a složky byste měli skenovat, kdykoli máte podezření, že jsou infikované. Pravým tlačítkem klikněte na soubor nebo složku, které chcete skenovat, vyberte položku **Bitdefender** a zvolte možnost **Skenovat antivirem Bitdefender**. Zobrazí se průvodce antivirovým skenem, který vás provede průběhem skenování. Na konci skenu budete vyzváni k výběru činností, které budou provedeny s případnými nalezenými soubory.

14.2.2. Provedení rychlého skenu

Rychlý sken používá k nalezení hrozeb ve vašem systému cloudovou detekci. Provedení rychlého skenu obvykle trvá méně než minutu a využije jen zlomek systémových prostředků, které potřebuje běžný sken.

Chcete-li spustit rychlou kontrolu:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .

3. V oknech **Skeny** klikněte na tlačítko **Spustit Sken** vedle **Rychlý Sken** .
4. Dokončete sken pomocí průvodce antivirovým skenem. Produkt Bitdefender automaticky provede doporučené činnosti na detekovaných souborech. Pokud zbývají nějaké nevyřešené hrozby, budete vyzváni k výběru činností, které s nimi budou provedeny.

14.2.3. Provedení kompletního skenu

Úloha Kontrola systému prohledává celé zařízení, zda neobsahuje všechny typy hrozeb ohrožujících jeho zabezpečení, například malware, spyware, adware, rootkity a další.

Poznámka
Protože **kompletní sken** provádí důkladné skenování celého systému, může chvíli trvat. Proto se doporučuje tuto úlohu spustit, když zařízení nepoužíváte.

Před spuštěním kompletního skenu doporučujeme provést následující:

- Ujistěte se, že je Bitdefender aktuální současně se svou informační databází o hrozbách. Skenování zařízení pomocí zastaralé databáze informací o hrozbách může zabránit Bitdefender v detekci nových hrozeb nalezených od poslední aktualizace. Další informace viz *„Aktualizace produktu Bitdefender“* (str. 39).
- Ukončete všechny spuštěné programy.

Pokud chcete na svém zařízení skenovat konkrétní umístění nebo konfigurovat možnosti skenování, nakonfigurujte a spusťte vlastní skenování. Další informace viz *„Konfigurace vlastního skenu“* (str. 86).

Chcete-li spustit Systémový sken:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. V oknech **Skeny** klikněte na tlačítko **Spustit Sken** vedle **System Sken** .
4. Poprvé, když spustíte sken systému, je vám představena tato funkce. Chcete-li pokračovat, klikněte na **Ok, mám to**
5. Dokončete sken pomocí průvodce antivirovým skenem. Produkt Bitdefender automaticky provede doporučené činnosti na detekovaných

souborech. Pokud zbývají nějaké nevyřešené hrozby, budete vyzváni k výběru činností, které s nimi budou provedeny.

14.2.4. Konfigurace vlastního skenu

V okně **Spravovat skenování** můžete nastavit Bitdefender pro spuštění prověřování, kdykoli se domníváte, že vaše zařízení potřebuje kontrolu potenciálních hrozeb. Můžete si naplánovat Sytémový sken nebo Rychlé skenování , nebo můžete vytvořit vlastní skenování dle svých potřeb.

Chcete-li nakonfigurovat detaily nového vlastního skenu:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. V oknech **Skeny** klikněte na **+Vytvořit sken** .
4. Do pole **Název úlohy** zadejte název skenu, poté vyberte umístění, která chcete prohledat, a poté klikněte na **Další**.
5. Konfigurovat tyto možnosti:
   - **Skenovat pouze aplikace**. Můžete nastavit Bitdefender tak, aby skenoval pouze přistupované aplikace.
   - **Priorita skenovací úlohy**. Můžete si vybrat, jaký dopad by měl mít proces kontroly na výkon vašeho systému.
     - Auto - Priorita procesu skenování bude záviset na aktivitě systému. Chcete-li se ujistit, že proces skenování neovlivní aktivitu systému, Bitdefender rozhodne, zda má být proces skenování spuštěn s vysokou nebo nízkou prioritou.
     - Vysoká - priorita skenování bude vysoká. Výběrem této možnosti umožníte, aby ostatní programy běžely pomaleji a aby se zkrátil čas potřebný k dokončení procesu skenování.
     - Nízká - priorita skenování bude nízká. Výběrem této možnosti umožníte, aby ostatní programy běžely rychleji a zvýší čas potřebný pro dokončení kontroly.
   - **Akce po skenování**. Vyberte, jaká akce by měla být provedena Bitdefender v případě, že nebudou nalezeny žádné hrozby.
     - Zobrazit okno s výsledky
     - Vypnout zařízení

- Zavřít okno skenu

6. Pokud chcete konfigurovat podrobné možnosti skenování, vyberte kartu **Pokročilé nastavení**. Informace o uvedených skenech naleznete na konci této sekce.

   Klikněte **Další**.

7. Pokud chcete, můžete povolit **Plánování skenu** a pak zvolit, kdy má začít vlastní skenování, které jste vytvořili.

   - Při spouštění systému
   - Denně
   - Měsíčně
   - Týdně

   Pokud zvolíte možnost Denní, Měsíční nebo Týdenní, přetáhněte jezdec podél stupnice a nastavte požadované časové období, kdy má naplánované skenování začít.

8. Klepnutím na **Uložit** uložíte nastavení a zavřete konfigurační okno.

   V závislosti na skenovaných oblastech může sken chvíli trvat. Pokud budou během procesu skenování nalezeny hrozby, budete vyzváni k výběru akcí, které mají být provedeny na zjištěných souborech.

Informace o možnostech skenu

Tyto informace pro vás mohou být užitečné:

- Pokud neznáte některé termíny, podívejte se na ně ve významovém slovníku. Užitečné informace můžete najít také pomocí Internetu.
- **Skenovat pro potenciálně nežádoucí aplikace.** Vyberte tuto možnost pro skenování na nežádoucí aplikace. Potenciálně nežádoucí aplikace (PUA) nebo potenciálně nežádoucí program (PUP) je software, který je obvykle součástí freewarového softwaru, a bude spouštět vyskakovací okna nebo nainstaluje panel nástrojů do výchozího prohlížeče. Některé změní domovskou stránku nebo vyhledávač, jiné spustí několik procesů na pozadí, zpomalujících tak výkon PC, nebo zobrazují početné reklamy. Tyto programy se mohou nainstalovat bez vašeho souhlasu (jsou známé také jako adware), nebo mohou být obsaženy v původní expresní instalační sadě (podporované reklamou).

- **Testovat archivy.** Archivy obsahující infikované soubory nepředstavují pro zabezpečení vašeho systému bezprostřední hrozbu. Hrozba může ovlivňovat váš systém, pouze pokud je infikovaný soubor z archivu extrahován a spuštěn bez zapnuté ochrany v reálném čase. Doporučujeme však tuto možnost použít, aby byly detekovány a odstraněny všechny potenciální hrozby, i když nejsou bezprostřední.

  Přetáhněte jezdec podél měřítka, abyste vyloučili skenování archivů, které jsou vetší než zadaná hodnota v MB (megabajtech).

  Poznámka
  Skenování archivovaných souborů zvyšuje celkovou dobu skenu a vyžaduje více systémových prostředků.

- **Skenovat pouze nové a změněné soubory.** Skenováním pouze nových a změněných souborů výrazně zlepšíte celkovou reakci systému s minimálními ústupky v oblasti zabezpečení.
- **Skenovat spouštěcí sektory.** Produkt Bitdefender lze nastavit, aby skenoval spouštěcí sektory pevného disku. Tento sektor pevného disku obsahuje počítačový kód nezbytný k zahájení spouštěcího procesu. Když virus infikuje spouštěcí sektor, jednotka se může stát nepřístupnou a nemusí být možné spustit systém a přistupovat k datům.
- **Skenovat paměť.** Tuto možnost použijte ke skenování programů běžících v paměti systému.
- **Skenovat registr.** Tuto možnost použijte ke skenování klíčů registru. Registr systému Windows je databáze, která uchovává nastavení konfigurací a možností pro součásti operačního systému Windows i pro nainstalované aplikace.
- **Skenovat cookies.** Tuto možnost vyberte, chcete-li skenovat soubory cookie uložené prohlížečem v zařízení.
- **Skenování keyloggerů.** Tuto možnost vyberte, pokud chcete v systému skenovat přítomnost aplikací typu keylogger. Keyloggery zaznamenávají, co píšete na klávesnici, a odesílají po Internetu zprávy osobě se zlými úmysly (hackerovi). Hacker může ze zcizených dat získat citlivé informace, jako čísla účtů a hesla, a použít je k vlastnímu prospěchu.

14.2.5. Průvodce antivirovým skenem

Kdykoli spustíte manuální sken (např. kliknutím pravým tlačítkem na složku, výběrem položky Bitdefender a zvolením možnosti **Skenovat antivirem Bitdefender**), objeví se průvodce antivirovým skenem produktu Bitdefender. Sken dokončete podle pokynů průvodce.

Poznámka

Pokud se průvodce skenem nezobrazí, sken může být nakonfigurovaný na skrytý režim běžící na pozadí. Hledejte ikonu průběhu skenu v oznamovací oblasti. Kliknutím na tuto ikonu zobrazíte okno skenu, kde můžete sledovat jeho průběh.

1. krok - provedení skenu

Produkt Bitdefender začne skenovat vybrané objekty. V reálném čase se zobrazují informace o stavu skenu a statistika (včetně uplynulé doby, odhadu zbývající doby a počtu nalezených hrozeb).

Počkejte, až produkt Bitdefender dokončí sken. V závislosti na složitosti skenu může skenování trvat delší dobu.

Zastavení nebo pozastavení skenu. Sken můžete kdykoli zastavit tlačítkem **Zrušit**. Přejdete přímo k poslednímu kroku průvodce. Pokud chcete průběh skenu dočasně pozastavit, klikněte na tlačítko **Pozastavit**. Ve skenování můžete pokračovat kliknutím na tlačítko **Pokračovat**.

Archivy chráněné heslem . Když je detekován archiv chráněný heslem, v závislosti na nastavení skenu můžete být vyzváni k poskytnutí hesla. Archivy chráněné heslem nemohou být bez poskytnutí hesla skenovány. K dispozici jsou následující možnosti:

- **Heslo.** Pokud chcete, aby produkt Bitdefender archiv oskenoval, vyberte tuto možnost a zadejte heslo. Jestliže heslo neznáte, vyberte jednu z ostatních možností.
- **Neptat se na heslo a přeskočit tuto položku ze skenování.** Výběrem této možnosti přeskočíte skenování tohoto archivu.
- **Přeskočit při skenování všechny položky chráněné heslem.** Tuto možnost zvolte, pokud nechcete být obtěžováni archivy chráněnými heslem. Produkt Bitdefender je nebude moci oskenovat, ale v protokolu skenu bude uchován záznam.

Vyberte požadovanou možnost a kliknutím na **OK** pokračujte ve skenu.

2. krok - výběr akcí

Na konci skenu budete vyzváni k výběru činností, které budou provedeny s případnými nalezenými soubory.

Poznámka

Když spustíte rychlý nebo systémový sken, Bitdefender bude s nalezenými soubory automaticky provádět doporučené akce. Pokud zbývají nějaké nevyřešené hrozby, budete vyzváni k výběru činností, které s nimi budou provedeny.

Infikované soubory se zobrazují ve skupinách, v závislosti na hrozbách, kterými jsou infikovány. Kliknutím na odkaz odpovídající hrozbě získáte další informace o infikovaných objektech.

Můžete zvolit obecnou akci, která se provede v případě všech problémů, nebo můžete zvolit samostatné akce pro každou skupinu problémů. V nabídce se může zobrazit jedna nebo více z následujících možností:

Provést vhodné akce

Produkt Bitdefender provede doporučené činnosti v závislosti na typu detekovaného souboru:

- **Počet infikovaných souborů.** Soubory detekované jako infikované shodující se s informacemi o ohrožení, které se nacházejí v databázi informací o hrozbách produktu Bitdefender Bitdefender se automaticky pokusí odstranit škodlivý kód z infikovaného souboru a rekonstruovat původní soubor. Tato operace se označuje jako dezinfekce.

  Soubory, které nelze dezinfikovat, budou přesunuty do karantény, která bude infekci zadržovat. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Další informace viz *„Správa souborů v karanténě“ (str. 96)*.

  ### Důležité

  V případě některých druhů hrozeb není dezinfekce možná, protože detekovaný soubor je celý škodlivý. V takových případech bude infikovaný soubor z disku odstraněn.

- **Podezřelé soubory.** Soubory detekuje jako podezřelé heuristická analýza. Podezřelé soubory nelze dezinfikovat, protože není k dispozici

žádná dezinfekční rutina. Budou přesunuty do karantény, aby bylo zamezeno potenciální infekci.

Ve výchozím stavu jsou soubory z karantény automaticky odesílány do laboratoří společnosti Bitdefender, aby je analyzovali pracovníci výzkumu malwaru společnosti Bitdefender. Jakmile je potvrzena přítomnost hrozby, následuje vydání aktualizace informací o hrozbě pro umožnění jejího odstranění.

- **Archivy obsahující infikované soubory.**
  - Archivy, které obsahují pouze infikované soubory, jsou automaticky odstraněny.
  - Pokud archiv obsahuje infikované i čisté soubory, produkt Bitdefender se pokusí odstranit infikované soubory, za předpokladu, že může rekonstruovat archiv s čistými soubory. Jestliže rekonstrukce archivu není možná, budete informováni, že nelze provést žádnou akci, aby nedošlo ke ztrátě čistých souborů.

Odstranit

Odstraní všechny nalezené soubory z disku.

Pokud jsou infikované soubory nalezeny v archivu společně s čistými, produkt Bitdefender se pokusí odstranit infikované soubory a rekonstruovat archiv s čistými soubory. Jestliže rekonstrukce archivu není možná, budete informováni, že nelze provést žádnou akci, aby nedošlo ke ztrátě čistých souborů.

Nedělat nic

S nalezenými soubory nebude provedena žádná akce. Po dokončení skenu můžete otevřít protokol skenu a podívat se na informace o těchto souborech.

Kliknutím na tlačítko **Pokračovat** aplikujete specifikované akce.

3. krok - souhrn

Když produkt Bitdefender dokončí opravu problémů, v novém okně se zobrazí výsledky skenu. Pokud se chcete podívat na podrobné informace o průběhu skenu, klikněte na položku **Zobrazit protokol** a zobrazí se protokol skenu.

Důležité

Ve většině případů produkt Bitdefender úspěšně vyčistí infikované soubory nebo infekci izoluje. Některé problémy však nelze vyřešit automaticky. Pokud

je to nutné, restartujte systém, aby se proces čištění dokončil. Další informace a pokyny o ručním odstranění hrozby najdete v části *„Odstranění hrozeb z vašeho systému“* (str. 198).

14.2.6. Kontrola protokolů skenů

Při každém skenu je vytvořen protokol skenu a produkt Bitdefender zaznamená zjištěné problémy v okně antiviru. Protokol skenu obsahuje podrobné informace o zaprotokolovaném průběhu skenování, jako možnosti skenu, skenované objekty, nalezené hrozby a činnosti, které byly na tyto hrozby aplikovány.

Protokol skenu můžete otevřít přímo z průvodce skenem, nebo, jakmile je sken dokončen, kliknutím na položku **Zobrazit protokol**.

Chcete-li zkontrolovat záznam skenu nebo detekované infekce později:

1. Klikněte na **Upozornění** v navigačním menu v rozhraní Bitdefender.
2. V záložce **Vše** vyberte notifikaci týkající se posledního skenu.

   Zde můžete najít všechny události skenu proti hrozbám, včetně hrozeb zjištěných skenováním při přístupu, uživatelem spuštěných skenů a změn stavu pro automatické skeny.
3. V seznamu notifikací můžete zjistit, které skeny byly v nedávné době provedeny. Klikněte na notifikaci a zobrazí se podrobnosti o ní.
4. Pokud chcete otevřít protokol skenu, klikněte na položku **Zobrazit protokol**.

14.3. Automatický sken vyjímatelných médií

Bitdefender automaticky detekuje, když k zařízení připojíte vyměnitelné úložné zařízení a naskenuje ho na pozadí, když je povolena možnost Autoscan. Doporučuje se, aby se zabránilo napadení zařízení hrozbami.

Detekovaná zařízení spadají do jedné z následujících kategorií:

- Disky CD/DVD
- Paměťová zařízení USB, jako flashdisky a externí pevné disky
- namapované (vzdálené) síťové jednotky

Automatický sken můžete nakonfigurovat samostatně pro každou kategorii paměťových zařízení. Automatický sken namapovaných síťových jednotek je ve výchozím stavu vypnutý.

14.3.1. Jak to funguje?

Když je detekováno vyjímatelné paměťové zařízení, produkt Bitdefender ho začne skenovat na přítomnost hrozeb (pokud je pro daný typ zařízení povoleno automatické skenování). Budete prostřednictvím vyskakovacího okna informováni, že bylo detekováno a skenuje se nové zařízení.

Ikona skenování produktem Bitdefender se objeví v oznamovací oblasti. Kliknutím na tuto ikonu zobrazíte okno skenu, kde můžete sledovat jeho průběh.

Když je sken dokončen, zobrazí se okno s výsledky skenu, které vás informuje, že soubory na vyjímatelném médiu jsou bezpečné.

Ve většině případů produkt Bitdefender automaticky odstraní nalezené hrozby a izoluje infikované soubory do karantény. Pokud po skenu existují nějaké nevyřešené hrozby, budete vyzváni k výběru činností, které s nimi budou provedeny.

Poznámka

Vezměte v úvahu, že s infikovanými nebo podezřelými soubory na discích CD/DVD nelze provést žádnou akci.. Obdobně platí, že nelze provést žádnou akci s infikovanými nebo podezřelými soubory na namapovaných síťových jednotkách, pokud nemáte příslušná oprávnění.

Tyto informace mohou být pro vás užitečné:

- Při použití disků infikovaných CD/DVD buďte opatrní, protože hrozbu z disku nelze odstranit (médium je určeno pouze ke čtení). Abyste zabránili rozšíření ohrožení do vašeho systému, ujistěte se, že je zapnutá ochrana v reálném čase. Je osvědčeným postupem zkopírovat z disku případná hodnotná data do systému, a poté disk zlikvidovat.
- V některých případech produkt Bitdefender nebude schopen z určitých souborů odstranit hrozby z důvodu zákonných nebo technických překážek. Takovým příkladem jsou soubory používající proprietární technologie (proto nelze archiv vytvořit správně).

  Pro zjištění jak se vypořádat s hrozbami, obraťte se na *„Odstranění hrozeb z vašeho systému“* (str. 198).

14.3.2. Správa skenů vyjímatelných médií

Chcete-li automaticky skenovat vyměnitelná média:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. Vyberte okno **Nastavení** .

Možnosti skenování jsou předkonfigurovány tak, aby dosahovaly nejlepších výsledků detekce. V případě nalezení infikovaných souborů se produkt Bitdefender pokusí o jejich vyléčení (odstranění škodlivého kódu) nebo je přesune do karantény. Pokud obě akce selžou, průvodce antivirovým skenem vám umožní určit jiné akce, které se mají s infikovanými soubory provést. Možnosti skenu jsou standardní a nelze je měnit.

Aby byla zajištěna co nejlepší ochrana, doporučujeme ponechat zapnuté **Automatické skenování** pro všechny druhy vyjímatelných paměťových zařízení.

14.4. Skenovat soubor hosts

Soubor hosts je dodáván standardně s instalací operačního systému a slouží k mapování názvů hostitelů na IP adresy při každém přístupu na novou webovou stránku, připojení k FTP nebo na jiné internetové servery. Je to prostý textový soubor a škodlivé programy jej mohou modifikovat. Zkušení uživatelé vědí, jak ji použít k blokování otravných reklam, bannerů, cookies třetích stran nebo hijackers.

Chcete-li konfigurovat skenování souboru hosts:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte **Pokročilou** kartu.
3. Zapněte nebo vypněte **Skenovat soubor hosts**.

14.5. Konfigurace výjimek skenování

Produkt Bitdefender umožňuje vyloučit určité soubory, složky nebo přípony souborů ze skenování. Tato funkce má za cíl předcházet rušení vaší práce a může rovněž pomoci zlepšit výkon systému. Výjimky mohou používat uživatelé s pokročilými počítačovými znalostmi, nebo v opačném případě mohou následovat doporučení zástupce společnosti Bitdefender.

Výjimky lze nakonfigurovat tak, aby se uplatnily pouze při skenech při přístupu, při manuálních skenech nebo při obou druzích skenů. Objekty

vyloučené ze skenu při přístupu nebudou skenovány, bez ohledu na to, zda k nim přistupujete vy nebo nějaká aplikace.

Poznámka

Výjimky se nevztahují na kontextové skenování. Kontextové skenování je druhem manuálního skenu: kliknete pravým tlačítkem na soubor nebo složku, které chcete skenovat, a zvolíte možnost **Skenovat antivirem Bitdefender**.

14.5.1. Vyloučení souborů a složek ze skenování

Pro vyloučení konkrétních souborů a složek ze skenování:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. V okně **Nastavení** klikněte na **Spravovat výjimky** .
4. Klikněte na **+ Přidat výjimku** .
5. Do příslušného pole zadejte cestu ke složce, kterou chcete kromě skenování.

   Případně můžete přejít do složky kliknutím na tlačítko Procházet v pravé části rozhraní, vyberte ji a klikněte na **OK** .
6. Zapněte přepínač vedle funkce ochrany, která by neměla prohledávat složku. Existují tři možnosti:
   - Antivirus
   - Prevence online hrozeb
   - Pokročilá Ochrana
7. Kliknutím na tlačítko **Uložit** uložte změny a zavřete okno.

14.5.2. Vyloučení přípon souborů ze skenování

Pokud vyjmete z kontroly příponu souboru, Bitdefender již nebude skenovat soubory s touto příponou, bez ohledu na jejich umístění v zařízení. Vyloučení se vztahuje i na soubory na vyjímatelných médiích, jako disky CD, DVD, paměťová zařízení USB nebo síťové jednotky.

Důležité

Při vyjímání rozšíření ze skenování buďte opatrní, protože takové výjimky mohou ohrozit vaše zařízení vůči hrozbám.

Chcete-li vyloučit přípony souborů ze skenování:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. V okně **Nastavení** klikněte na **Spravovat výjimky** .
4. Klikněte na **+ Přidat výjimku** .
5. Zadejte přípony, které mají být vyjmuty ze skenování, s tečkou před nimi, oddělte je středníky (;).

   txt;avi;jpg
6. Zapněte přepínač vedle ochranné funkce, která by neměla prověřovat rozšíření.
7. Klikněte na tlačítko **Save**.

14.5.3. Správa výjimek ze skenování

Pokud již nakonfigurované výjimky skenování nejsou zapotřebí, doporučujeme je odstranit nebo výjimky skenování vypnout.

Chcete-li spravovat výjimky skenování:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. V okně **Nastavení** klikněte na **Spravovat výjimky** . Zobrazí se seznam všech vašich výjimek.
4. Chcete-li vyjmout nebo upravit výjimky ze skenování, klikněte na jedno z dostupných tlačítek. Pokračujte následovně:

   - Chcete-li odstranit položku ze seznamu, klikněte na tlačítko vedle ní.
   - Chcete-li upravit položku z tabulky, klikněte vedle ní na tlačítko **Upravit** . Objeví se nové okno, kde můžete podle potřeby změnit rozšíření nebo cestu, která má být vyjmuta, a bezpečnostní funkci, ze které mají být vyjmuty. Proveďte nezbytné změny a poté klikněte na tlačítko **UPRAVIT**.

14.6. Správa souborů v karanténě

Produkt Bitdefender izoluje hrozbami infikované soubory, které nedokáže dezinfikovat, a podezřelé soubory v zabezpečené oblasti zvané karanténa.

Virus v karanténě nemůže způsobit žádnou škodu, protože ho nelze spustit ani přečíst.

Ve výchozím stavu jsou soubory z karantény automaticky odesílány do laboratoří společnosti Bitdefender, aby je analyzovali pracovníci výzkumu malwaru společnosti Bitdefender. Jakmile je potvrzena přítomnost hrozby, následuje vydání aktualizace informací o hrozbě pro umožnění jejího odstranění.

Navíc produkt Bitdefender skenuje soubory v karanténě po každé aktualizaci databáze s informacemi o hrozbách. Vyčištěné soubory budou automaticky vráceny do původního umístění.

Chcete-li zkontrolovat a spravovat soubory v karanténě:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
3. Přejděte do okna **Nastavení** .

   Zde můžete zobrazit název souborů v karanténě, jejich původní umístění a název zjištěných hrozeb.
4. Soubory v karanténě automaticky spravuje produkt Bitdefender dle výchozího nastavení karantény.

   Ačkoliv se to nedoporučuje, můžete upravit nastavení karantény podle vašich preferencí kliknutí na **Zobrazit Nastavení**.

   Kliknutím na přepínače zapnete nebo vypnete následující funkce:

   Zkontrolovat karanténu po updatu
   Aby se automaticky skenovaly soubory v karanténě po každé aktualizaci databáze informací o hrozbách, nechte tuto možnost zapnutou. Vyčištěné soubory budou automaticky vráceny do původního umístění.

   Smazat obsah starší než 30 dní
   Soubory v karanténě starší než 30 dní jsou automaticky smazány.

   Vytvořit výjimky pro obnovené soubory
   Soubory, které obnovíte z karantény, jsou přesunuty zpět do původního umístění, aniž by byly opraveny a automaticky vyloučeny z budoucích skenů.

5. Pokud chcete odstranit soubor v karanténě, označte ho a klikněte na tlačítko **Odstranit**. Pokud chcete obnovit soubor z karantény do původního umístění, vyberte ho a klikněte na tlačítko **Obnovit**.

15. POKROČILÁ OCHRANA

Bitdefender Pokročilá ochrana před hrozbami je inovativní, proaktivní detekční technologie, která využívá heuristických metod k detekci ransomwaru a ostatních potenciálních hrozeb v reálném čase.

Pokročilá ochrana před hrozbami průběžně sleduje aplikace spuštěné v zařízení a hledá akce podobné hrozbám. Každá z těchto akcí je ohodnocena a pro každý proces je spočítáno celkové skóre.

Z bezpečnostních důvodů, bude vždy informováni o hrozbách a potenciálně škodlivých procesech, které byli detekovány a zablokovány.

15.1. Zapnutí/vypnutí Pokročilé ochrany před hrozbami

Pro zapnutí/vypnutí Pokročilé ochrany před hrozbami:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ROZŠÍŘENÁ OCHRANA PROTI HROZBÁM** klikněte na **Otevřít** .
3. Přejděte do okna **Nastavení** a klikněte na přepínač vedle položky **Bitdefender Pokročilá ochrana před hrozbami** .

> **Poznámka**
> Pro zajištění ochrany Vašeho systému proti ransomwaru a jiným útokům, doporučujeme vypínat Pokročilou ochranu před hrozbami na co nejkratší možnou dobu.

15.2. Kontrola detekovaných škodlivých útoků

Kdykoli jsou detekovány hrozby nebo potenciálně škodlivé procesy, Bitdefender je zablokuje, aby zabránil infikování vašeho zařízení ransomwarem nebo jiným malwarem. Můžete kdykoliv zkontrolovat seznam zjištěných škodlivých útoků pomocí následujících kroků:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ROZŠÍŘENÁ OCHRANA PROTI HROZBÁM** klikněte na **Otevřít** .
3. Přejděte do okna **Ochrana před hrozbami** .

Jsou zobrazeny útoky rozpoznané za posledních 90 dní. Pro detaily ohledně rozpoznaného ransomwaru, cesty nebezpečného procesu, nebo pro zjištění, zdali dezinfekce proběhla úspěšně, jednoduše na položku klikněte.

15.3. Přidávání procesů mezi výjimky

Můžete nakonfigurovat pravidla výjimek pro důvěryhodné aplikace, aby je Pokročilá ochrana před hrozbami neblokovala, když provádějí činnosti vypadající jako ohrožující chování.

Pro přidání procesů do seznamu výjimek Pokročilé ochrany před hrozbami:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ROZŠÍŘENÁ OCHRANA PROTI HROZBÁM** klikněte na **Otevřít** .
3. V okně **Nastavení** klikněte na **Spravovat výjimky** .
4. Klikněte na **+ Přidat výjimku** .
5. Do příslušného pole zadejte cestu ke složce, kterou chcete kromě skenování.

   Případně můžete přejít na spustitelný soubor kliknutím na tlačítko Procházet v pravé části rozhraní, vyberte jej a klikněte na **OK** .
6. Zapněte přepínač vedle položky **Pokročilá ochrana před hrozbami** .
7. Klikněte na tlačítko **Save**.

15.4. Detekce Exploitu

Způsob, jakým hackeři narušují systémů, je využití určitých bugů nebo chyb zabezpečení v počítačovém softwaru (aplikacích nebo pluginech) a hardwaru. Aby se zajistilo, že vaše zařízení nebude dál od takových útoků, které se běžně šíří velmi rychle, používá Bitdefender nejnovější technologie proti zneužití.

Zapnout nebo vypnout detekci exploitu.

Pro vypnutí nebo zapnutí detekce exploitu:

- Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.

- V podokně **ROZŠÍŘENÁ OCHRANA PROTI HROZBÁM** klikněte na **Otevřít** .
- Chcete-li tuto funkci zapnout nebo vypnout, přejděte do okna **Nastavení** a kliknutím na přepínač vedle položky **Detekce zneužití** .

Poznámka
Ve výchozím nastavení je povolena detekce exploitu.

16. PREVENCE ONLINE HROZEB

Bitdefender Prevence online hrozeb zaručí bezpečné procházení a oznámí vám potenciálně nebezpečné weby.

Bitdefender poskytuje online prevenci hrozeb v reálném čase pro:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Pro konfiguraci nastavení Prevence online hrozeb:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **PREVENCE ONLINE HROZEB** klikněte na **Nastavení**.

V sekci **Ochrana webu** klepnutím na přepínače zapněte nebo vypněte:

- Prevence webových útoků blokuje hrozby pocházející z internetu, včetně automatických stahování.
- Tester odkazů, součást, která klasifikuje výsledky dotazů ve vyhledávači a odkazy zveřejněné na sociálních sítích, umístěním ikony vedle každého výsledku:

  Tuto webovou stránku byste neměli navštěvovat.

  Tato webová stránka může obsahovat nebezpečný obsah. Pokud se rozhodnete ji navštívit, buďte opatrní.

  Návštěva této stránky je bezpečná.

  Tester odkazů klasifikuje výsledky vyhledávání v následujících vyhledávačích:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Tester odkazů klasifikuje odkazy zveřejněné na následujících sociálních sítích:

- Facebook
- Twitter

- Šifrované skenování webu.

  Sofistikovanější útoky mohou využívat zabezpečený webový provoz, a oklamat tak své oběti. Proto vám doporučujeme ponechat zapnutou možnost Šifrované skenování webu.

- Ochrana před podvody.
- Ochrana před phishingem.

Přejděte dolů a dostanete se do části **Prevence síťových hrozeb** . Zde máte možnost **Prevence síťových hrozeb** . Chcete-li zabránit zneužití zranitelných míst v zařízení před útoky složitým škodlivým softwarem (například ransomware), ponechte tuto možnost zapnutou.

Můžete vytvořit seznam webových stránek, domén a IP adres, které nebudou skenovány Bitdefender antivirovými, antiphishing a antifraudovými enginy. Seznam by měl obsahovat pouze webové stránky, domény a adresy IP, kterým plně důvěřujete.

Pro nastavení a správu webových stránek za využití Prevence online hrozeb poskytované Bitdefender:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **PREVENCE ONLINE HROZEB** klikněte na **Nastavení**.
3. Klikněte na **Spravovat výjimky** .
4. Klikněte na **+ Přidat výjimku** .
5. Do odpovídajícího pole zadejte název webu, název domény nebo IP adresu, kterou chcete přidat k výjimkám.
6. Klikněte na přepínač vedle položky **Prevence online hrozeb** .
7. Chcete-li odstranit položku ze seznamu, klikněte na tlačítko vedle ní.

   Kliknutím na tlačítko **Uložit** uložte změny a zavřete okno.

16.1. Výstrahy produktu Bitdefender v prohlížeči

Kdykoli se pokusíte navštívit webovou stránku klasifikovanou jako nebezpečná, webová stránka bude zablokována a v prohlížeči se zobrazí stránka s varováním.

Stránka obsahuje informace, jako URL webové stránky a detekovaná hrozba.

Musíte rozhodnout, co následně provedete. K dispozici jsou následující možnosti:

- Opusťte webovou stránku kliknutím na **ZPÁTKY DO BEZPEČÍ**.
- Přejdete na webovou stránku bez ohledu na varování kliknutím na odkaz **Chápu rizika, chci danou stránku otevřít i tak**.
- Pokud jste si jisti, že zjištěná webová stránka je bezpečná, klikněte na **ODESLAT** a přidejte ji do výjimek. Doporučujeme přidávat pouze stránky, kterým plně důvěřujete.

17. ANTISPAM

Spam je termín používaný k popisu nevyžádaných emailů. Spam se stává stále závažnějším problémem pro jednotlivce i organizace. Není příjemný, nechcete, aby se dostal do rukou vašim dětem, může vést k vašemu propuštění (kvůli ztrátě času nebo proto, že Vám chodí porno do služebního emailu) a nelze zabránit tomu, aby ho lidé posílali. To nejlepší, co se dá udělat, je zastavit jeho příjem. Bohužel má však spam spoustu forem a přichází ve velkém množství.

Antispamový modul produktu Bitdefender využívá pozoruhodné technologické inovace a standardní antispamové filtry, aby spam vyřadil dřív, než dorazí do složky přijaté pošty uživatele. Další informace viz *„Náhled do antispamové technologie“ (str. 106)*.

Antispamová ochrana produktu Bitdefender je k dispozici pouze pro emailové klienty nakonfigurované pro příjem emailových zpráv prostřednictvím protokolu POP3. POP3 je jedním z nejčastěji používaných protokolů pro stahování emailových zpráv z poštovního serveru.

Poznámka
Produkt Bitdefender neposkytuje antispamovou ochranu pro emailové účty, ke kterým přistupujete prostřednictvím webové emailové služby.

Spamové zprávy detekované produktem Bitdefender jsou označeny předponou [spam] v předmětu zprávy. Bitdefender spamové zprávy automaticky přesouvá do určité složky, viz dále:

- V aplikaci Microsoft Outlook jsou spamové zprávy přesouvány do složky **Spam**, která se nachází ve složce **Odstraněná pošta**. Složka **Spam** je vytvořena, když je nějaký email zaznamenán jako spam.
- V aplikaci Mozilla Thunderbird se spamové zprávy přesouvají do složky **Spam**, která se nachází ve složce **Koš**. Složka **Spam** je vytvořena, když je nějaký email zaznamenán jako spam.

Pokud používáte jiné poštovní klienty, je třeba vytvořit pravidlo po přesun emailových zpráv označených produktem Bitdefender jako [spam] do vlastní karanténní složky. Při smazání složek Smazané soubory nebo Koš se smaže také složka Spam. Jakmile však bude nějaký email rozpoznán jako spam, vytvoří se nová složka Spam.

17.1. Náhled do antispamové technologie

17.1.1. Antispamové filtry

Antispamové jádro produktu Bitdefender zahrnuje cloudovou ochranu a několik dalších různých filtrů, které zajišťují, aby ve vaší složce přijaté pošty nebyly žádné spamy. Konkrétně jde o filtry Seznam přátel, Seznam spamerů a Filtr znakových sad.

Seznam přátel / seznam spamerů

Většina lidí komunikuje pravidelně se skupinou lidí nebo dokonce dostávají zprávy od společností či organizací ve stejné doméně. S pomocí **seznamu friends nebo spamerů** můžete snadno klasifikovat, od kterých lidí (přátel) chcete přijímat emaily bez ohledu na to, co zpráva obsahuje, nebo o kterých lidech už nikdy nechcete slyšet (spameři).

> **Poznámka**
> Doporučujeme přidat jména a emailové adresy vašich přátel do **seznamu přátel**. Bitdefender neblokuje zprávy od lidí na tomto seznamu. Přidáním přátel tak pomůžete zajistit, že projdou pouze legitimní zprávy.

Filtr znakových sad

Mnoho spamových zpráv je napsáno v azbuce nebo asijskými znakovými sadami. Filtr znakových sad takové zprávy detekuje a označí je jako spam.

17.1.2. Provoz antispamové ochrany

Antispamové jádro produktu Bitdefender používá kombinaci všech antispamových filtrů, aby určilo, zda má být určitá emailová zpráva doručena do vaší **složky přijaté pošty** nebo ne.

Každý email, který přijde z Internetu, je zkontrolován filtry Seznam přátel / Seznam spamerů. Pokud je adresa odesílatele nalezena v Seznamu přátel, přesune se přímo do vaší **složky přijaté pošty**.

Jinak emailovou zprávu převezme filtr Seznam spamerů a ověří, zda není adresa odesílatele na tomto seznamu. Pokud je nalezena shoda, email bude označen jako spam a přesunut do složky **Spam**.

Jinak filtr znakových sad zkontroluje, zda je zpráva napsána azbukou nebo asijskými znaky. Pokud je tomu tak, email bude označen jako spam a přesunut do složky **Spam**.

> **Poznámka**
> Pokud je email v předmětu označen jako SEXUÁLNĚ EXPLICITNÍ, bude jej produkt Bitdefender považovat za spam.

17.1.3. Podporovaní emailoví klienti a protokoly

Antispamová ochrana je poskytována pro všechny emailové klienty používající protokoly POP3/SMTP. Lišta nástrojů antispamové ochrany produktu Bitdefender je však integrovaná pouze do následujících klientů:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 nebo vyšší

17.2. Zapnutí nebo vypnutí antispamové ochrany

Antispamová ochrana je ve výchozím stavu zapnutá.

Pro zapnutí/vypnutí modulu Antispam:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTISPAM** zapněte nebo vypněte přepínač.

17.3. Použití antispamové lišty nástrojů v hlavním okně klienta

V horní části okna vašeho poštovního klienta se nachází lišta nástrojů Antispam. Lišta nástrojů Antispam vám pomáhá spravovat antispamovou ochranu přímo z vašeho poštovního klienta. Produkt Bitdefender můžete snadno opravit, pokud označil legitimní zprávu jako spam.

> **Důležité**
> Produkt Bitdefender se integruje do nejčastěji používaných poštovních klientů ve formě snadno ovladatelné antispamové lišty nástrojů. Úplný seznam podporovaných poštovních klientů najdete zde *„Podporovaní emailoví klienti a protokoly“ (str. 107)*.

Níže jsou popsána jednotlivá tlačítka lišty nástrojů produktu Bitdefender:

Nastavení - otevře okno, ve kterém můžete konfigurovat antispamové filtry a nastavení lišty nástrojů.
Je spam - označí vybraný email jako spam. Email bude ihned přesunut do složky **Spam**. Pokud jsou aktivované antispamové cloudové služby, zpráva bude odeslána do cloudu produktu Bitdefender k další analýze.
Není spam - indikuje, že vybraný email není spam a produkt Bitdefender by ho neměl označovat. Email bude přesunut ze složky **Spam** do složky **přijaté pošty**. Pokud jsou aktivované antispamové cloudové služby, zpráva bude odeslána do cloudu produktu Bitdefender k další analýze.

Důležité
Tlačítko **Není spam** se aktivuje, jakmile vyberete zprávu označenou produktem Bitdefender jako spam (obvykle jsou tyto zprávy umístěny ve složce **Spam**).

Přidat spamera - přidá odesílatele vybraného emailu do seznamu spamerů. Může být nutné potvrzení tlačítkem **OK**. Emailové zprávy přijaté z adres v seznamu spamerů budou automaticky označeny jako [spam].
Přidat přítele - přidá odesílatele vybraného emailu do seznamu přátel. Může být nutné potvrzení tlačítkem **OK**. E-mailové zprávy z této adresy obdržíte vždy, bez ohledu na jejich obsah.
Spameři - otevře **Seznam spamerů**, který obsahuje všechny emailové adresy, z nichž nechcete dostávat zprávy, bez ohledu na jejich obsah. Další informace viz *„Konfigurace seznamu spamerů“* (str. 111).
Přátelé - otevře **Seznam přátel**, který obsahuje všechny emailové adresy, z nichž vám budou emailové zprávy doručovány bez ohledu na jejich obsah. Další informace viz *„Konfigurace seznamu přátel“* (str. 110).

17.3.1. Indikace chyb detekce

Jestliže používáte podporovaného poštovního klienta, můžete snadno opravovat antispamový filtr (indikací emailových zpráv, které by neměly být označeny jako [spam]). Tím zlepšíte účinnost antispamového filtru. Postupujte následovně:

1. Otevřete poštovního klienta.
2. Přejděte do složky nevyžádané pošty, kam jsou přesouvány spamové zprávy.
3. Vyberte legitimní zprávu nesprávně označenou produktem Bitdefender jako [spam].

4. Kliknutím na tlačítko **Přidat přítele** na liště antispamových nástrojů produktu Bitdefender přidáte odesílatele do seznamu přátel. Může být nutné potvrzení tlačítkem **OK**. E-mailové zprávy z této adresy obdržíte vždy, bez ohledu na jejich obsah.
5. Klikněte na tlačítko **Není spam** na liště antispamových nástrojů produktu Bitdefender (obvykle se nachází v horní části okna poštovního klienta). Emailová zpráva bude přesunuta do složky přijaté pošty.

17.3.2. Indikace nedetekovaných spamových zpráv

Jestliže používáte podporovaného poštovního klienta, můžete označit, které emailové zprávy měly být detekovány jako spam. Tím zlepšíte účinnost antispamového filtru. Postupujte následovně:

1. Otevřete poštovního klienta.
2. Přejděte do složky přijaté pošty.
3. Vyberte nedetekované spamové zprávy.
4. Klikněte na tlačítko **Je spam** na liště antispamových nástrojů produktu Bitdefender (obvykle se nachází v horní části okna poštovního klienta). Okamžitě se označí jako [spam] a budou přesunuty do složky nevyžádané pošty.

17.3.3. Konfigurace nastavení lišty nástrojů

Pokud chcete konfigurovat nastavení lišty antispamových nástrojů v emailovém klientovi, klikněte na tlačítko **Nastavení** na liště nástrojů a poté na kartu **Nastavení lišty nástrojů**.

Zde jsou k dispozici následující možnosti:

- **Označit spamy jako přečtené** - automaticky označí spamové zprávy jako přečtené, aby při doručení nerušily.
- Můžete zvolit, zda se mají zobrazovat potvrzovací okna, když kliknete tlačítka **Přidat spamera** a **Přidat přítele** na liště antispamových nástrojů.

  Potvrzovací okna mohou zabránit nechtěnému přidání odesílatelů emailů do seznamů přátel/spamerů.

17.4. Konfigurace seznamu přátel

Seznam přátel je seznam všech emailových adres, ze kterých chcete vždy přijímat zprávy, bez ohledu na jejich obsah. Zprávy od vašich přátel nejsou nikdy označeny jako spam, i kdyby svým obsahem spam připomínaly.

> **Poznámka**
> Každý e-mail, který přijde z adresy na **seznamu přátel**, bude automaticky doručen do vaší složky přijaté pošty bez dalšího zpracování.

Postup konfigurace a správy seznamu přátel:

- Pokud používáte Microsoft Outlook nebo Thunderbird, klikněte na tlačítko **Přátelé** na liště antispamových nástrojů produktu Bitdefender.
- Alternativně:
  1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
  2. V okně **ANTISPAM** klikněte na **Nastavení**.
  3. Otevřete okno **Spravovat přátele** .

Chcete-li přidat emailovou adresu, vyberte možnost **Emailová adresa**, zadejte adresu a poté klikněte na **PŘIDAT**. Syntaxe: name@domain.com.

Chcete-li přidat emailové adresy z určité domény, vyberte možnost **Jméno domény**, zadejte název domény a poté klikněte na **PŘIDAT**. Syntaxe:

- @doména.com a doména.com - všechny emailové zprávy přicházející z domény doména.com dorazí do vaší **Přijaté pošty** bez ohledu na jejich obsah;
- doména - veškerá pošta z domény doména (bez ohledu na příponu domény) bude označena jako spam;
- com - veškerá pošta s příponou domény com bude označena jako spam;

Je doporučeno nepřidávat celé domény, ale v některých situacích to může být užitečné. Například můžete přidat emailovou doménu společnosti, pro kterou pracujete, nebo domény vašich důvěryhodných partnerů.

Chcete-li odstranit položku ze seznamu, klikněte na příslušné tlačítko vedle ní. Chcete-li odstranit všechny položky ze seznamu, klikněte na **Vymazat seznam** .

Seznam Přátelé můžete uložit do souboru, abyste jej mohli použít na jiném zařízení nebo po přeinstalování produktu. Chcete-li seznam přátel uložit,

klikněte na tlačítko **Uložit** a uložte ho do požadovaného umístění. Soubor bude mít příponu .bwl.

Chcete-li načíst dříve uložený seznam přátel, klikněte na **Načíst** a otevřete odpovídající soubor .bwl . Chcete-li obnovit obsah existujícího seznamu při načítání dříve uloženého seznamu, zaškrtněte políčko vedle **Přepsat aktuální seznam** .

17.5. Konfigurace seznamu spamerů

Seznam spamerů je seznam veškerých emailových adres, ze kterých nechcete dostávat žádné zprávy, bez ohledu na jejich obsah. Každý email, který přijde z adresy na **Seznamu spamerů**, bude automaticky označen jako spam, bez dalšího zpracování.

Postup konfigurace a správy seznamu spamerů:

- Pokud používáte Microsoft Outlook nebo Thunderbird, klikněte na tlačítko **Spameři** na liště antispamových nástrojů produktu Bitdefender integrované ve vašem poštovním klientovi.
- Alternativně:
  1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
  2. V okně **ANTISPAM** klikněte na **Nastavení**.
  3. Otevřete okno **Spravovat spammery** .

Chcete-li přidat emailovou adresu, vyberte možnost **Emailová adresa**, zadejte adresu a poté klikněte na **PŘIDAT**. Syntaxe: name@domain.com.

Chcete-li přidat emailové adresy z určité domény, vyberte možnost **Jméno domény**, zadejte název domény a poté klikněte na **PŘIDAT**. Syntaxe:

- @doména.com a doména.com - všechny emailové zprávy přicházející z domény doména.com dorazí do vaší **Přijaté pošty** bez ohledu na jejich obsah;
- doména - veškerá pošta z domény doména (bez ohledu na příponu domény) bude označena jako spam;
- com - veškerá pošta s příponou domény com bude označena jako spam.

Je doporučeno nepřidávat celé domény, ale v některých situacích to může být užitečné.

Varování

Nepřidávejte do seznamu spamerů domény legitimních webových emailových služeb (jako Post, Gmail, Centrum a pod.). V opačném případě budou emailové adresy přijaté od všech registrovaných uživatelů těchto služeb označeny jako spam. Pokud například přidáte do seznamu spamerů doménu post.cz, všechny emailové zprávy přijaté z adres domény post.cz budou označeny jako [spam].

Chcete-li odstranit položku ze seznamu, klikněte na příslušné tlačítko vedle ní. Chcete-li odstranit všechny položky ze seznamu, klikněte na **Vymazat seznam** .

Seznam spammerů můžete uložit do souboru, abyste jej mohli použít na jiném zařízení nebo po přeinstalování produktu. Chcete-li seznam spamerů uložit, klikněte na tlačítko **Uložit** a uložte ho do požadovaného umístění. Soubor bude mít příponu .bwl.

Chcete-li načíst dříve uložený seznam spamerů, klikněte na **NAČÍST** a otevřete příslušný soubor .bwl. Pro obnovení obsahu stávajícího seznamu, do kterého chcete nahrát dříve uložený seznam, zvolte možnost **Přepsat aktuální seznam**.

17.6. Konfigurace místních antispamových filtrů

Jak je popsáno v části *„Náhled do antispamové technologie“* (str. 106), produkt Bitdefender používá k identifikaci spamu kombinaci různých antispamových filtrů. Antispamové filtry jsou předkonfigurovány pro účinnou ochranu.

Důležité

V závislosti na tom, zda přijímáte legitimní emaily psané asijskými písmy nebo azbukou, vypněte nebo zapněte nastavení, které takové emaily automaticky blokuje. Příslušné nastavení je vypnuto v lokalizovaných verzích programu, který tyto znakové sady používá (např. v ruské nebo čínské verzi).

Konfigurace místních antispamových filtrů

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTISPAM** klikněte na **Nastavení**.
3. Přejděte do okna **Nastavení** a klikněte na odpovídající přepínače zapnutí a vypnutí.

Pokud používáte Microsoft Outlook nebo Thunderbird, můžete místní antispamové filtry konfigurovat přímo z poštovního klienta. Klikněte na tlačítko ⚙ **Nastavení** na liště antispamových nástrojů produktu Bitdefender (obvykle se nachází v horní části okna poštovního klienta) a poté na kartu **Antispamové filtry**.

17.7. Konfigurace nastavení cloudu

Cloudová detekce používá cloudové služby produktu Bitdefender k zajištění účinné a stále aktuální antispamové ochrany.

Funkce cloudové ochrany funguje, pokud je zapnutá antispamová ochrana produktu Bitdefender.

Vzorky legitimních nebo spamových emailů lze odeslat do cloudu produktu Bitdefender, když indikujete chyby detekce nebo nedetekované spamové emaily. Tím pomůžete zlepšit antispamovou detekci produktu Bitdefender.

Nakonfigurujte odeslání vzorku emailu do cloudu produktu Bitdefender označením požadovaných možností pomocí následujícího postupu:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTISPAM** klikněte na **Nastavení**.
3. Přejděte do okna **Nastavení** a klikněte na odpovídající přepínače zapnutí a vypnutí.

Pokud používáte Microsoft Outlook nebo Thunderbird, můžete cloudovou detekci konfigurovat přímo z poštovního klienta. Klikněte na tlačítko ⚙ **Nastavení** na liště antispamových nástrojů produktu Bitdefender (obvykle se nachází v horní části okna poštovního klienta) a poté na kartu **Nastavení cloudu**.

18. FIREWALL

Firewall chrání zařízení před příchozími a odchozími neautorizovanými pokusy o připojení, a to jak v místních sítích, tak na internetu. Lze ji přirovnat k hlídači u vaší brány - sleduje pokusy a připojení a rozhoduje se, které povolit a které zablokovat.

Brána firewall produktu Bitdefender používá sadu pravidel k filtrování dat přenášených do vašeho systému a z něj.

Za normálních podmínek produkt Bitdefender automaticky vytvoří pravidlo, když se nějaká aplikace pokusí o přístup k Internetu. Pravidla pro aplikace můžete přidávat nebo upravovat i ručně.

Jakožto bezpečnostní opatření budete upozorněni pokaždé, když je potenciálně škodlivá aplikace zablokována od přístupu k internetu.

Produkt Bitdefender automaticky přiřadí typ sítě každému detekovanému síťovému připojení. V závislosti na typu připojení je ochrana branou firewall pro každé připojení nastavena na patřičnou úroveň.

Chcete-li se dozvědět více o nastavení brány firewall pro jednotlivé typy sítí a o postupu úpravy nastavení sítě, čtěte část *„Správa nastavení připojení“* (str. 117).

18.1. Zapnutí nebo vypnutí brány firewall

Chcete-li zapnout nebo vypnout Firewall:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **FIREWALL** zapněte nebo vypněte přepínač.

Varování

Vypnutí brány firewall by mělo být pouze dočasným opatřením, protože vystavuje vaše zařízení neautorizovanému připojení. Bránu firewall znovu co nejdříve zapněte.

18.2. Správa pravidel aplikace

Chcete-li zobrazit a spravovat pravidla brány firewall řídící přístup aplikací k síťovým prostředkům a Internetu, postupujte následovně:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.

2. V okně **FIREWALL** klikněte na **Nastavení**.
3. Přejděte do okna **Přístup k aplikaci** .

Uvidíte programů (procesů), které prošly přes Bitdefender Firewall a internetovou síť, ke které jste připojeni. Pro zobrazení pravidel vytvořených pro konkrétní aplikaci na ni jednoduše klikněte a poté klikněte na odkaz **Zobrazit pravidla aplikace**. Otevře se okno **Pravidla**.

Pro každé pravidlo jsou zobrazeny následující informace:

- **SÍŤ** - proces a typy síťových adaptérů (Doma/Kancelář, Veřejné, nebo Všechny), kterých se dané pravidlo týká. Automaticky se vytvářejí pravidla pro filtrování přístupu k síti nebo Internetu pomocí libovolného adaptéru. Ve výchozím stavu pravidla platí pro libovolnou síť. Můžete ručně vytvořit pravidla nebo upravit existující pravidla tak, aby filtrovala přístup aplikace k síti nebo Internetu prostřednictvím konkrétního adaptéru (např. adaptéru bezdrátové sítě).
- **PROTOKOL** - IP protokol, na který se pravidlo vztahuje. Ve výchozím stavu pravidla platí pro libovolný protokol.
- **PROVOZ** - pravidlo platí pro oba směry, příchozí i odchozí.
- **PORTY** - protokol portu, na který se pravidlo vztahuje. Ve výchozím stavu pravidla platí automaticky pro všechny porty.
- **IP** - internetový protokol (IP), na který se pravidlo vztahuje. Ve výchozím stavu pravidla platí automaticky pro všechny IP adresy.
- **PŘÍSTUP** - má-li aplikace za daných podmínek povolený nebo blokovaný přístup k síti nebo internetu.

Pro změnu nebo smazání pravidel pro vybranou aplikaci, klikněte na ikonu ⋯.

- **Upravit pravidlo** - otevře okno, ve kterém můžete upravovat současné pravidlo.
- **Smazat pravidlo** - můžete vymazat aktuální seznam pravidel vybrané aplikace.

Přidání pravidel aplikací

Přidání pravidla aplikace:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.

2. V okně **FIREWALL** klikněte na **Nastavení**.
3. V okně **Pravidla** klikněte na **Přidat pravidlo**.

Zde můžete použít následující změny:

- **Aplikovat pravidlo pro všechny aplikace.** Povolením této volby aplikujete vytvořené pravidlo na všechny aplikace.
- **Program:** Klikněte na **PROCHÁZET** a vyberte aplikaci, na niž se pravidlo vztahuje.
- **Oprávnění.** Vyberte jedno z dostupných oprávnění:

Oprávnění	Popis
Povolit	Specifikované aplikaci bude povolen přístup k síti/Internetu za určitých okolností.
Zakázat	Specifikované aplikaci bude zakázán přístup k síti/Internetu za určitých okolností.

- **Typ sítě.** Vyberte typ sítě, na nějž se pravidlo vztahuje. Typ můžete změnit otevřením rozevírací nabídky **Typ sítě** a výběrem jednoho z dostupných typů ze seznamu.

Typ sítě	Popis
Jakákoli síť	Povolte veškerý provoz mezi vaším zařízením a ostatními zařízeními bez ohledu na typ sítě.
Domov/kancelář	Povolte veškerý provoz mezi vaším zařízením a různými v místní síti.
Veřejné	Veškerý provoz je filtrovaný.

- **Protokol.** Vyberte v nabídce protokol IP, na který se pravidlo vztahuje.
  - Pokud chcete pravidlo aplikovat na všechny protokoly, vyberte možnost **Vše**.
  - Pokud chcete pravidlo aplikovat na protokol TCP, vyberte možnost **TCP**.
  - Pokud chcete pravidlo aplikovat na protokol UDP, vyberte možnost **UDP**.
  - Pokud chcete pravidlo aplikovat na protokol ICMP, vyberte možnost **ICMP**.

- Pokud chcete pravidlo aplikovat na protokol IGMP, vyberte možnost **IGMP**.
- Pokud chcete, aby se pravidlo vztahovalo na GRE, vyberte **GRE** .
- Pokud chcete pravidlo aplikovat na konkrétní protokol, zadejte číslo přiřazené protokolu, který chcete filtrovat, do prázdného editačního pole.

> **Poznámka**
>
> Čísla protokolům IP přiděluje organizace Internet Assigned Numbers Authority (IANA). Kompletní seznam přidělených čísel protokolů IP najdete na adrese http://www.iana.org/assignments/protocol-numbers.

- **Směr.** Vyberte v nabídce směr komunikace, na který se pravidlo vztahuje.

Směr	Popis
Odchozí	Pravidlo se použije pouze pro odchozí provoz.
Příchozí	Pravidlo se použije pouze pro příchozí provoz.
Obojí	Pravidlo se použije pro oba směry komunikace.

Kliknutím na tlačítko **Pokročilá nastavení** v dolní části okna můžete upravit následující nastavení:

- **Vlastní lokální adresa.** Specifikujte místní IP adresu a port, na které se pravidlo vztahuje.
- **Vlastní vzdálená adresa.** Specifikujte vzdálenou IP adresu a port, na které se pravidlo vztahuje.

Pro odstranění aktuální sady pravidel a obnovení výchozích, klikněte na odkaz **Obnovit pravidla** v horní části okna **Pravidla**.

18.3. Správa nastavení připojení

Zda se chcete připojit k internetu za použití Wi-fi nebo ethernetového adaptéru, můžete konfigurovat nastavení aplikovaná pro bezpečnou navigaci. Možnosti, ze kterých máte na výběr, jsou:

- **Dynamické** - typ sítě bude zvolen automaticky podle profilu sítě, ke které se připojujete - Doma/V kanceláři, nebo Veřejná. Nastane-li tato situace,

budou aplikována pouze pravidla Firewall pro daný typ sítě, nebo pravidla, která jsou nastavena tak, aby byla použita pro všechny typy sítí.

- **Doma/V kanceláři** - typ sítě bude vždy Doma/V kanceláři, nehledě na profil připojené sítě. Nastane-li tato situace, budou aplikována pouze pravidla Firewall pro Doma/V kanceláři, nebo pravidla, která jsou nastavena tak, aby byla použita pro všechny typy sítí.
- **Veřejná** - typ sítě bude vždy Veřejná, nehledě na profil připojené sítě. Nastane-li tato situace, budou aplikována pouze pravidla Firewall pro Veřejné sítě, nebo pravidla, která jsou nastavena tak, aby byla použita pro všechny typy sítí.

Pro nastavení síťových adaptérů:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **FIREWALL** klikněte na **Nastavení**.
3. Vyberte okno **Síťové adaptéry** .
4. Vyberte nastavení, která chcete použít při připojení se k následujícím adaptérům:
   - WiFi
   - Ethernet

18.4. Konfigurace pokročilých nastavení

Pro konfiguraci pokročilého nastavení firewallu:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **FIREWALL** klikněte na **Nastavení**.
3. Vyberte okno **Nastavení** .

Můžete konfigurovat následující funkce:

- **Ochrana skenování portů** - detekuje a blokuje pokusy o zjištění otevřených portů.

  Hackeři často používají prohledávání portů, aby zjistili, které porty jsou v zařízení otevřené. Pokud naleznou méně bezpečný nebo zranitelný port, mohou do vašeho zařízení vniknout.

- **Paranoidní režim** - zobrazí varování pokaždé, když se aplikace pokusí se připojit k internetu. Vyberte **Povolit** nebo **Odmítnout**. Když je zapnutý

Paranoidní režim, funkce Profily je automaticky vypnuta. Paranoidní režim lze použít současně s **Úsporným režimem**.

- **Povolit přístup k síti domény** - povolit nebo zakázat přístup ke zdrojům a sdíleným položkám definovaným správcem domény.
- **Mód Utajení** - zda vás mohou detekovat jiná zařízení. Kliknutím na **Upravit nastavení utajení** vyberte, kdy má být vaše zařízení viditelné pro jiná zařízení.
- **Výchozí chování aplikace** - umožní produktu Bitdefender použít automatická nastavení pro aplikace s žádnými vymezenými pravidly. Klepnutím na tlačítko **Upravit výchozí pravidla** vyberte, zda chcete použít automatické nastavení nebo ne.
  - Automatické - přístup bude aplikacím povolen nebo zakázán podle automatických Firewall a uživatelských pravidel.
  - Povolit - aplikace, které nemají zadané žádné Firewall pravidlo, budou automaticky povoleny.
  - Blokovat - aplikace, které nemají zadané žádné Firewall pravidlo, budou automaticky blokovány.

19. ZRANITELNOSTI

Důležitým krokem při ochraně zařízení před škodlivými akcemi a aplikacemi je udržovat operační systém a aplikace, které pravidelně používáte, aktuální. Navíc, aby se zabránilo neoprávněnému fyzickému přístupu k vašemu zařízení, musí být pro každý uživatelský účet Windows a pro sítě Wi-Fi, ke kterým se také připojujete, nakonfigurována silná hesla (hesla, která nelze snadno uhodnout).

Produkt Bitdefender nabízí jednoduché postupy k opravě zranitelností vašeho systému:

- Můžete skenovat zranitelnosti ve vašem systému a opravit je krok po kroku pomocí funkce **Sken zranitelností**.
- Pomocí automatického sledování zranitelností můžete kontrolovat a opravovat zjištěné zranitelnosti v okně Notifikace.

Zranitelnosti systému byste měli kontrolovat a opravovat každý týden nebo dva.

19.1. Skenování zranitelností systému

K odhalení chyb zabezpečení systému vyžaduje produkt Bitdefender aktivní připojení k internetu.

Skenování zranitelností systému

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ZRANITELNOSTI** klikněte na **Otevřít** .
3. Na kartě **Kontrola zranitelnosti** klikněte na **Spustit prověřování** a poté počkejte, až Bitdefender zkontroluje zranitelnost systému. Zjištěné chyby zabezpečení jsou seskupeny do tří kategorií:
   - **OPERAČNÍ SYSTÉM**
     - **Zabezpečení operačního systému**

       Změněné nastavení systému, které může ohrozit vaše zařízení a data, například nezobrazovat varování, když provedené soubory provádějí změny ve vašem systému bez vašeho svolení nebo když se zařízení MTP, jako jsou telefony nebo fotoaparáty, připojují a provádějí různé operace bez vašeho vědomí.
     - **Důležité aktualizace systému Windows**

Zobrazí se seznam kritických aktualizací systému Windows, které nejsou nainstalovány v počítači. Po dokončení instalace Bitdefender může být vyžadován restart systému. Instalace aktualizací může chvíli trvat.

- **Slabé účty systému Windows**

  Můžete vidět seznam uživatelských účtů systému Windows nakonfigurovaných ve vašem zařízení a úroveň ochrany, kterou jejich heslo poskytuje. Můžete zvolit, zda má být uživatel vyzván ke změně hesla při příštím přihlášení, nebo zda chcete heslo ihned změnit sami. Pro nastavení nového hesla do vašeho systému, zvolte **Změnit heslo nyní**.

  Chcete-li vytvořit silné heslo, doporučujeme použít kombinaci velkých a malých písmen, čísel a speciálních znaků (například # , $ nebo @).

- **APLIKACE**
  - **Zabezpečení prohlížeče**

    Změňte nastavení zařízení, které umožňuje provádění souborů a programů stažených prostřednictvím aplikace Internet Explorer bez ověření integrity, což může vést k ohrožení zařízení.

  - **Aktualizace aplikací**

    Chcete-li zobrazit informace o aplikaci, kterou je třeba aktualizovat, klepněte na její název v seznamu.

    Pokud aplikace není aktuální, klikněte na **Stáhnout novou verzi** a stáhněte si nejnovější verzi.

- **SÍŤ**
  - **Síť a pověření**

    Změněno nastavení systému, jako je automatické připojení k otevřeným hotspotovým sítím bez vašeho vědomí nebo nevynucení šifrování odchozího provozu zabezpečeného kanálu.

  - **Wi-Fi sítě a routery**

    Chcete-li se dozvědět více o bezdrátové síti a routeru, ke kterému jste připojeni, klepněte na jeho název v seznamu. V případě, že je doporučeno nastavit silnější heslo pro vaši domácí síť, ujistěte se, že budete postupovat podle našich pokynů, abyste mohli zůstat připojení bez obav o své soukromí.

Pokud jsou k dispozici doporučení, sledujte instrukce aby jste se ujistili že vaše domácí síť je v bezpečí před hackery.

19.2. Používání automatického sledování zranitelností

Produkt Bitdefender pravidelně skenuje zranitelnosti vašeho systému na pozadí a záznamy o nalezených problémech uchovává v okně Notifikace.

Chcete-li zkontrolovat a detekovat problémy:

1. Klikněte na **Upozornění** v navigačním menu v rozhraní Bitdefender.
2. V záložce **Vše** vyberte notifikaci týkající se skenu zranitelností.
3. Můžete si prohlédnout podrobné informace o nalezených zranitelnostech systému. V závislosti na problému postupujte při opravě konkrétní zranitelnosti následovně:
   - Pokud jsou k dispozici aktualizace systému Windows, klikněte na **Instalovat**.
   - Pokud jsou automatické aktualizace systému Windows vypnuty, klikněte na položku **Zapnout**.
   - Pokud se jedná o neaktuální aplikaci, kliknutím na položku **Aktualizovat nyní** vyhledáte odkaz na webovou stránku dodavatele, odkud můžete nainstalovat nejnovější verzi příslušné aplikace.
   - Pokud má některý uživatelský účet systému Windows slabé heslo, klikněte na položku **Změna hesla**, aby si uživatel musel změnit heslo při příštím přihlášení, nebo heslo změňte sami. Silné heslo vytvoříte použitím kombinace malých a velkých písmen, číslic a speciálních symbolů (např. #, $ nebo @).
   - Pokud je v systému Windows zapnutá funkce automatického spouštění, kliknutím na položku **Opravit** ji vypnete.
   - Pokud vámi konfigurovaný router má nastaveno slabé heslo, klikněte na **Změnit heslo** kde můžete v jeho rozhraní nastavit silnější.
   - Pokud síť ke které jste připojení má zranitelnosti které mohou ohrozit váš systém, klikněte na **Změnit nastavení Wi-Fi**.

Chcete-li konfigurovat nastavení monitoru zranitelností:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ZRANITELNOSTI** klikněte na **Otevřít** .

Důležité
Abyste byli automaticky informováni o zranitelnostech systému nebo aplikací, nechte možnost **Zranitelnosti** zapnutou.

3. Přejděte na kartu **Nastavení** .
4. Vyberte zranitelnosti systému, které chcete pravidelně kontrolovat, pomocí příslušných přepínačů.

Windows updates
Zkontrolujte, zda jsou ve vašem operačním systému Windows nainstalovány nejnovější důležité aktualizace zabezpečení od společnosti Microsoft.

Aktualizace aplikací
Zkontrolujte, zda jsou aplikace nainstalované ve vašem systému aktuální. Zastaralé aplikace mohou být zneužity škodlivým softwarem a činí tak váš počítač zranitelným útoky zvnějšku.

Uživatelská hesla
Zkontrolujte, zda jsou hesla účtů systému Windows a routerů nakonfigurovaná v systému snadno uhodnutelná nebo ne. Nastavení obtížně uhodnutelných (silných) hesel výrazně ztíží hackerům snahu proniknout do vašeho systému. Silné heslo obsahuje kombinaci malých a velkých písmen, číslic a speciálních symbolů (např. #, $ nebo @).

Autoplay
Zkontrolujte stav funkce automatického spouštění v systému Windows. Tato funkce umožňuje automatické spouštění aplikací z disků CD, DVD, jednotek USB a dalších externích zařízení.

Některé druhy hrozeb používají automatické spouštění pro automatické šíření z vyjímatelných médií do počítače. Proto je doporučeno tuto funkci systému Windows vypnout.

Wi-Fi Bezpečnostní Poradce
Zkontrolujte, zda je domácí bezdrátová síť, ke které jste připojeni bezpečná, nebo ne a zda má slabá místa. Také zkontrolujte, zda je heslo vašeho domácího routeru dostatečně silné, a jak může být bezpečnější.

Většina nezabezpečených bezdrátových sítí není bezpečná, což umožňuje zvědavým očím hackerů mít přístup k vašim soukromým aktivitám.

Poznámka
Pokud vypnete sledování určité zranitelnosti, související problémy již nebudou zaznamenávány v okně Notifikace.

19.3. Wi-Fi Bezpečnostní Poradce

Na cestách, při práci v kavárně nebo čekání na letišti, připojení se k veřejné bezdrátové síti pro provádění plateb, kontrolu e-mailů nebo účtů na sociálních sítích může být nejrychlejší řešení. Ale zvědavé pohledy snažící se ukrást vaše osobní data zde mohou existovat. Mohou sledovat informace tak, jak proudí sítí.

Osobními údaji je myšleno, že hesla a uživatelská jména, které používáte k přístupu ke svým online účtům, jako jsou e-maily, bankovní účty, účty sociálních médií, ale i odeslaných zpráv.

Obvykle veřejné bezdrátové sítě jsou více náchylné na bezpečnost, protože nevyžadují heslo při přihlášení, a pokud ano, heslo by mohlo být k dispozici pro každého, kdo se chce připojit. Kromě toho to mohou být škodlivé nebo Honeypot sítě, což představuje cíl pro počítačové zločince.

Chcete-li chránit před nebezpečím nezabezpečených nebo nešifrovaných veřejných bezdrátových přístupových bodů, Bitdefender Wi-Fi Poradce ochrany analyzuje, jak bezpečná je bezdrátová síť, a pokud je to nutné, doporučí používat Bitdefender VPN.

Bitdefender Wi-Fi Poradce ochrany udává informace o:

- Domácí Wi-Fi sítě
- Wi-Fi sítě v kanceláři
- Veřejné Wi-Fi sítě

19.3.1. Zapnutí nebo vypnutí notifikací Wi-Fi Poradce bezpečnosti

Chcete-li zapnout nebo vypnout ohlášení Wi-Fi Poradce bezpečnosti:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.

2. V podokně **ZRANITELNOSTI** klikněte na **Otevřít** .
3. Přejděte do okna **Nastavení** a zapněte nebo vypněte možnost **Poradce zabezpečení Wi-Fi** .

19.3.2. Konfigurace domácí Wi-Fi sítě

Chcete-li konfigurovat vaši domácí síť:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ZRANITELNOSTI** klikněte na **Otevřít** .
3. Přejděte do okna **Wi-Fi Security Advisor** a klikněte na **Domácí Wi-Fi** .
4. V okně **Domácí Wi-Fi** vyberte volbu **VYBRAT DOMÁCÍ WI-FI**.

   Seznam s bezdrátovými sítěmi ke kterým jste byli dosud připojeni.
5. Vyberte domácí síť, a klepněte na tlačítko **Vybrat**.

Pokud je domácí síť považována za nezabezpečenou nebo je nebezpeční, zobrazí se konfigurační doporučení ke zlepšení bezpečnosti.

Chcete-li odstranit bezdrátovou síť kterou jste nastavili jako domácí, klikněte na tlačítko **ODEBRAT**.

Abyste přidali novou bezdrátovou síť jako domácí, klikněte na **zvolit novou domácí síť**.

19.3.3. Konfigurace kancelářské Wi-Fi sítě

Chcete-li konfigurovat vaši kancelářskou síť:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ZRANITELNOSTI** klikněte na **Otevřít** .
3. Přejděte do okna **Poradce pro zabezpečení Wi-Fi** , klikněte na **Kancelářské Wi-Fi** .
4. V okně **Wi-Fi kancelář** klikněte na **VYBRAT WI-FI PRO KANCELÁŘ**.

   Seznam s bezdrátovými sítěmi ke kterým jste byli dosud připojeni.
5. Přejděte na síť své kanceláře a poté klepněte na tlačítko **VYBRAT**.

Pokud je síť v kanceláři považována za nezabezpečenou nebo nebezpečnou, zobrazí se doporučení pro konfiguraci pro zlepšení zabezpečení.

Chcete-li odstranit bezdrátovou síť kterou jste nastavili jako kancelář, klikněte na **ODEBRAT**.

Chcete-li přidat novou bezdrátovou síť pro kancelář, klepněte na tlačítko **Zvolit novou wi-fi pro kancelář**.

19.3.4. Veřejná Wi-Fi

Zatímco jste připojení k nezabezpečené nebo nebezpečné bezdrátové síti, je aktivován profil pro připojení k veřejné Wi-Fi. Zatímco je spuštěn tento profil, Bitdefender Internet Security je nastaven k automatickému dokončená nastavená následujících programů:

- Pokročilá ochrana před hrozbami je zapnuta
- Bitdefender Firewall je zapnutý a následující nastavení jsou aplikované na váš bezdrátový adaptér.
  - Tichý režim - ON
  - Typ Sítě - Veřejná
- V Prevenci online hrozeb jsou zapnuta následující nastavení:
  - Šifrované skenování webu
  - Ochrana proti podvodům
  - Ochrana proti phishingu
- Tlačítko otevírající Bitdefender Safepay™ je dostupné. V tomto případě je ochrana Hotspot pro nezabezpečené sítě povolena již v základním nastavení.

19.3.5. Kontroluji informace o síti Wi-Fi

Chcete-li zkontrolovat informace o bezdrátových sítích ke kterým jste byli připojeni:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ZRANITELNOSTI** klikněte na **Otevřít** .
3. Přejděte do okna **Poradce pro zabezpečení Wi-Fi** .
4. Podle toho, jaké informace potřebujete, vyberte jednu ze tří karet, **Domácí Wi-Fi**, **Wi-Fi v kanceláři** nebo **Veřejná Wi-Fi**.
5. Klikněte na **Zobrazit detaily** vedle sítě o které chcete vědět více.

Existují tři druhy bezdrátových sítí filtrované podle jejich důležitosti, přičemž každý je indikován konkrétní ikonou:

Wi-Fi je nebezpečná - indikuje že úroveň zabezpečení sítě je nízká. To znamená, že existuje vysoké riziko ji použít, a nedoporučuje se provádět platby nebo kontrolovat bankovní účty bez zvláštní ochrany. V takových situacích doporučujeme použít Bitdefender Safepay™ s ochranou Hotspot pro nezabezpečené sítě.

Wi-Fi je nebezpečná - indikuje že úroveň zabezpečení sítě je průměrná. To znamená, že její použití může obsahovat zranitelnosti a nedoporučuje se provádět platby nebo kontrolovat bankovní účty bez zvláštní ochrany. V takových situacích doporučujeme použít Bitdefender Safepay™ s ochranou Hotspot pro nezabezpečené sítě.

Wi-Fi je bezpečná - indikuj že Wi-Fi kterou používáte je bezpečná. V tomto případě můžete dělat operace online s použitím citlivých dat.

Kliknutím na odkaz **Zobrazit detaily** se u každé ze sítí zobrazí následující detaily:

- **Zabezpečeno** - zde se můžete podívat, zda je zvolená síť zabezpečená, nebo ne. Nešifrované sítě mohou odhalit data které ji opouští.
- **Typ šifrování** - zde můžete vidět jaký typ šifrován používá zvolená síť. Některé typy šifrování nemusí být bezpečné. Z tohoto důvodu silně doporučujeme, aby jste si zkontrolovali informace o šifrování aby jste si mohli být jisti že jste během procházení webu v bezpečí.
- **Kanál/Frekvence** - zde můžete vidět kanál a frekvenci používané zvolenou sítí.
- **Síla hesla** - zde vidíte jak silné je vaše heslo. Pamatujte že sítě které mají slabé heslo představují cíl pro kybernetické útočníky.
- **Typ přihlášení** - Zde můžete vidět, zda vybraná síť využívá heslo nebo ne. Doporučujeme se připojovat pouze k sítím, které mají silné heslo.
- **Typ ověření** - zde můžete vidět typ ověřování použitý zvolenou sítí.

20. OCHRANA VIDEO & AUDIO

Stále více hrozeb je navrženo, aby se snažily o přístup k vestavěným webovým kamerám a mikrofonům. Chcete-li zabránit neoprávněnému přístupu k webové kameře a být informováni o tom, jaké nedůvěryhodné aplikace mají přístup k mikrofonu zařízení a kdy, Bitdefender Video & Audio obsahuje:

- Ochrana webových kamer
- Monitor mikrofonu

20.1. Ochrana webových kamer

To, že hackeři mohou převzít kontrolu nad Vaší webkamerou a sledovat Vás již není žádnou novinkou a způsoby ochrany, jako odebrání výsad aplikacím, zakázání vestavěné kamery v zařízení, nebo její zakrytí, nejsou příliš praktické. Aby zabránil pokusům o získání přístupu do Vašeho soukromí,Bitdefender Ochrana webových kamer neustále monitoruje aplikace, které se snaží získat přístup k Vaší webkameře, a blokuje ty, které nejsou zaznamenány jako důvěryhodné.

Jakožto bezpečnostní opatření budete upozorněni pokaždé, když se nedůvěryhodná aplikace pokusí získat přístup k vašemu fotoaparátu.

Zapnutí nebo vypnutí Ochrany webových kamer

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **OCHRANA VIDEO & AUDIO** klikněte na **Nastavení**.
3. Nyní přejděte do okna **Nastavení** a zapněte nebo vypněte příslušný přepínač.

Nastavování Ochrany webových kamer

Můžete nastavit, jakých pravidel má být využito v případě, že se některá aplikace pokusí získat přístup k Vaší kameře, pomocí následujících kroků:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **OCHRANA VIDEO & AUDIO** klikněte na **Nastavení**.
3. Přejděte na kartu **Nastavení** .

K dispozici jsou následující možnosti:

Pravidla pro blokování aplikací

- **Zakázat veškerý přístup k webkameře** - žádná aplikace nebude mít povolen přístup k Vaší webkameře.
- **Blokovat přístup k webkameře prohlížečům** - žádný internetový prohlížeč kromě Internet Explorer a Microsoft Edge nebude mít povolen přístup k Vaší webkameře. Kvůli proceduře Windows store, kdy všechny jejich aplikace pracují jako jeden proces, Bitdefender nedokáže rozpoznat Internet Explorer a Microsoft Edge jako internetové prohlížeče, a proto jsou vyloučeny z tohoto nastavení.
- **Nastavit přístup aplikace k webkameře na základě volby uživatelů** pokud většina uživatelů Bitdefender považuje oblíbenou aplikaci za neškodnou, její přístup k webkameře bude automaticky povolen. Pokud je oblíbená aplikace většinou uživatelů považována za nebezpečnou, její přístup bude automaticky blokován.

  Budete upozorněni pokaždé, když některá z vašich nainstalovaných aplikací bude zaznamenána jako blokovaná většinou uživatelů Bitdefender.

Upozornění

- **Upozornit, když se povolené aplikace připojí k webové kameře** - budete upozorněni pokaždé, když povolená aplikace přistoupí k vaší webové kameře.

Přidání aplikací do seznamu Ochrany webových kamer

Aplikace, které se pokusí připojit k Vaší webkameře jsou automaticky rozpoznány jejich přístuo je povolen nebo blokován v závislosti na jejich chování a na rozhodnutí komunity. Nicméně můžete také sami ručně nastavit, jaká opatření by měla být přijata, pomocí následujících kroků:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **OCHRANA VIDEO & AUDIO** klikněte na **Nastavení**.
3. Přejděte do okna **Ochrana webové kamery** .
4. Klikněte na okno **Přidat aplikaci** .
5. Klikněte na požadovaný odkaz:
   - **Z Windows Store** - zobrazí se seznam detekovaných aplikací Windows Store. Zapněte přepínače vedle aplikací, které chcete přidat do seznamu.

- **Z vašich aplikací** - přejděte do souboru .exe, který chcete přidat do seznamu, a poté klikněte na **OK** .

Pro zobrazení informací o tom, co se ostatní uživatelé produktu Bitdefender rozhodli udělat s vybranou aplikací, klikněte na ikonu .

Aplikace, které budou požadovat přístup k Vaší kameře se společně s časem poslední aktivitiy zobrazí v tomto okně.

Budete upozorněni pokaždé, když je některá z povolených aplikací zablokována uživateli Bitdefender.

Pro zastavení přístupu přidaných aplikací k vaší webové kameře, klikněte na ikonu . Ikona se změní na , znamená, že zvolené aplikace nebudou mít k webkameře přístup.

20.2. Monitor mikrofonu

Nebezpečné aplikace mohou přistupovat k vestavěnému mikrofonu tiše nebo na pozadí bez vašeho souhlasu. Aby jste si byli vědomi potenciálních škodlivých zneužití, Bitdefender Monitor Mikrofonu vás na takové události upozorní. Tímto způsobem, žádná aplikace nebude moci získat přístup k mikrofonu.

Zapnutí nebo vypnutí Monitoru mikrofonu.

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **OCHRANA VIDEO & AUDIO** klikněte na **Nastavení**.
3. Vyberte okno **Nastavení** .
4. V okně **Nastavení** zapněte nebo vypněte přepínač **Mikrofon** .

Konfigurace oznámení pro Monitor mikrofonu

Chcete-li nakonfigurovat, která oznámení se mají zobrazit, pokud se aplikace pokusí získat přístup k mikrofonu, postupujte takto:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **OCHRANA VIDEO & AUDIO** klikněte na **Nastavení**.
3. Přejděte do okna **Nastavení** .

Upozornění

- **Upozornit, když se aplikace pokusí o přístup k mikrofonu**
- **Upozornit, když prohlížeče přistupuje k mikrofonu**
- **Upozornit, když se nedůvěryhodné aplikace snaží o přístup k mikrofonu.**
- **Zobrazit oznámení na základě volby uživatelů Bitdefender**

Přidání aplikací do seznamu Monitoru mikrofonu

Aplikace, které se pokusí připojit k vašemu mikrofonu, budou automaticky rozpoznány a přidány do seznamu oznámení. Zda se má oznámení zobrazovat nebo ne, můžete ručně nakonfigurovat sami podle následujících kroků:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **OCHRANA VIDEO & AUDIO** klikněte na **Nastavení**.
3. Přejděte do okna **Ochrana zvuku** .
4. Klikněte na okno **Přidat aplikaci** .
5. Klikněte na požadovaný odkaz:
   - **Z Windows Store** - zobrazí se seznam detekovaných aplikací Windows Store. Zapněte přepínače vedle aplikací, které chcete přidat do seznamu.
   - **Z vašich aplikací** - přejděte do souboru .exe, který chcete přidat do seznamu, a poté klikněte na **OK** .

Pro zobrazení informací o tom, co se ostatní uživatelé produktu Bitdefender rozhodli udělat s vybranou aplikací, klikněte na ikonu .

Aplikace, které budou požadovat přístup k vašemu mikrofonu, se společně s časem poslední aktivity zobrazí v tomto okně.

Chcete-li přestat dostávat oznámení týkající se aktivity přidané aplikace, klikněte na ikonu . Ikona se změní na , což znamená, že se nezobrazí žádné oznámení Bitdefender, když se zvolené aplikace pokusí o přístup k vašemu mikrofonu.

21. ZOTAVENÍ PO INFEKCI RANSOMWARE

Bitdefender Náprava Ransomware zálohu vaše soubory jako jsou dokumenty, obrázky, videa nebo muzika, aby vám zajistil, že budete chráněni, před poškozením nebo ztrátou v případě zašifrování ransomwarem. Při každém detekovaném útoku ransomware, Bitdefender zablokuje všechny procesy zapojené do útoku a začne procesy napravovat. Tímto způsobem, budete moci obnovit obsah vašich celých souborů, bez placení za výkupné.

21.1. Zapnutí nebo vypnutí ochrany před ransomwarem

Pro zapnutí nebo vypnutí ochrany před ransomwarem:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V panelu **NÁPRAVA RANSOMWARE**, zapněte nebo vypněte vypínač.

> **Poznámka**
> Pro ujištění, že vaše soubory jsou chráněny proti ransomware, doporučujeme aby jste Nápravu Ransomware nechaly zapnutou.

21.2. Zapínání a vypínaní automatické obnovy

Automatická Obnova zajišťuje, které vaše soubory jsou automaticky obnovené v případě šifrování ransomwarem.

Pro zapnutí nebo vypnutí automatické obnovy:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V panelu **NÁPRAVA RANSOMWARE**, klikněte na **Nastavení**.
3. V okně Nastavení zapněte nebo vypněte přepínač **Automatické obnovení** .

21.3. Zobrazování souborů, které byly automaticky obnoveny

Když je možnost **Automatické obnova** zapnutá, Bitdefender bude automaticky obnovovat soubory, které byly zašifrovány ransomwarem. Tím si můžete vychutnat bezstarostný zážitek s vědomím, že vaše soubory jsou bezpečné.

Pro zobrazení souborů, které byly automaticky obnovené:

1. Klikněte na **Upozornění** v navigačním menu v rozhraní Bitdefender.

2. V záložce **Vše**, vyberte upozornění týkající se nejnovější vylepšené chování ransomware a klikněte na **Obnovit Soubory**.

   Zobrazí se seznam se obnovenými soubory. Zde můžete také zobrazit místo, kde jsou vaše soubory obnoveny.

21.4. Ruční obnovení zašifrovaných souborů

V případě, že musí manuálně obnovit soubory, které byly zašifrovány ransomwarem, postupujte podle těchto kroků:

1. Klikněte na **Upozornění** v navigačním menu v rozhraní Bitdefender.
2. V záložce **Vše**, vyberte upozornění ohledně nejnovějších detekovaných chování ransomware, a poté klikněte na **Šifrované Soubory**.
3. Seznam se zašifrovanými soubory se zobrazí.

   Pokračujte kliknutím na **Obnovit soubory** .
4. V případě celého nebo části selhání obnovovacího procesu, musíte vybrat umístěného, kde se dešifrované soubory mohou uložit. Klikněte na **Obnovit polohu** a poté vyberte umístění v počítači.
5. Zobrazí se potvrzovací okno.

   Proces obnovení dokončíte kliknutím na **Dokončit** .

Soubory s následujícími příponami, mohou být obnoveny v případě že jsou zašifrovány:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

21.5. Přidávání aplikací do výjimek

Můžete nastavit pravidla výjimek pro aplikace, kterým věříte, tak že funkce Náprava Ransomware je nebude blokovat, pokud projeví akci podobnou ransomware.

Pro přidání aplikace do seznamu výjimek v Nápravě Ransomware:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V panelu **NÁPRAVA RANSOMWARE**, klikněte na **Nastavení**.
3. Přejděte do okna **Výjimky** a klikněte na **+ Přidat výjimku** .

22. OCHRANA VAŠICH OSOBNÍCH DAT SPRÁVCEM HESEL

Pomocí našich zařízení nakupujeme online nebo platíme účty, připojujeme se k platformám sociálních médií nebo se přihlašujeme pomocí aplikací pro rychlé zasílání zpráv.

Jak však každý ví, není vždy snadné si zapamatovat heslo.

A pokud při procházení webu nejsme opatrní, naše osobní informace, jako emailová adresa, ID služby zasílání zpráv nebo údaje o kreditní kartě, mohou být vyzrazeny.

Zapisovat si hesla nebo osobní údaje na papír nebo do počítače může být nebezpečné, protože mohou být přístupné lidem, kteří chtěji tyto informace zcizit a zneužít. A pamatovat si každé heslo, které jste nastavili ve vašich online účtech a pro oblíbené webové stránky, není snadný úkol.

Existuje tedy způsob, jak zajistit, abychom našli svá hesla, když je potřebujeme? A můžeme mít jistotu, že naše tajná hesla jsou stále v bezpečí?

Správce hesel vám pomáhá sledovat vaše hesla, chrání vaše soukromí a zajišťuje bezpečné procházení webu.

Správce hesel, který používá jedno hlavní heslo pro přístup k vašim osobním datům, vám pomáhá uchovávat vaše hesla v bezpečí v portmonce.

Pro zajištění nejlepší ochrany vašich online aktivit je do prohlížeče Bitdefender Safepay™ integrován Správce hesel, který poskytuje sjednocené řešení pro různé způsoby, kterými mohou být vyzrazena vaše osobní data.

Správce hesel chrání následující osobní informace:

- Osobní informace, jako emailová adresa nebo telefonní číslo
- Přihlašovací údaje k webovým stránkám
- Informace o bankovních účtech nebo čísla kreditních karet
- Přístup k datům k emailovým účtům
- Hesla pro aplikace
- Hesla k sítím Wi-Fi

22.1. Vytvoření nové portmonkové databáze

Bitdefender - Portmonka je místo, do kterého můžete ukládat svá osobní data. Pro pohodlnější prohlížení internetu si vytvořte portmonkovou databázi podle následujících kroků:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** vyberte **Nastavení**.
3. V okně **Moje peněženky** klikněte na **Přidat peněženku** .
4. Klikněte na **Vytvořit nový** .
5. Zadejte požadované informace do příslušných polí.
   - Název peněženky - zadejte jedinečný název pro vaši databázi Peněženky.
   - Hlavní heslo - zadejte heslo pro vaši portmonku.
   - Nápověda - zadejte nápovědu pro připomenutí hesla.
6. Klikněte na tlačítko **Pokračovat**.
7. V tomto kroku si můžete vybrat, zda chcete své informace uložit do cloudu, a to aktivací přepínače vedle položky **Synchronizovat všechny mé přístroje** . Vyberte požadovanou možnost a poté klikněte na tlačítko **Pokračovat**.
8. Otevřete webový prohlížeč, ze kterého chcete importovat přihlašovací údaje.
9. Klikněte na tlačítko **Dokončit**.

22.2. Importovat existující databázi

Pro importování lokálně uložené portmonkové databáze:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** vyberte **Nastavení**.
3. V okně **Moje peněženky** klikněte na **Přidat peněženku** .
4. Klikněte na **Import existující databáze** .
5. Vyhledejte v zařízení místo, kde jste uložili databázi peněženky, a vyberte ji.
6. Klikněte na **Otevřít**.

7. Pojmenujte svou Portmonku a zadejte heslo, které jste poprvé použili při její tvorbě.
8. Klikněte na **Importovat**.
9. Zvolte programy, ze kterých chcete, aby Portmonka importovala přihlašovací údaje, a poté klikněte na tlačítko **Dokončit**.

22.3. Export portmonkové databáze

Chcete-li exportovat databázi portmonky:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** vyberte **Nastavení**.
3. Přejděte do okna **Moje peněženky** .
4. Klikněte na ikonu ••• na požadované portmonce a poté zvolte **Exportovat**.
5. Vyhledejte v zařízení místo, kam chcete uložit databázi peněženky, a poté pro ni vyberte název.
6. Klikněte na tlačítko **Save**.

Poznámka
Aby byla funkce **Exportovat** dostupná, Portmonka musí být otevřená.
Pokud je peněženka, kterou chcete exportovat, uzamčena, klikněte na **Aktivovat peněženku** a poté zadejte heslo, které bylo při prvním vytvoření přiřazeno.

22.4. Synchronizace vašich portmonek do cloudu

Chcete-li zapnout nebo vypnout synchronizaci portmonky s cloudem:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** vyberte **Nastavení**.
3. Přejděte do okna **Moje peněženky** .
4. Klikněte na ikonu ••• na požadované portmonce a poté zvolte **Nastavení**.
5. V zobrazeném okně vyberte požadovanou možnost a poté klikněte na tlačítko **Uložit**.

Poznámka
Aby byla funkce **Exportovat** dostupná, Portmonka musí být otevřená. Pokud je portmonka, kterou chcete synchronizovat, uzamčená, klikněte na tlačítko **AKTIVOVAT PORTMONKU** a poté zadejte heslo, které jste poprvé použili při její tvorbě.

22.5. Správa přihlašovacích údajů v Portmonce

Pro správu vašich hesel:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** vyberte **Nastavení**.
3. Přejděte do okna **Moje peněženky** .
4. Vyberte požadovanou databázi Peněženky a potom klikněte na **Aktivovat peněženku** .
5. Zadejte Hlavní heslo a poté klikněte **OK**.

Objeví se nové okno. Vyberte požadovanou kategorii v horní části okna:

- Identita
- Webové stránky
- Online banking
- Emaily
- Aplikace
- Sítě Wi-Fi

Přidávání/úpravy přihlašovacích údajů

- Chcete-li přidat nové heslo, vyberte nahoře požadovanou kategorii, klikněte na Tlačítko **+ Přidat položku**, zadejte informace do příslušných polí a klikněte na tlačítko Uložit.
- Chcete-li upravit položku z tabulky, vyberte ji a klikněte na tlačítko **Upravit** na pravé straně.
- Pro smazání položky ji vyberte a klikněte na tlačítko **Odstranit**.

22.6. Zapnutí nebo vypnutí ochrany Správcem hesel

Chcete-li zapnout nebo vypnout ochranu správce hesel:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** zapněte nebo vypněte přepínač.

22.7. Správa nastavení Správce hesel

Chcete-li konfigurovat detaily hlavního hesla:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** vyberte **Nastavení**.
3. Přejděte do okna **Nastavení** .

V části **Nastavení zabezpečení** jsou k dispozici následující možnosti:

- **Zeptat se na hlavní heslo, když se přihlásím k zařízení** - budete vyzváni k zadání hlavního heslo, když budete přistupovat k zařízení.
- **Zeptat se na hlavní heslo po otevření prohlížeče nebo aplikace** - při přístupu k prohlížeči nebo aplikaci budete vyzváni k zadání vašeho hlavního hesla.
- **Nepožádat mě o hlavní heslo** - při přístupu k zařízení, prohlížeči nebo aplikaci nebudete vyzváni k zadání hlavního hesla.
- **Automaticky zamknout portmonku, když opustím zařízení** - budete vyzváni k zadání hlavního heslo, pokud opustíte zařízení na více jak 15 minut.

> **Důležité**
> Hlavní heslo si zapamatujte nebo si záznam o něm uschovejte na bezpečném místě. Pokud heslo zapomenete, bude nutné program přeinstalovat nebo kontaktovat podporu produktu Bitdefender.

Vylepšení komfortu

Chcete-li vybrat prohlížeče nebo aplikace, do kterých se má integrovat Správce hesel:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** vyberte **Nastavení**.
3. Vyberte okno **Nastavení** .

Chcete-li použít Správce hesel a vylepšit své prostředí, zapněte přepínač vedle aplikace:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safepay

Konfigurace automatického vyplňování

Funkce automatického vyplňování vám usnadňuje připojení k oblíbeným webovým stránkám nebo přihlašování k účtům online. Při prvním zadání přihlašovacích údajů a osobních informací do webového prohlížeče se tato data automaticky uloží do Portmonky.

Pro konfiguraci nastavení **Automatického vyplňování**:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** vyberte **Nastavení**.
3. V okně **Nastavení** přejděte na kartu **Nastavení automatického vyplňování** .
4. Nakonfigurujte následující možnosti:
   - **Konfigurace způsobu, jakým Správce hesel zabezpečuje vaše přihlašovací údaje**:
     - **Přihlašovací údaje automaticky ukládat do portmonky** - přihlašovací údaje a další identifikovatelné informace, jako vaše osobní údaje a podrobnosti o kreditních kartách, se automaticky uloží a odešlou do Portmonky.
     - **Vždy se mě zeptat** - pokaždé budete dotázáni, zda chcete přidat své přihlašovací údaje do Portmonky.
     - **Neukládat, zadám si informace ručně** - přihlašovací údaje lze do Portmonky přidat pouze ručně.
   - **Automatické vyplňování přihlašovacích údajů**:
     - **Přihlašovací údaje automaticky vyplnit vždy** - přihlašovací údaje se automaticky vloží do prohlížeče.
   - **Automatické vyplňování formulářů**:

- **Nabídnout možnost vyplnění, když navštívím stránku s formulářem** - vždy, když produkt Bitdefender zjistí, že chcete provést online platbu nebo se přihlásit, zobrazí se vyskakovací okno s možnostmi vyplňování.

Správa informací ve Správci hesel z vašeho prohlížeče

Podrobnosti ve Správci hesel můžete snadno spravovat přímo z prohlížeče, abyste měli všechny důležité údaje po ruce. Doplněk Bitdefender - Portmonka je podporován následujícími prohlížeči: Google Chrome, Internet Explorer a Mozilla Firefox a rovněž je integrován do prohlížeče Safepay.

Pokud chcete přejít do rozšíření Bitdefender- Portmonka, otevřete webový prohlížeč, povolte instalaci doplňku a klikněte na ikonu  na liště nástrojů.

Rozšíření Bitdefender - Portmonka obsahuje následující možnosti:

- Otevřít portmonku - otevře portmonku.
- Uzamknout portmonku - uzamkne portmonku.
- Webové stránky - otevře podnabídku se všemi přihlášeními k webovým stránkám uložených v portmonce. Klikněte na **Přidat webovou stránku** pro přidání nové webové stránky do seznamu.
- Vyplňte formulář - Otevře podnabídku obsahující informace, které jste přidali pro konkrétní kategorii. Odsud můžete do portmonky přidávat nová data.
- Generátor hesel - umožňuje generovat náhodná hesla, která můžete použít pro nové i stávající účty. Složitost hesla můžete přizpůsobit po kliknutí na položku **Zobraz pokročilá nastavení**.
- Nastavení - otevře okno nastavení Správce hesel.
- Nahlásit problém - hlášení problémů, se kterými se setkáte ve Správci hesel produktu Bitdefender.

23. ANTI-TRACKER

Mnoho navštívených webových stránek používá trackery ke shromažďování informací o vašem chování, a to buď pro sdílení informací se společnostmi třetích stran, nebo pro zobrazování reklam, které jsou pro vás nejrelevantnější. Majitelé webových stránek tímto způsobem vydělávají peníze, aby vám mohli poskytovat obsah zdarma nebo pokračovat ve svém provozu. Kromě shromažďování informací mohou trackery zpomalit procházení webu nebo ztrácet šířku pásma.

S aktivovaným rozšířením Bitdefender Anti-tracker ve vašem prohlížeči, se vyhnete sledování, když jste online a urychlíte tak načítání webových stránek.

Rozšíření Bitdefender je kompatibilní s následujícími webovými prohlížeči:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Detekované trackery, jsou seskupeny do následujících kategorií:

- **Reklama** - slouží k analýze návštěvnosti webových stránek a k analýze chování uživatelů.
- **Interakce se zákazníkem** - slouží k měření interakce uživatele s různými vstupními formami, jako je chat nebo podpora.
- **Základní** - používá se k monitorování kritických funkcí webových stránek.
- **Analytika stránek** - slouží ke shromažďování údajů o používání webových stránek.
- **Sociální média** - slouží k monitorování sociálního publika, aktivity a zapojení uživatelů do různých platforem sociálních médií.

23.1. Rozhraní Anti-trackeru

Pokud je aktivováno rozšíření Bitdefender Anti-tracker, ve vašem prohlížeči se vedle ikony pro vyhledávání se zobrazí ikona  . Pokaždé, když navštívíte webovou stránku, lze na ikoně zaznamenat čítač s odkazem na detekované a blokované trackery. Chcete-li zobrazit další podrobnosti o blokovaných trackerech, klikněte na ikonu a otevřete rozhraní. Kromě počtu blokovaných trackerů, si můžete zobrazit čas potřebný pro načtení stránky a kategorie,

do kterých detekované trackery patří. Chcete-li zobrazit seznam sledovaných webových stránek, klikněte na požadovanou kategorii.

Chcete-li zakázat Bitdefender blokování trackerů na stránkách, které navštěvujete, klikněte na **Pozastavte ochranu na této webové stránce**. Toto nastavení platí pouze tehdy, pokud máte webovou stránku otevřenou a při zavření webu se vrátíte do výchozího stavu.

Chcete-li povolit trackerům sledování konkrétní aktivity, klikněte na požadovanou aktivitu a poté klikněte na odpovídající tlačítko. V případě, že si to rozmyslíte, znovu klikněte na to stejné tlačítko.

23.2. Vypnutí Bitdefender Anti-trackeru

Pro vypnutí Bitdefender Anti-tracker:

- Z webového prohlížeče:
  1. Otevřete svůj internetový prohlížeč.
  2. Klikněte na ikonu vedle řádku s adresou ve webovém prohlížeči.
  3. Klikněte na ikonu v pravém horním rohu.
  4. Vypněte pomocí odpovídajícího přepínače.

     Ikona Bitdefender se změní na šedou.
- Z rozhraní produktu Bitdefender:
  1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
  2. V okně **ANTI-TRACKER**, klikněte na **Nastavení**
  3. Vedle webového prohlížeče, pro který chcete zakázat rozšíření, vypněte odpovídající přepínač.

23.3. Povolení sledování webové stránky

Pokud chcete být sledováni při návštěvě určité webové stránky, můžete ji přidat k výjimkám následujícím způsobem:

1. Otevřete svůj internetový prohlížeč.
2. Vedle vyhledávacího panelu klikněte na ikonu .
3. Klikněte na ikonu v pravém horním rohu.

4. Pokud jste na webové stránce, kterou chcete přidat k výjimkám, klikněte na **Přidat aktuální webovou stránku do seznamu**.

   Chcete-li přidat další webovou stránku, zadejte její adresu do příslušného pole a klikněte na tlačítko .

24. VPN

Aplikace VPN může být nainstalována z vašeho produktu Bitdefender a můžete ji využít kdykoli budete chtít přidat svému připojení vrstvu ochrany navíc. VPN slouží jako tunel mezi vaším zařízením a sítí, ke které jste připojeni, chrání vaše připojení, šifruje data na úrovni šifrování v bankovnictví a skrývá vaši IP adresu, ať jste kdekoliv. Váš internetový provoz je přesměrováván přes oddělený server, čímž činí vaše zařízení téměř nemožné k identifikaci mezi nesčetnými dalšími zařízeními, které využívají našich služeb. Navíc, když jste připojeni k internetu s Bitdefender VPN, získáte přístup k obsahu, který je běžně v určitých lokalitách nepřístupný.

Poznámka
V některých zemích podléhá internet cenzuře a proto je používání VNP na jejich území zákonně zakázáno. Pro vyhnutí se právním důsledkům se při prvním spuštění aplikace Bitdefender VPN může zobrazit varovná zpráva. Pokračováním v používání aplikace potvrzujete, že jste si vědomi platných předpisů dané země a rizik, kterým můžete být vystaveni.

24.1. Instalace VPN

Aplikace VPN může být naistalována z vašeho rozhraní Bitdefender, a to následovně:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **VPN** klikněte na **Zapnout VPN**.
3. V okně s popisem VPN aplikace si přečtěte **Smlouvu o předplatném** a poté klikněte na **INSTALOVAT BITDEFENDER VPN**.

   Počkejte několik minut, než se soubory stáhnou a nainstalují.

   Pokud je detekována jiná VPN, doporučujeme ji odinstalovat. V případě instalace více řešení VPN se může vyskytnout zpomalení systému nebo jiné problémy s funkčností.
4. Klikněte na **OTEVŘÍT BITDEFENDER VPN** pro dokončení instalace.

Poznámka
Instalace Bitdefender VPN vyžaduje .Net Framework 4.5.2 nebo vyšší. V případě, že tento balíček nemáte nainstalovaný, se zobrazí okno s upozorněním. Klikněte na **instalovat .Net Framework** a budete přesměrováni na stránku, ze které můžete stáhnout nejnovější verzi tohoto softwaru.

24.2. Otevírám VPN

Pro přístup do hlavního rozhraní produktu Bitdefender VPN použijte jeden z následujících postupů:

- Z oznamovací oblasti
  1. Klikněte pravým tlačítkem myši na ikonu na systémové liště, a poté zvolte **Zobrazit**.
- Z rozhraní produktu Bitdefender:
  1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
  2. V okně **VPN** klikněte na **Otevřít VPN**.

24.3. Rozhraní VPN

Rozhraní VPN zobrazuje stav aplikace, připojené nebo nepřipojené. Serverové umístění je pro uživatele bezplatné verze automaticky nastaveno produktem Bitdefender na ten nejvhodnější server, zatímco prémioví uživatelé mají možnost změnit serverové umístění na to, ke kterému se chtějí připojit. Další informace o předplatném VPN naleznete na *„Předplatná“* (str. 147).

Pro připojení nebo odpojení jednoduše klikněte na stav, který je zobrazen v horní části obrazovky, nebo klikněte pravým tlačítkem na ikonu na liště. Ikona na systémové liště je zaškrtnutá zeleně, když je VPN připojená, a červeně, když je odpojená.

Během připojení je uplynulý čas zobrazen ve spodní části uživatelského rozhraní.

Chcete-li zcela zobrazit oblast **Menu** , klikněte na ikonu v levé horní části. Zde jsou k dispozici následující možnosti:

- **Můj účet** - zobrazuje podrobnosti o vašem Bitdefender účtu a VPN předplatném Chcete-li se přihlásit pomocí jiného účtu, klikněte na **Přepnout účet**.

  Klikněte na **Přidat sem** a přidejte aktivační kód pro Bitdefender Premium VPN.

- **Nastavení** - můžete upravovat chování produktu dle svých potřeb. Nastavení jsou seskupena do dvou kategorií:
  - **Hlavní**
    - Upozornění

- Spuštění - vyberte, zda chcete spustit Bitdefender VPN při spuštění nebo ne
- Hlášení o produktech - odesílejte anonymní zprávy o produktech, které nám pomohou vylepšit vaše prostředí
- Dark mód
- Jazyk

- **Pokročilé**
  - Internet Kill-Switch - tato funkce dočasně pozastaví veškerý internetový provoz, pokud dojde k náhodnému výpadku připojení VPN. Jakmile se vrátíte do režimu online, bude připojení VPN obnoveno.
  - Autoconnect - Připojte Bitdefender VPN automaticky při přístupu k veřejné/nezabezpečené síti Wi-Fi nebo při spuštění aplikace pro sdílení souborů typu peer-to-peer

- **Podpora** - máte přístup k platformě Centra podpory, odkud si můžete přečíst užitečný článek o tom, jak používat Bitdefender VPN nebo nám poslat zpětnou vazbu.
- **Informace o aplikaci** - vidíte informace o aktuálně nainstalované verzi.

24.4. Předplatná

Bitdefender VPN nabízí denní kvótu 200 MB přenosu na zařízení, a tak zabezpečuje vaše připojení, kdykoli potřebujete, a automaticky vás připojí k nejvýhodnějšímu serverovému umístění.

Pro neomezený přenos a neomezený přístup k obsahu z celého světa pomocí volby libovolného umístění serveru, přejděte na prémiovou verzi.

Na verzi Bitdefender Premium VPN můžete kdykoli upgradovat kliknutím na tlačítko **Upgradovat** dostupné v rozhraní produktu.

Předplatné pro Bitdefender Premium VPN je nezávislé na předplatném produktu Bitdefender Internet Security, takže ho můžete využívat v celém jeho rozsahu, nehledě na stav předplatného pro antivirus. V případě, že předplatné pro Bitdefender Premium VPN vyprší, ale to pro Bitdefender Internet Security je stále aktivní, budete přepnuti zpět na bezplatnou verzi.

Bitdefender VPN je multiplatformový produkt, k dostání v produktech Bitdefender kompatibilních s Windows, macOS, Android a iOS. Jakmile

přejdete na prémiový účet, budete moci používat své předplatné pro všechny pro všechny produkty, pokud se přihlásíte s tím samým Bitdefender účtem.

25. ZABEZPEČENÍ SAFEPAY PRO ONLINE TRANSAKCE

Počítač se rychle stává hlavním nástrojem pro nákupy a bankovnictví. Placení účtů, převody peněz, nákupy takřka všeho, co si dokážete představit, jsou stále rychlejší a jednodušší.

Při tom je třeba odesílat osobní data, údaje o účtech a kreditních kartách a další druhy soukromých informací po Internetu, což je přesně ten druh dat, o který se velmi zajímají počítačoví piráti. Hackeři se neustále snaží tyto informace zcizit, takže zabezpečení vašich online transakcí musíte věnovat maximální péči.

Bitdefender Safepay™ je především chráněný prohlížeč, zabezpečené prostředí, které slouží k tomu, aby vaše online bankovnictví, nákupy v e-shopech a další druhy online transakcí byly soukromé a bezpečné.

Pro co nejlepší ochranu soukromí byl do prostředí Bitdefender Safepay™ integrován Správce hesel Bitdefender, který zabezpečuje vaše osobní údaje při přístupu k umístěním online. Další informace viz *„Ochrana vašich osobních dat správcem hesel“* (str. 135).

Prohlížeč Bitdefender Safepay™ nabízí následující funkce:

- Blokuje přístup k ploše a jakékoli pokusy o pořízení snímků obrazovky.
- Chrání vaše tajná hesla při procházení webu pomocí Správce hesel.
- Je vybavený virtuální klávesnici, která znemožňuje hackerům číst stisky kláves.
- Je zcela nezávislý na vašich ostatních prohlížečích.
- Dodává se s vestavěnou ochranou hotspotu, která se používá, když je zařízení připojeno k nezabezpečeným sítím Wi-Fi.
- Podporuje záložky a umožňuje přecházet mezi vašimi oblíbenými stránkami bank a e-shopů.
- Není omezený na bankovnictví a e-shopy. V prohlížeči Bitdefender Safepay™ lze otevřít libovolnou webovou stránku.

25.1. Použití prohlížeče Bitdefender Safepay™

Ve výchozím nastavení Bitdefender detekuje, když v kterémkoli prohlížeči v zařízení přejdete na web online bankovnictví nebo online obchod a vyzve vás k jeho spuštění v Bitdefender Safepay™.

Pro přístup do hlavního rozhraní prohlížeče Bitdefender Safepay™ použijte jeden z následujících postupů:

- Z rozhraní produktu Bitdefender:
  1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
  2. V okně **Safepay** klikněte na **Nastavení**.
  3. V okně **Safepay** klikněte na **Spustit Safepay** .
- V systému Windows:
  - V systému **Windows 7**:
    1. Klikněte na nabídku **Start** a přejděte do nabídky **Všechny programy**.
    2. Klikněte na položku **Bitdefender**.
    3. Klikněte na položku **Bitdefender Safepay™**.
  - V systémech **Windows 8 a Windows 8.1**:

    Na úvodní obrazovce systému Windows najděte položku Bitdefender Safepay™ (můžete například začít psát „Bitdefender Safepay™“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
  - V systému **Windows 10**:

    Do vyhledávacího pole na hlavním panelu zadejte „Bitdefender Safepay™“ a klikněte na příslušnou ikonu.

Pokud jste zvyklí na ovládání webových prohlížečů, s používáním prohlížeče Bitdefender Safepay™ nebudete mít žádné potíže - vypadá a chová se jako běžný prohlížeč:

- v panelu adresy zadejte adresu URL, na kterou chcete přejít.
- přidáváním panelů můžete otevřít více stránek v okně prohlížeče Bitdefender Safepay™ kliknutím na tlačítko  .
- ve stránkách se můžete pohybovat zpět a vpřed a obnovovat je pomocí tlačítek  .
- kliknutím na položku a výběrem možnosti **Nastavení** přejdete do nastavení prohlížeče Bitdefender Safepay™.

- kliknutím na  aktivujete ochranu vašich hesel pomocí Správce hesel.
- kliknutím na  vedle panelu adresy můžete spravovat vaše záložky.
- kliknutím na  otevřete virtuální klávesnici.
- velikost prohlížeče zvýšíte nebo snížíte současným stisknutím kláves **Ctrl +/-** na numerické klávesnici.
- kliknutím na a výběrem možnosti **O produktu** zobrazíte informace o produktu Bitdefender.
- vytiskněte důležité informace klepnutím na tlačítko a výběrem položky **Tisk**.

Poznámka
Pro přepínání mezi Bitdefender Safepay™ a plochou Windows stiskněte klávesy **Alt+Tab**, nebo klikněte na možnost **Přepnout na Plochu** v horní levé části okna.

25.2. Konfigurace nastavení

Klikněte na a po výběru položku **Nastavení** proveďte konfiguraci prohlížeče Bitdefender Safepay™:

Použít Bitdefender Safepay pravidla pro přístup domény
Zde se zobrazí webové stránky, které jste přidali do ZÁLOŽEK s povolenou možností **Automaticky otevřít v Safepay**. Chcete-li přes webovou stránku ze seznamu přestaňte automaticky otevírat stránku Bitdefender Safepay ™, klepněte na sloupec **Odstranit** na tlačítko × vedle požadované položky.

Blokování vyskakovacích oken
Kliknutím na příslušný přepínač můžete nastavit blokování vyskakovacích oken.

Můžete rovněž vytvořit seznam webových stránek, na kterých budou vyskakovací okna povolena. Seznam by měl obsahovat pouze webové stránky, kterým plně důvěřujete.

Chcete-li přidat stránku do seznamu, zadejte její adresu do příslušného pole a klikněte na tlačítko **Přidat doménu**.

K odstranění webu z listu vyberte X u odpovídajícího záznamu.

Manage Plugins
Můžete si vybrat, zda chcete povolit nebo zakázat konkrétní moduly v Bitdefender Safepay™.

Spravovat certifikáty
Můžete importovat certifikáty ze systému do úložiště certifikátů.

Klepněte na **DŮLEŽITÉ** a postupujte podle pokynů pro použití certifikátů v Bitdefender Safepay™.

Použít virtuální klávesnici
Virtuální klávesnice se automaticky zobrazí když je vybráno pole pro heslo.

Použít odpovídající přepínač pro zapnutí nebo vypnutí funkce.

Potvrzení tisku
Povolte tuto funkci, pokud si přejete dát svůj souhlas před zahájením tisku.

25.3. Správa záložek

Pokud jste vypnuli automatickou detekci některých nebo všech webových stránek, nebo jestliže produkt Bitdefender některé webové stránky nerozpozná, můžete do prohlížeče Bitdefender Safepay™ přidat záložky, abyste v budoucnu mohli snadno otvírat oblíbené stránky.

Pomocí následujícího postupu přidáte adresu URL do záložek prohlížeče Bitdefender Safepay™:

1. Klepnutím na ••• a výběrem **Záložky** otevřete stránku Záložky.

   Poznámka
   Stránka záložek se implicitně zobrazí při spuštění prohlížeče Bitdefender Safepay™.

2. Klikněte na tlačítko **+** a přidejte novou záložku.
3. Zadejte adresu URL a název záložky a klikněte na tlačítko **Vytvořit**. Pokud chcete stránku uloženou do záložek otevřít v prohlížeči Bitdefender

Safepay™ při každé návštěvě, zaškrtněte políčko **Automaticky otevřít v Safepay**. Adresa URL se rovněž přidá do seznamu domén na stránce nastavení.

25.4. Vypnutí upozornění Safepay

Když je rozpoznána bankovní stránka, produkt Bitdefender je nastaven tak, aby vás upozornil prostřednictvím vyskakovacího okna.

Pro vypnutí upozornění Safepay:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **Safepay** klikněte na **Nastavení**.
3. V okně **Nastavení** vypněte přepínač u položky **Safepay upozornění** .

25.5. Používání VPN se Safepay

Pro provádění online plateb v bezpečném prostředí během připojení k nezabezpečeným sítím, produkt Bitdefender lze nastavit tak, aby automaticky spustil aplikaci VPN současně se Safepay.

Abyste začali používat aplikaci VPN současně se Safepay:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **Safepay** klikněte na **Nastavení**.
3. V okně **Nastavení** zapněte přepínač vedle položky **Použít VPN se Safepay** .

26. RODIČOVSKÁ KONTROLA

Bitdefender Rodičovská kontrola vám umožňuje spravovat a chránit online aktivity vašich dětí. Jakmile nakonfigurujete Bitdefender Rodičovskou kontrolu, můžete snadno zjistit, co vaše děti dělají na zařízeních, která používají, a místa, kde byly v posledních 24 hodinách. Abyste měli lepší přehled o tom, co vaše dítě dělá, aplikace vám navíc poskytuje statistiky o jeho činnostech a zájmech.

Ve vašem předplatném Bitdefender jsou zahrnuty následující funkce:

- V zařízeních se systémem Windows, MacOS a Android:
  - Blokování nevhodných stránek.
  - Blokování aplikací jako jsou hry, chat, programy pro sdílení souborů a další.
  - Blokovat používání sledovaného zařízení.
  - Blokování přístupu k internetu během určitého času (jako například během školního vyučování).
  - Nastavení časových omezení pro používání zařízení.
  - Zobrazení průměrného času stráveného dětmi na zařízení.
  - Zobrazení přehledu s aplikacemi používanými ve sledovaném zařízení za posledních 30 dní.
  - Nastavte zakázané oblasti.
  - Najděte umístění zařízení s Androidem svého dítěte.
- Na zařízeních se systémem iOS:
  - Blokovat příchozí hovory ze seznamu kontaktů.
  - Nastavte zakázané oblasti.
  - Lokalizujte zařízení s iOS vašeho dítěte.

Chcete-li zkontrolovat online aktivity svých dětí, spravovat zařízení, která vaše děti používají, nebo změnit nastavení rodičovské kontroly, musíte se přihlásit ke svému Bitdefender účtu.

Jsou zde možnosti, jak můžete přistupovat na svůj Bitdefender účet,a to buď z webového prohlížeče prostřednictvím služby

https://central.bitdefender.com, nebo z Bitdefender Central, který lze nainstalovat na systémech s Androidem a iOS.

Pro nainstalování aplikace Bitdefender Central na vaše zařízení:

- **Na Androidu** - hledejte na Google Play Bitdefender Central a poté stáhněte a nainstalujte aplikaci. Následujte požadované kroky pro dokončení instalace.
- **Na iOS** - hledejte v App Store Bitdefender Central a poté stáhněte a nainstalujte aplikaci. Následujte požadované kroky pro dokončení instalace.

Poznámka
V tomto materiálu máte k dispozici možnosti a pokyny dostupné na webové platformě.

26.1. Přístup k nastavení Parental Control - My Children

Po vstupu do části Parental Control je k dispozici okno **My Children**. Zde můžete začít vytvářet profily pro své děti a později je můžete prohlížet a upravovat. Profily se zobrazují jako karty profilů a umožňují vám rychlou správu a přehlednou kontrolu stavu.

Jakmile vytvoříte profil, můžete začít přizpůsobovat podrobnější nastavení pro sledování a řízení přístupu vašich dětí k Internetu a konkrétním aplikacím.

K nastavení rodičovské kontroly můžete přistupovat z Bitdefender Central na jakémkoli počítači nebo mobilním zařízení připojeném k internetu.

Přejděte do vašeho Bitdefender účtu.

- Na kterémkoli zařízení s přístupem k Internetu:
  1. Přihlaš se na Bitdefender Central.
  2. Přihlaste se k účtu Bitdefender pomocí Vaší emailové adresy a hesla.
  3. Vyberte panel **Parental Control**.
  4. V zobrazeném okně můžete spravovat a konfigurovat profily rodičovské kontroly pro každé zařízení.
- Z rozhraní produktu Bitdefender:
  1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
  2. V okně **RODIČOVSKÝ KONTROLA** klikněte na **Konfigurovat**.

Budete přesměrováni na webovou stránku účtu Bitdefender. Přihlaste se pomocí svých přihlašovacích údajů.

3. Vyberte panel **Rodičovský poradce**.
4. V zobrazeném okně můžete spravovat a konfigurovat profily rodičovské kontroly pro každé zařízení.

Poznámka
Ujistěte se, že jste k zařízení přihlášeni pomocí účtu správce. Přístup k Rodičovskému poradci a jeho konfiguraci mají pouze uživatelé s oprávněními správy systému (správci systému).

26.2. Vytvořte profily pro své děti

Chcete-li začít sledovat aktivity vašeho dítěte, je třeba nakonfigurovat profil a nainstalovat aplikaci Bitdefender Parental Control Agent na zařízeních, která používá.

K vytvoření profilu dítěte:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel Parental Control.
3. V okně **Moje děti** klikněte na **PŘIDAT DĚTSKÝ PROFIL** .
4. Nastavte konkrétní informace, jako jméno, datum narození nebo pohlaví. Chcete-li přidat obrázek do profilu vašeho dítěte, klikněte na ikonu v pravém dolním rohu možnost **Obrázek profilu**. Pro pokračování klikněte na **ULOŽIT**.

   V závislosti na standardech rozvoje dítěte se nastavením věku dítěte automaticky načtou specifická nastavení pro prohlížení internetu, která jsou pro jeho věkovou kategorii považována za patřičná.
5. Klikněte na **PŘIDAT ZAŘÍZENÍ**.
6. Pokud je na zařízení Vašeho dítěte již nainstalován Bitdefender , vyberte jeho zařízení ze seznamu a poté zvolte účet, který chcete sledovat. KLIKNĚTE NA **PŘIŘADIT**.

   Pokud dítě nemá v zařízení, které používá, nainstalován žádný Bitdefender produkt, klepněte na tlačítko **Instalovat na novém zařízení** a poté klikněte na tlačítko**ODESLAT ODKAZ KE STAŽENÍ**. Do příslušného pole zadejte e-mailovou adresu a klikněte na **Odeslat e-mail** . Pamatujte, že

vygenerovaný odkaz ke stažení je platný pouze 24 hodin. Pokud doba platnosti odkazu vyprší, musíte vygenerovat nový pomocí stejných kroků.

Na zařízení, kde chcete nainstalovat Bitdefender zkontrolujte emailový účet, který jste zadaly, a poté klikněte na příslušné tlačítko stáhnout.

Důležité
Na zařízeních se systémem Windows a MacOS, která nemají nainstalovaný Bitdefender, bude nainstalován sledovací program Bitdefender Rodičovská Kontrola, který umožní sledovat online aktivity vašich dětí.
Na zařízení se systémem Android a iOS musí být stažena a nainstalována aplikace Bitdefender Rodičovská kontrola.

Chcete-li přiřadit další zařízení, klikněte na **PŘIDAT ZAŘÍZENÍ** vedle profilu dítěte. Postupujte podle pokynů v kroku 6 uvedených v této kapitole.

26.2.1. Instalace Bitdefender Rodičovské kontroly na zařízení se systémem Android a iOS

Chcete-li sledovat online aktivity svých dětí na zařízeních se systémem Android nebo iOS, musíte nainstalovat Rodičovskou kontrolu a poté propojit jejich zařízení s Bitdefender účtem. V závislosti na zařízeních, která vaše děti mají, postupujte takto:

- Na zařízení s **Android**:

  1. Přejděte do obchodu Google Play, vyhledejte Bitdefender Rodičovská kontrola a klepněte na možnost instalace.
  2. Když budete požádáni o povolení k oprávnění, klepněte na možnost **PŘIJMOUT**. Bitdefender potřebuje oprávnění k tomu, aby jste mohli být informováni o aktivitách Vašeho dítěte, a pokud je neschválíte, aplikace nebude nainstalována.
  3. Otevřete aplikaci Rodičovské kontroly.
  4. Při prvním spuštění aplikace se spustí úvodní průvodce obsahující detaily o funkcích produktu. Zvolte **DÁLE**, pokud chcete být dále naváděni, nebo **PŘESKOČIT** pro ukončení průvodce.
  5. Chcete-li pokračovat v instalaci, Bitdefender potřebuje váš souhlas se shromažďováním osobních údajů, týkající se vašeho dítěte a které budou použity pouze k poskytnutí informací o činnosti vašeho dítěte. Další podrobnosti získáte klepnutím na **Zásady ochrany osobních údajů**.

Klepnutím na **POKRAČOVAT** souhlasíte se shromažďováním osobních údajů ze zařízení.

6. Přihlaste se k vašemu stávajícímu účtu Bitdefender. Pokud účet Bitdefender nemáte, můžete si vytvořit nový pomocí příslušného tlačítka. Alternativně, se můžete přihlásit pomocí účtu Facebook, Google nebo Microsoft.
7. Klikněte na **ZAPNOUT** a budete přesměrováni na obrazovku, kde můžete zapnout možnost Usnadnění přístupu k aplikaci. Řiďte se pokyny na obrazovce pro správné nastavení aplikace.
8. Klikněte na **POVOLIT** a budete přesměrováni na obrazovku, kde můžete zapnout možnost Povolit přístup k užívání pro aplikaci. Řiďte se pokyny na obrazovce pro správné nastavení aplikace.
9. Klikněte na **AKTIVOVAT** a budete přesměrováni na obrazovku, kde můžete zapnout možnost Aktivovat práva správce zařízení pro aplikaci. Řiďte se pokyny na obrazovce pro správné nastavení aplikace.

   Tím zabráníte, aby vaše dítě aplikaci Parental Control Agent odinstalovalo.
10. Klikněte na **POVOLIT** a udělte všechna požadovaná oprávnění.
11. Přiřaďte zařízení k profilu Vašeho dítěte.

- Na zařízeních **iOS**:

1. Přejděte do obchodu Google Play, vyhledejte Bitdefender Rodičovská kontrola a klepněte na možnosti instalace.
2. Chcete-li pokračovat v instalaci, Bitdefender potřebuje váš souhlas se shromažďováním osobních údajů, týkající se vašeho dítěte a které budou použity pouze k poskytnutí informací o činnosti vašeho dítěte. Další podrobnosti získáte klepnutím na **Zásady ochrany osobních údajů**. Klepnutím na **Pokračovat** souhlasíte se shromažďováním osobních údajů ze zařízení.
3. Přihlaste se k vašemu stávajícímu účtu Bitdefender. Pokud účet Bitdefender nemáte, můžete si vytvořit nový pomocí příslušného tlačítka. Alternativně, se můžete přihlásit pomocí účtu Facebook, Google nebo Microsoft.
4. Budete požádán o povolení přístupu ke všem požadovaným oprávněním požadovaných aplikací. Klikněte na **Povolit**.

5. Povolte přístup k poloze Vašeho zařízení, aby ji mohl Bitdefender lokalizovat.
6. Povolte aplikaci zasílat oznámení. Pro správu upozornění Bitdefender, přejděte do Nastavení > Upozornění >Rodičovská kontrola
7. Abyste mohli sledovat kontakty svého dítěte, musíte povolit **Blokování hovorů & identifikaci**. Postupujte podle požadovaných kroků, abyste mohli použít Bitdefender Rodičovská kontrola pro omezení příchozích telefonních hovorů.
8. Přiřaďte zařízení k profilu Vašeho dítěte.

26.2.2. Sledování online aktivit vašich dětí

Bitdefender Rodičovská Kontrola vám umožňuje sledovat, co vaše dítě dělá na svém počítači. Tímto způsobem se můžete vždy přesně dozvědět, co za činnosti provozovali, zatímco trávily čas na přiřazených zařízeních.

V závislosti na provedených nastaveních poskytuje Bitdefender přehledy, které mohou obsahovat podrobné informace pro každou událost, například:

- Stav události.
- Závažnost oznámení.
- Název zařízení.
- Datum a čas výskytu události.

Pokud chcete sledovat internetový provoz, použité aplikace nebo aktivitu vašeho dítěte online:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel Parental Control.
3. Vyberte podřízený profil.

   V hlavním okně **Aktivita** si můžete zobrazit informace, které vás zajímají.

26.2.3. Konfigurace nastavení přehledů

Ve výchozím nastavení je při zapnuté Rodičovské kontrole zaprotokolována online aktivita vašich dětí.

Chcete-li dostávat e-mailová oznámení o online aktivitách svých dětí:

1. Přihlaš se na Bitdefender Central.

2. Vyberte panel Parental Control.
3. Klikněte na **NASTAVENÍ HLÁŠENÍ** .
4. Povolte odpovídající přepínač pro příjem zpráv o činnosti.
5. Zadejte emailovou adresu, na kterou mají být zasílána oznámení.
6. Upravte frekvenci výběrem: denně, týdně nebo měsíčně a poté klikněte na **ULOŽIT** .

Můžete si také zvolit, že se vám oznámení bude zobrazovat ve svém Bitdefender účtu, a to v následujících situacích:

- Pokaždé, když se vaše děti pokoušejí o přístup k blokovaným aplikacím (v systému Windows, MacOS a Android).
- Pokaždé, když vaše děti přijímají hovory z blokovaných/neznámých telefonních čísel (na iOS).
- Pokaždé, když vaše děti opustí bezpečnou oblast nebo vstoupí do zakázané.
- Pokaždé, když jsou vaše děti v bezpečí.

26.2.4. Úprava profilu

Pokud chcete upravit existující profil:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel **Parental Control**.
3. Klikněte na **MOŽNOSTI** na požadované kartě profilu a poté vyberte **Upravit profil** .
4. Po přizpůsobení požadovaných nastavení klikněte na **Uložit**.

26.2.5. Odebrání profilu

Pokud chcete odebrat existující profil:

1. Přihlaš se na Bitdefender Central.
2. Vyberte panel **Parental Control**.
3. Vyberte profil dítěte.
4. Klikněte na tlačítko **MOŽNOSTI** a vyberte možnost **Smazat profil**.
5. Potvrďte vaši volbu.

26.3. Konfigurace profilů Rodičovské Kontroly

Chcete-li začít monitorovat své děti, je třeba je přiřadit k zařízení s nainstalovanou aplikací Bitdefender Rodičovské kontroly.

Po přidání profilu vašeho dítěte můžete přizpůsobit další podrobná nastavení pro sledování a řízení přístupu k internetu a konkrétním aplikacím.

Chcete-li zahájit nastavení profilu, vyberte požadovanou kartu profilu a klikněte na **MOŽNOSTI**.

Klikněte na kartu a nakonfigurujte příslušnou funkci Rodičovského poradce pro zařízení:

- Screentime - zde můžete zablokovat přístup k zařízením, která jste určili v profilech svých dětí. Přístup může být omezen jak určitým časovým intervalem , tak pro denní limit.
- Aplikace - umožňuje zakázat přístup určitým aplikacím, například hrám, softwaru pro zasílání zpráv, filmům, apod.
- Webové stránky - zde můžete filtrovat pohyb na webu.
- Poloha dítěte - zde můžete nastavit lokace, které jsou nebo nejsou bezpečné pro vaše dítě.
- Telefonní kontakty - zde můžete vidět kontakty v telefonu vašeho dítěte.
- Zobrazit zařízení - zde můžete zobrazit stav sledovaných zařízení, přiřadit nové zařízení k profilu vašeho dítěte nebo přiřazené zařízení odebrat.

26.3.1. Aktivita

Hlavní okno poskytuje podrobné informace o online aktivitách vašich dětí za posledních 24 hodin nebo za posledních 7 dní, v závislosti na vašem výběru, uvnitř i mimo domov. Chcete-li zobrazit aktivity z předchozích sedmi dnů, klikněte na **Posledních 7 dní** .

V závislosti na aktivitě může toto okno zahrnovat informace o:

- **Poloha Díťete** - zde můžete zobrazit místa, kde se vaše děti během dne pohybovaly.
- **Aktivita webových stránek** - zde si můžete prohlédnout informace o kategoriích webových stránek, které vaše děti navštívily. Kliknutím na odkaz **ZMĚNIT NASTAVENÍ** povolíte nebo zakážete přístup ke konkrétním zájmům.

- **Nejnovější přidané telefonní kontakty** - zde si můžete prohlédnout, zda byly do zařízení vašeho dítěte přidány nějaké nové kontakty. Kliknutím na odkaz **ZOBRAZIT VŠECHNY TELEFONNÍ KONTAKTY** vyberte kontakty, s nimiž by vaše děti měly zůstat v kontaktu či nikoli.
- **Aplikace** - zde můžete vidět aplikace, které vaše dítě používalo. Kliknutím na odkaz **ZOBRAZIT VŠECHNY APLIKACE** zablokujete nebo povolíte přístup ke konkrétním aplikacím.
- **Čas obrazovky** - zde můžete vidět čas strávený online na všech zařízeních přiřazených vašim dětem. Kliknutím na **ZOBRAZIT ČAS OBRAZOVKY** otevřete okno **Čas obrazovky** .

26.3.2. Aplikace

Okno aplikací vám umožňuje blokovat aplikace před spuštěním na Windows, macOS a Android zařízeních. Tímto způsobem lze blokovsat hry, mediální software a aplikace pro zasílání zpráv a rovněž další kategorie softwaru.

Zde můžete také zobrazit aplikace nejvíce využívané vašim dítětem v posledních 30-ti dnech společně s časem na nich stráveným. Informace o času stráveném používáním aplikací, může být získávána pouze ze zařízení s Windows, macOS a Androidem.

Chcete-li nakonfigurovat kontrolu aplikací pro konkrétní uživatelský účet:

1. Zobrazí se seznam se přiřazenými zařízeními.

   Vyberte kartu se zařízením, kterému chcete zakázat přístup k aplikaci.

2. Klikněte na **Spravovat aplikace používané ...**.

   Zobrazí se seznam s nainstalovanými aplikacemi.

3. Vyberte **Blokované** vedle aplikací, které nechcete aby vaše dítě používalo.
4. Kliknutím na tlačítko **ULOŽIT** nastavení aplikujete.

Můžete přestat monitorovat nainstalované aplikace vypnutím možnosti **Sledování aplikací** v pravém horním rohu okna.

26.3.3. Websites

Okno Webové stránky pomáhá blokovat webové stránky s nevhodným obsahem v zařízeních se systémem Windows, MacOS a Android. Tímto způsobem lze blokovat webové stránky s videem, hrami, médii a softwarem pro zasílání zpráv a rovněž další kategorie nevhodného obsahu.

Modul lze povolit nebo zakázat pomocí příslušného přepínače.

V závislosti na nastaveném věku vašeho dítěte je seznam Zájmů ve výchozím stavu zaplněn výběrem povolených kategorií. Chcete-li povolit nebo zakázat přístup k určité kategorii, klikněte na ni.

Zobrazená ikona označuje, že vaše dítě nebude mít přístup k obsahu souvisejícímu s určitou kategorií.

Povolení nebo zablokování webové stránky

Chcete-li omezit přístup k určitým webovým stránkám, musíte je přidat do seznamu výjimek pomocí následujícího postupu:

1. Klikněte na tlačítko **MANAGE**.
2. Do příslušného pole zadejte webovou stránku, kterou chcete povolit nebo zablokovat.
3. Vyberte **Povolit** nebo **Odmítnout**.
4. Kliknutím na ikonu **+** změny uložte.

Poznámka
Omezení přístupu k webovým stránkám lze nastavit pouze na zařízeních Windows, Android nebo iOS, připojených k profilu k vašeho dítěte.

26.3.4. Telefonní kontakty

Okno Kontakty telefonu vám dává možnost vidět kontakty v telefonu vašeho dítěte.

Tato funkce je k dispozici na zařízeních iOS a Android.

26.3.5. Umístění dítěte

Zobrazení aktuální polohy zařízení v Mapách Google. Místo se obnovuje každých 5 sekund, takže můžete sledovat, pokud je v pohybu.

Přesnost polohy závisí na tom, jak ji produkt Bitdefender dokáže určit:

- Pokud je v zařízení povolená funkce GPS, polohu lze určit s přesností na několik metrů, jestliže je v dosahu satelitů GPS (tj. ne uvnitř budovy).

- Pokud se zařízení nachází v interiéru, jeho polohu lze určit s přesností na desítky metrů, jestliže je povolená funkce Wi-Fi a v jeho dosahu se nacházejí bezdrátové sítě.
- Jinak bude poloha určena pouze s pomocí informací z mobilní sítě, které nedokáží poskytnout přesnost na méně než několik stovek metrů.

Nastavování polohy & Bezpečné přihlášení

Abyste měli jistotu, zda vaše dítě chodí na určitá místa, můžete vytvořit seznam bezpečných a nebezpečných míst. Pokaždé, když vaše dítě vstoupí na území předem definované lokace, v aplikaci Rodičovský poradce se zobrazí upozornění s požadavkem o potvrzení, že je v pořádku. Kliknutím na **DORAZIL JSEM V POŘÁDKU** budete informováni prostřednictvím oznámení na vašem Bitdefender účtu, že dítě dorazilo na místo určení.

V případě, že od dítěte neobdržíte žádné potvrzení, stále můžete sledovat historii jeho polohy během celého dne tak, že zkontrolujete jeho profil ve vašem Bitdefender účtu.

Postup konfigurace místa:

1. V rozhraní Rodičovská kontrola otevřete profil vašeho dítěte, klikněte na **MOŽNOSTI** a vyberte okno **Umístění dítěte** .
2. Klikněte na **Zařízení** .
3. Klepněte na zařízení, které chcete konfigurovat.
4. V okně **Areas** klikněte na tlačítko **ADD AREA**.
5. Vyberte typ umístění - **Safe** (Bezpečné) nebo **Restricted** (Omezené).
6. Zadejte platné jméno pro oblast, kam vaše dítě smí nebo nesmí vstoupit.
7. Nastavte rádius, který by měl být sledován, pomocí posuvníku **Radius**.
8. Kliknutím na tlačítko **ADD AREA** uložte nastavení. Budete dotázáni, zda vaše dítě smí či nesmí cestovat samo. Povrďte kliknutím na Ano nebo Ne.

Poznámka

Sledování polohy můžete využít pro monitorování zařízení Android a iOS, která mají nainstalovanou aplikaci Bitdefender Rodičovský poradce.

26.3.6. Čas strávený na zařízení

V okně Screentime jste informováni o čase stráveném na přiřazených zařízeních v aktuální den, o kolik času zbývá z denního limitu, který jste nastavili, a stavu vybraného profilu, aktivního nebo pozastaveného. Z toho okna můžete také nastavit časové omezení pro různou dobu dne, jako například čas jít spát, domácí úkoly nebo osobní hodiny.

Časová Omezení

Pro počáteční nastavení časového omezení:

1. Klikněte na **MOŽNOSTI** a vyberte **Screentime** .
2. V oblasti **Naplánováno** klikněte na **PŘIDAT PLÁN**.
3. Pojmenujte plán, který chcete nastavit (například čas na spaní, domácí úkoly, lekce tenisu atd.).
4. Nastavte časový rámec a dny, kdy by měla být omezení uplatněna, a klepnutím na **PŘIDAT PLÁN** nastavení uložte.

Chcete-li upravit omezení, které jste nastavili, přejděte do části Plány, ukažte na omezení, které chcete upravit, a klikněte na tlačítko **EDIT** .

Chcete-li odstranit omezení, přejděte do okna Čas obrazovky, přejděte na omezení, které chcete upravit, klikněte na **EDIT** , pak vyberte **ODSTRANIT PLÁN** .

Denní limit

Používání denního limitu lze aplikovat na zařízení se systémem Windows, MacOS a Android. Pokud nastavíte profil, aby byl pozastaven jakmile dosáhnutí limitu, poté toto nastavení bude aplikováno na všechna přiřazená zařízení, nezáleží jestli je to Windows, macOS, Android nebo iOS.

Pro nastavení denního limitu:

1. Klikněte na **MOŽNOSTI** a vyberte **NASTAVTE DENNÍ ČASOVÉ LIMITY** .
2. Nastavte čas a dny, kdy by měla být omezení uplatněna, a kliknutím na **ULOŽIT ZMĚNY** nastavení uložte.

27. USB IMMUNIZER

Funkce Autorun zabudovaná do operačních systémů Windows je velmi užitečným nástrojem, který umožňuje zařízením automaticky spouštět soubor z připojeného média. Například se může automaticky spustit instalace softwaru po vložení disku CD do optické jednotky.

Tuto funkci bohužel mohou také využít hrozby k automatickému spuštění a infiltraci zařízení z přepisovatelných médií, jako jsou USB flash disky a paměťové karty připojené prostřednictvím čteček karet. V posledních letech bylo vytvořeno velké množství útoků založených na automatickém spouštění.

Pomocí funkce USB imunizér můžete navždy zabránit flashdiskům naformátovaným v systémech souborů NTFS, FAT32 nebo FAT v automatickém spouštění hrozeb. Jakmile je zařízení USB imunizováno, hrozby již nemohou nakonfigurovat spouštění určité aplikace, když je zařízení připojeno k zařízení se systémem Windows.

Pro imunizaci USB zařízení:

1. Připojte jednotku Flash k zařízení.
2. Procházejte zařízení a vyhledejte vyměnitelné úložné zařízení a klikněte pravým tlačítkem na jeho ikonu.
3. V kontextové nabídce vyberte položku **Bitdefender** a zvolte možnost **Imunizovat tuto jednotku**.

> **Poznámka**
> Pokud již jednotka byla imunizována, místo možnosti Imunizovat se zobrazí zpráva **USB zařízení je chráněno proti autorunovým hrozbám**.

Chcete-li zabránit zařízení ve spouštění hrozeb z neimunizovaných zařízení USB, vypněte funkci automatického spouštění médií. Další informace viz *„Používání automatického sledování zranitelností“* (str. 122).

SLUŽBY

28. PROFILY

Každodenní pracovní činnosti, sledování filmů nebo hraní her mohou způsobovat zpomalení systému, zejména pokud běží zároveň s procesy aktualizací a činností údržby systému Windows. S pomocí produktu Bitdefender nyní můžete zvolit a použít upřednostňovaný profil, který provede nastavení systému vhodná pro zvýšení výkonu určitých nainstalovaných aplikací.

Produkt Bitdefender nabízí následující profily:

- Pracovní profil
- Filmový profil
- Herní profil
- Profil Veřejná Wi-Fi
- Profil režimu baterie

Pokud se rozhodnete **profily** nepoužít, povolí se výchozí profil nazvaný **Standardní** a neprovedou se žádné optimalizace systému.

V závislosti na vaší činnosti se aplikuje nastavení produktu pro Práci, Film nebo Hraní:

- Všechny výstrahy a vyskakovací okna produktu Bitdefender jsou vypnuty.
- Automatická aktualizace bude odložena.
- Naplánované skeny jsou odloženy.
- Tester odkazů je vypnutý.
- Oznámení o zvláštních nabídkách jsou vypnuta.

V závislosti na vaší činnosti se aplikuje nastavení systému pro Práci, Film nebo Hraní:

- Automatické aktualizace systému Windows jsou odloženy.
- Výstrahy a vyskakovací okna systému Windows budou vypnuty.
- Nepotřebné programy na pozadí budou pozastaveny.
- Vizuální efekty jsou nastaveny na nejlepší výkon.
- Činnosti údržby budou odloženy.

- Upraví se nastavení schématu napájení.

Zatímco je spuštěn profil Veřejná Wi-Fi, Bitdefender Internet Security je nastaven k automatickému dokončení nastavení následujících programů:

- Pokročilá ochrana před hrozbami je zapnuta
- Bitdefender Firewall je zapnutý a následující nastavení jsou aplikované na váš bezdrátový adaptér.
  - Tichý režim - ON
  - Typ Sítě - Veřejná
- V Prevenci online hrozeb jsou zapnuta následující nastavení:
  - Šifrované skenování webu
  - Ochrana proti podvodům
  - Ochrana proti phishingu

28.1. Pracovní profil

Provozování více úloh v práci, jako odesílání emailů, videokonference se vzdálenými kolegy nebo práce s návrhářskými aplikacemi, může ovlivnit výkon systému. Byl vytvořen Pracovní profil, jehož cílem je pomoci vám zlepšit produktivitu tím, že vypíná některé služby na pozadí a činnosti údržby.

Konfigurace Pracovního profilu

Chcete-li nakonfigurovat činnosti, které se provedou v Pracovním profilu:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. Na kartě **Profily** klikněte na **Nastavení**.
3. Klikněte na tlačítko **KONFIGURACE** z karty Pracovního Profilu.
4. Vyberte nastavení systému, která chcete použít, zaškrtnutím následujících možností:
   - Zvýšení výkonu pro pracovní aplikace
   - Optimalizovat nastavení produktu pro Pracovní profil
   - Odložit programy na pozadí a úlohy údržby
   - Odložit automatické aktualizace systému Windows

5. Klikněte na **ULOŽIT** k uložení změn a zavření okna.

Ruční přidávání aplikací do seznamu pracovního profilu

Pokud produkt Bitdefender automaticky nepřejde do pracovního profilu, když spustíte určitou pracovní aplikaci, můžete aplikaci přidat ručně do **Seznamu pracovních aplikací**.

Chcete-li ručně přidat aplikace do Seznamu pracovních aplikací v Pracovním profilu:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. Na kartě **Profily** klikněte na **Nastavení**.
3. Klikněte na tlačítko **KONFIGURACE** z karty Pracovního Profilu.
4. V okně **Nastavení pracovního profilu** klikněte na **Seznam aplikací**.
5. Klikněte na **PŘIDAT**.

   Objeví se nové okno. Přejděte ke spustitelnému souboru aplikace, vyberte ho a kliknutím na tlačítko **OK** ho přidejte do seznamu.

28.2. Filmový profil

Zobrazení videa ve vysoké kvalitě, jako filmy ve vysokém rozlišení, vyžaduje značné systémové prostředky. Filmový profil upravuje nastavení systému a produktu, abyste si mohli vychutnat nepřerušovaný a bezproblémový filmový zážitek.

Konfigurace Filmového profilu

Chcete-li nakonfigurovat činnosti, které se provedou ve filmovém profilu:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. Na kartě **Profily** klikněte na **Nastavení**.
3. Klikněte na tlačítko **KONFIGURACE** z karty Filmového Profilu.
4. Vyberte nastavení systému, která chcete použít, zaškrtnutím následujících možností:
   - Zvýšení výkonu pro přehrávače videa
   - Optimalizovat nastavení produktu pro Filmový profil
   - Odložit programy na pozadí a úlohy údržby

- Odložit automatické aktualizace systému Windows
- Upravit nastavení schématu napájení pro filmy

5. Klikněte na **ULOŽIT** k uložení změn a zavření okna.

Ruční přidávání přehrávačů videa do seznamu filmového profilu

Pokud produkt Bitdefender automaticky nepřejde do filmového profilu, když spustíte určitou aplikaci pro přehrávání videa, můžete ji do **Seznamu filmových aplikací** přidat ručně.

Chcete-li ručně přidat přehrávače videa do seznamu filmových aplikací ve Filmovém profilu:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. Na kartě **Profily** klikněte na **Nastavení**.
3. Klikněte na tlačítko **KONFIGURACE** z karty Filmového Profilu.
4. V okně **Nastavení filmového profilu** klikněte na **Seznam přehrávačů**
5. Klikněte na **PŘIDAT**.

   Objeví se nové okno. Přejděte ke spustitelnému souboru aplikace, vyberte ho a kliknutím na tlačítko **OK** ho přidejte do seznamu.

28.3. Herní profil

Abyste si mohli vychutnat nerušené herní aktivity, je třeba omezit zatížení systému a snižovat zpomalování. Pomocí behaviorální heuristiky ve spojení se seznamem známých her může produkt Bitdefender automaticky detekovat spuštěné hry a optimalizovat systém tak, abyste si svou přestávku na hraní mohli vychutnat.

Konfigurace Herního profilu

Chcete-li nakonfigurovat činnosti, které se provedou v Herním profilu:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. Na kartě **Profily** klikněte na **Nastavení**.
3. V oblasti Herní profil klikněte na tlačítko **Konfigurovat**.

4. Vyberte nastavení systému, která chcete použít, zaškrtnutím následujících možností:
   - Zvýšení výkonu pro hry
   - Optimalizovat nastavení produktu pro Herní profil
   - Odložit programy na pozadí a úlohy údržby
   - Odložit automatické aktualizace systému Windows
   - Upravit nastavení schématu napájení pro hry
5. Klikněte na **ULOŽIT** k uložení změn a zavření okna.

Ruční přidávání her do Seznamu her

Pokud produkt Bitdefender automaticky nepřejde do herního profilu, když spustíte určitou hru nebo aplikaci, můžete ji do **seznamu her** přidat ručně.

Chcete-li ručně přidávat hry do Seznamu herních aplikací v Herním profilu:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. Na kartě **Profily** klikněte na **Nastavení**.
3. Klikněte na tlačítko **KONFIGURACE** z karty Herního Profilu.
4. V okně **Nastavení herního profilu** klikněte na **Seznam her**
5. Klikněte na **PŘIDAT**.

   Objeví se nové okno. Přejděte ke spustitelnému souboru hry, vyberte ho a kliknutím na tlačítko **OK** ho přidejte do seznamu.

28.4. Profil Veřejná Wi-Fi

Odesílání mailů, psaní citlivých údajů nebo nakupování online zatímco jste připojení k nezabezpečené bezdrátové síti může představovat riziko pro vaše osobní data. Profil veřejné Wi-Fi upraví nastavení produktu, aby jste mohli provádět platby online a používat citlivé informace v chráněném prostředí.

Konfigurace Profilu veřejné Wi-Fi

Chcete-li konfigurovat Bitdefender k aplikaci nastavení produktu, zatímco jste připojen k nezabezpečené bezdrátové síti:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.

2. Na kartě **Profily** klikněte na **Nastavení**.
3. Klikněte na tlačítko **KONFIGURACE** z karty Profilu veřejné Wi-Fi.
4. Nechte **Upravit nastavení produktu na posílení ochrany při připojení nezabezpečené veřejné Wi-Fi síti** povoleno.
5. Klikněte na tlačítko **Save**.

28.5. Profil režimu baterie

Úsporný režim je speciálně navržený pro uživatele notebooků a tabletů. Jeho účelem je minimalizovat dopad systému a produktu Bitdefender na spotřebu, když je úroveň nabití baterie nižší než vybraná.

Konfigurace úsporného režimu

Pro nastavení profilu Módu Baterie:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. Na kartě **Profily** klikněte na **Nastavení**.
3. Klikněte na tlačítko **Konfigurovat** v oblasti Profil režimu baterie.
4. Zaškrtnutím následujících možností vyberte nastavení systému, která budou použita.
   - Optimalizovat nastavení produktu pro Úsporný režim.
   - Odložit programy na pozadí a úlohy údržby.
   - Odložit automatické aktualizace systému Windows.
   - Upravit nastavení napájení pro Úsporný režim.
   - Vypnout externí zařízení a síťové porty.
5. Klikněte na **ULOŽIT** k uložení změn a zavření okna.

Zadejte platnou hodnotu nebo jednu vyberte pomocí šipek nahoru a dolů, k určení kdy by měl systém začít fungovat v režimu napájení z baterie. Ve výchozím nastavení se režim aktivuje, když úroveň baterie poklesne pod 30 %.

Když produkt Bitdefender pracuje v úsporném režimu, použijí se následující nastavení produktu:

- Automatické aktualizace produktu Bitdefender jsou odloženy.

- Naplánované skeny jsou odloženy.

Produkt Bitdefender detekuje, když se notebook přepne na bateriové napájení a na základě úrovně nabití baterie automaticky přejde do úsporného režimu. Stejně tak produkt Bitdefender úsporný režim automaticky ukončí, když zjistí, že notebook již není napájen z baterie.

28.6. Optimalizace v reálném čase

Bitdefender - Optimalizace v reálném čase je modul plug-in, který tiše na pozadí zlepšuje výkon systému a zaručuje, abyste nebyli rušeni, když jste v režimu profilu. V závislosti na zatížení procesoru sleduje modul plug-in všechny procesy a zaměřuje se na ty, které způsobují větší zátěž. Tyto procesy přizpůsobí vašim potřebám.

Chcete-li zapnout nebo vypnout Optimalizaci v reálném čase:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. Na kartě **Profily** klikněte na **Nastavení** .
3. Posouvejte se dolů, dokud neuvidíte položku Optimalizování v reálném čase, a poté klikněte na příslušný vypínač a zapněte/vypněte ji.

29. OCHRANA DAT

29.1. Trvalé odstranění souborů

Když odstraníte soubor, není již běžnými prostředky nadále přístupný. Zůstává však uložený na pevném disku, dokud nebude přepsán při kopírování nových souborů.

Likvidátor souborů produktu Bitdefender vám pomůže trvale odstranit data fyzickým smazáním z pevného disku.

Soubory nebo složky z vašeho zařízení můžete rychle skartovat pomocí kontextové nabídky systému Windows podle následujících kroků:

1. Klikněte pravým tlačítkem na soubor nebo složku, které chcete trvale odstranit.
2. V zobrazené kontextové nabídce vyberte položku **Bitdefender** > **Likvidátor souborů**.
3. Klikněte na **Smazat trvale** a potvrďte, že chcete pokračovat v procesu.

   Počkejte, dokud produkt Bitdefender nedokončí likvidaci souborů.
4. Zobrazí se výsledky. Průvodce ukončíte kliknutím na **Dokončit** .

Nebo také můžete likvidovat soubory z rozhraní produktu Bitdefender následovně:

1. Klikněte na **Nástroje** v navigačním menu v rozhraní Bitdefender.
2. V podokně **Ochrana dat** klikněte na **Skartovačka** .
3. Postupujte podle průvodce likvidací souborů:
   a. Kliknutím na tlačítko **Přidat složky** přidejte soubory nebo složky, které chcete trvale odebrat.

      Nebo také můžete přetáhnout soubory nebo složky přímo do tohoto okna.

   b. Klikněte na **Smazat trvale** a potvrďte, že chcete v procesu pokračovat.

      Počkejte, dokud produkt Bitdefender nedokončí likvidaci souborů.

   c. **Přehled výsledků**

      Zobrazí se výsledky. Průvodce ukončíte kliknutím na **Dokončit** .

ŘEŠENÍ PROBLÉMŮ

30. ŘEŠENÍ BĚŽNÝCH PROBLÉMŮ

Tato kapitola představuje některé problémy, na které můžete při používání produktu Bitdefender narazit, a nabízí jejich možná řešení. Většinu těchto problémů lze vyřešit řádnou konfigurací nastavení produktu.

- *„Systém je pomalý“* (str. 177)
- *„Sken se nespustí“* (str. 178)
- *„Nemůžete používat aplikaci“* (str. 181)
- *„Co dělat, když Bitdefender blokuje webovou stránku, doménu, IP adresu nebo online aplikaci, která je bezpečná“* (str. 182)
- *„Jak aktualizovat produkt Bitdefender na pomalém připojení k Internetu“* (str. 186)
- *„Služby produktu Bitdefender neodpovídají“* (str. 187)
- *„Antispamový filtr nefunguje správně“* (str. 187)
- *„Funkce automatického vyplňování v mé portmonce nefunguje“* (str. 192)
- *„Odebrání produktu Bitdefender se nezdařilo“* (str. 193)
- *„Po instalaci produktu Bitdefender se můj systém nespustí“* (str. 194)

Pokud zde svůj problém nemůžete najít nebo ho navrhovaná řešení neodstraní, můžete kontaktovat zástupce technické podpory společnosti Bitdefender dle postupu uvedeného v kapitole *„Žádost o pomoc“* (str. 206).

30.1. Systém je pomalý

Po instalaci zabezpečovacího softwaru obvykle může dojít k mírnému zpomalení systému, které je do určité míry normální.

Pokud zaznamenáte výrazné zpomalení, může k němu docházet z následujících důvodů:

- **Produkt Bitdefender není jediný zabezpečovací program nainstalovaný v systému.**

  I když produkt Bitdefender vyhledá a odinstaluje nalezené zabezpečovací programy během instalace, doporučujeme odinstalovat všechny ostatní antivirové programy, které jste před instalací produktu Bitdefender

používali. Další informace viz *„Jak odinstalovat jiná řešení zabezpečení?“ (str. 75)*.

- **Systémové požadavky pro spuštění Bitdefender nejsou splněny.**

  Pokud váš počítač nesplňuje systémové požadavky, zařízení se stane pomalým, zejména pokud běží více aplikací současně. Další informace viz *„Požadavky na systém“ (str. 3)*.

- **Máte nainstalované aplikace, které nepoužíváte**.

  Každé zařízení obsahuje programy nebo aplikace, které nepoužíváte. A každý nepotřebný program běžící na pozadí zabírá místo na disku a v paměti. Pokud nějaký program nepoužíváte, odinstalujte ho. To platí i pro ostatní předinstalovaný software nebo zkušební aplikace, které jste zapomněli odinstalovat.

  > **Důležité**
  > Pokud máte podezření, že některý program nebo aplikace jsou důležitou součástí operačního systému, neodebírejte je a požádejte o pomoc zákaznickou podporu produktu Bitdefender.

- **Váš systém může být infikovaný**.

  Rychlost systému a jeho celkové chování mohou být rovněž ovlivněny hrozbami. Spyware, malware, trojské koně a adware všechny snižují výkon zařízení. Pravidelně systém skenujte alespoň jednou týdně. Doporučujeme používat Kompletní sken produktu Bitdefender, protože skenuje všechny druhy hrozeb ohrožujících zabezpečení vašeho systému.

  Chcete-li spustit sken systému:

  1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
  2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
  3. V okně **Skeny** klikněte na **Spustit Sken** vedle **System Sken** .
  4. Postupujte podle pokynů průvodce.

30.2. Sken se nespustí

Tento druh problému může mít dvě hlavní příčiny:

- **Instalace předchozí verze produktu Bitdefender, která nebyla zcela odebrána, nebo vadná instalace produktu Bitdefender**.

V tomto případě přeinstalujte Bitdefender:

- V systému **Windows 7**:
  1. Klikněte na nabídku **Start**, přejděte do **Ovládacích panelů** a dvakrát klikněte na položku **Programy a funkce**.
  2. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
  3. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
  4. Počkejte na dokončení procesu přeinstalace a poté restartujte systém.
- V systémech **Windows 8 a Windows 8.1**:
  1. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
  2. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
  3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
  4. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
  5. Počkejte na dokončení procesu přeinstalace a poté restartujte systém.
- V systému **Windows 10**:
  1. Klikněte na nabídku **Start** a poté na položku Nastavení.
  2. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Nainstalované aplikace**.
  3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
  4. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.
  5. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
  6. Počkejte na dokončení procesu přeinstalace a poté restartujte systém.

Poznámka

Provedením tohoto přeinstalačního procesu jsou osobní nastavení uložena a k dispozici v nově nainstalovaném produktu. Ostatní nastavení mohou být vrácena zpět do svého výchozího nastavení.

- **Produkt Bitdefender není jediný zabezpečovací program nainstalovaný ve vašem systému**.

  V tomto případě:

  1. Odeberte druhé řešení zabezpečení. Další informace viz *„Jak odinstalovat jiná řešení zabezpečení?“* (str. 75).
  2. Přeinstalovat Bitdefender:
     - V systému **Windows 7**:
       a. Klikněte na nabídku **Start**, přejděte do **Ovládacích panelů** a dvakrát klikněte na položku **Programy a funkce**.
       b. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
       c. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
       d. Počkejte na dokončení procesu přeinstalace a poté restartujte systém.
     - V systémech **Windows 8 a Windows 8.1**:
       a. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
       b. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
       c. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
       d. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
       e. Počkejte na dokončení procesu přeinstalace a poté restartujte systém.
     - V systému **Windows 10**:
       a. Klikněte na nabídku **Start** a poté na položku Nastavení.
       b. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Nainstalované aplikace**.
       c. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
       d. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.

e. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.

f. Počkejte na dokončení procesu přeinstalace a poté restartujte systém.

> **Poznámka**
> Provedením tohoto přeinstalačního procesu jsou osobní nastavení uložena a k dispozici v nově nainstalovaném produktu. Ostatní nastavení mohou být vrácena zpět do svého výchozího nastavení.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

30.3. Nemůžete používat aplikaci

K tomuto problému dochází, když se snažíte použít program, který před instalací produktu Bitdefender normálně fungoval.

Po instalaci produktu Bitdefender může dojít k jedné z následujících situací:

- Od produktu Bitdefender můžete obdržet zprávu, že se program snaží provést změnu v systému.
- Může se zobrazit chybová zpráva od programu, který se snažíte použít.

K této situaci dojde, když Pokročilá ochrana před hrozbami chybně rozpozná některé aplikace jako škodlivé.

Pokročilá ochrana před hrozbami je modul produktu Bitdefender, který neustále sleduje aplikace spuštěné v systému a hlásí ty, které mají potenciálně nebezpečné chování. Protože je tato funkce založená na heuristickém systému, může docházet k případům, kdy jsou Pokročilou ochranou před hrozbami hlášeny bezpečné aplikace.

Když taková situace nastane, můžete příslušnou aplikaci vyloučit ze sledování Pokročilé ochrany před hrozbami.

Pro přidání programu na seznam výjimek:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ROZŠÍŘENÁ OCHRANA PROTI HROZBÁM** klikněte na **Otevřít**.
3. V okně **Nastavení** klikněte na **Spravovat výjimky**.
4. Klikněte na **+ Přidat výjimku**.

5. Do příslušného pole zadejte cestu spustitelného souboru, který chcete vyjmout ze skenování.

   Případně můžete přejít na spustitelný soubor kliknutím na tlačítko Procházet v pravé části rozhraní, vyberte jej a klikněte na **OK** .

6. Zapněte přepínač vedle položky **Pokročilá ochrana před hrozbami** .

7. Klikněte na tlačítko **Save**.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

30.4. Co dělat, když Bitdefender blokuje webovou stránku, doménu, IP adresu nebo online aplikaci, která je bezpečná

Produkt Bitdefender poskytuje bezpečné procházení webu díky filtrování veškerého webového provozu a blokování škodlivého obsahu. Je však možné, že Bitdefender považuje webovou stránku, doménu, adresu IP nebo online aplikaci, která je bezpečná, za nebezpečnou, což způsobí, že je HTTP skenování provozu Bitdefender chybně zablokuje.

Pokud je stejná stránka nebo aplikace blokována opakovaně, můžete ji přidat k výjimkám, aby nebyly Bitdefender skenovány, což zaručí bezproblémové procházení webu.

Pro přidání webové stránky mezi **Výjimky**:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **PREVENCE ONLINE HROZEB** klikněte na **Nastavení**.
3. Klikněte na **Spravovat výjimky** .
4. Klikněte na **+ Přidat výjimku** .
5. Do odpovídajícího pole zadejte název webu, název domény nebo IP adresu, kterou chcete přidat k výjimkám.
6. Klikněte na přepínač vedle položky **Prevence online hrozeb** .
7. Kliknutím na tlačítko **Uložit** uložte změny a zavřete okno.

Do tohoto seznamu by měly být přidány pouze webové stránky, domény, adresy IP a aplikace, kterým plně důvěřujete. Tyto budou vyloučeny ze skenování následujícími jádry: hrozby, phishing a podvody.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

30.5. Nelze se připojit k Internetu

Může se stát, že se nějaký program nebo webový prohlížeč po instalaci produktu Bitdefender nemůže připojit k Internetu nebo nemá přístup k síťovým službám.

V takovém případě je nejlepším řešením nakonfigurovat produkt Bitdefender tak, aby automaticky povoloval připojení k příslušným aplikacím a z těchto aplikací:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **FIREWALL** klikněte na **Nastavení**.
3. V okně **Pravidla** klikněte na **Přidat pravidlo**.
4. Zobrazí se nové okno, ve kterém můžete přidat podrobnosti. Vyberte všechny dostupné typy sítí a v části **Oprávnění** vyberte možnost **Povolit**.

Zavřete produkt Bitdefender, otevřete aplikaci a zkuste se znovu připojit k Internetu.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

30.6. Nemám přístup k zařízení v mojí síti

V závislosti na síti, ke které jste připojeni, může brána firewall Bitdefender blokovat spojení mezi vaším systémem a jiným zařízením (například jiným počítačem nebo tiskárnou). V důsledku toho není nadále možné sdílet nebo tisknout soubory.

V takovém případě je nejlepším řešením nastavit produkt Bitdefender tak, aby automaticky povoloval připojení k příslušnému zařízení a z tohoto zařízení, a to následovně:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **FIREWALL** klikněte na **Nastavení**.
3. V okně **Pravidla** klikněte na **Přidat pravidlo**.
4. Zapněte možnost **Použít toto pravidlo na všechny aplikace** .
5. Klikněte na tlačítko **Pokročilá nastavení** .

6. Do pole **Vlastní vzdálená adresa** zadejte IP adresu počítače nebo tiskárny, ke kterému chcete mít neomezený přístup.

Pokud se stále nemůžete k zařízení připojit, problém nemusí být způsobený produktem Bitdefender.

Zkontrolujte možné příčiny, jako např.:

- Brána firewall na jiném zařízení může blokovat sdílení souborů a tiskáren s počítačem.
  - Pokud je použita brána firewall systému Windows, lze ji nakonfigurovat pro sdílení souborů a tiskáren následujícím způsobem:
    - V systému **Windows 7**:
      1. Klikněte na nabídku **Start**, předjděte do **Ovládacích panelů** a vyberte položku **Systém a zabezpečení**.
      2. Přejděte do částí **Brána Windows Firewall** a klikněte na položku **Povolit program v bráně Windows Firewall**.
      3. Zaškrtněte políčko **Sdílení souborů a tiskáren**.
    - V systémech **Windows 8 a Windows 8.1**:
      1. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
      2. Klikněte na položku **Systém a zabezpečení**, přejděte do **Brány Windows Firewall** a vyberte možnost **Povolit aplikaci v bráně Windows Firewall**.
      3. Zaškrtněte políčko **Sdílení souborů a tiskáren** a klikněte na tlačítko **OK**.
    - V systému **Windows 10**:
      1. Do vyhledávacího pole na hlavním panelu zadejte „Povolit aplikaci v bráně Windows Firewall“ a klikněte na příslušnou ikonu.
      2. Klikněte na položku **Změnit nastavení**.
      3. V seznamu **Povolené aplikace a funkce** zaškrtněte políčko **Sdílení souborů a tiskáren** a klikněte na tlačítko **OK**.
  - Pokud používáte jiný program brány firewall, přečtěte si jeho dokumentaci nebo soubor nápovědy.

- Obecné podmínky, které mohou bránit používání nebo připojení ke sdílené tiskárně.
  - Pro přístup ke sdílené tiskárně může být nutné přihlášení pod účtem správce systému Windows.
  - Oprávnění jsou nastavena pro sdílenou tiskárnu, která umožňují přístup pouze k určitému zařízení a uživatelům. Pokud sdílíte svou tiskárnu, zkontrolujte oprávnění nastavená pro tiskárnu, abyste zjistili, zda uživatel na druhém zařízení má povolený přístup k tiskárně. Pokud se pokoušíte připojit ke sdílené tiskárně, zkontrolujte u uživatele na druhém zařízení, že máte oprávnění k připojení k tiskárně.
  - Tiskárna připojená k vašemu zařízení nebo k druhému není sdílena.
  - Sdílená tiskárna není přidána do zařízení.

  Poznámka
  Chcete-li se dozvědět, jak spravovat sdílení tiskáren (sdílení tiskárny, nastavení nebo odebrání oprávnění pro tiskárnu, připojení k síťové tiskárně nebo ke sdílené tiskárně), přejděte do Centra pro nápovědu a podporu systému Windows (v nabídce Start klikněte na položku **Nápověda a podpora**).

- Přístup k síťové tiskárně může být omezen pouze na určitá zařízení nebo uživatele. U správce sítě byste měli ověřit, zda máte oprávnění připojit se k dané tiskárně.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

30.7. Internet je pomalý

Tato situace může nastat po instalaci produktu Bitdefender. Problém může být způsoben chybami v konfiguraci brány firewall produktu Bitdefender.

Chcete-li vyřešit tuto situaci:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **FIREWALL** vypněte přepínač pro vypnutí modulu.
3. Zkontrolujte, zda se připojení k Internetu po vypnutí brány firewall produktu Bitdefender zlepšilo.

- Pokud je připojení k Internetu stále pomalé, problém nemusí být způsobený produktem Bitdefender. Obraťte se na svého poskytovatele připojení k Internetu, aby ověřil, zda je připojení na jejich straně funkční.

  Pokud obdržíte od poskytovatele připojení potvrzení, že připojení je na jeho straně funkční, a problém stále přetrvává, kontaktujte podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“ (str. 206)*.

- Pokud se připojení k Internetu po vypnutí brány firewall produktu Bitdefender zlepšilo, postupujte následovně:

  a. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.

  b. V okně **FIREWALL** klikněte na **Nastavení**.

  c. Přejděte na kartu **Síťové adaptéry** a nastavte své internetové připojení jako **Doma/V kanceláři**.

  d. Na kartě **Nastavení** vypněte **Ochranu skenování portů**.

     V oblasti **Režim Stealth** klikněte na **Upravit nastavení stealth** Zapněte Režim Stealth pro síťový adaptér, ke kterému jste připojeni.

  e. Zavřete produkt Bitdefender, restartujte systém a zkontrolujte rychlost připojení k Internetu.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“ (str. 206)*.

30.8. Jak aktualizovat produkt Bitdefender na pomalém připojení k Internetu

Pokud máte pomalé připojení k Internetu (např. vytáčené), může v průběhu aktualizace docházet k chybám.

Pro udržení vašeho systému aktuálního s nejnovější databází s informacemi o hrozbách produktu Bitdefender:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Aktualizace**.
3. Vypněte přepínač **Tichá aktualizace**.
4. Při příští dostupné aktualizaci budete vyzváni k výběru, kterou aktualizaci chcete stáhnout. Vyberte pouze **Aktualizace signatur**.

5. Bitdefender stáhne a nainstaluje pouze databázi s informacemi o hrozbách.

30.9. Služby produktu Bitdefender neodpovídají

Tento článek vám pomůže vyřešit problém s chybou **Služby produktu Bitdefender neodpovídají**. K této chybě může dojít v následující situaci:

- Ikona produktu Bitdefender v oznamovací oblasti je šedá a jste informováni, že služby produktu Bitdefender neodpovídají.
- Okno produktu Bitdefender indikuje, že služby produktu Bitdefender neodpovídají.

Chyba může být způsobena jednou z následujících podmínek:

- dočasné chyby komunikace mezi službami produktu Bitdefender.
- některé ze služeb produktu Bitdefender jsou zastaveny.
- další bezpečnostní řešení běžící na vašem zařízení současně s Bitdefender.

Chcete-li tuto chybu odstranit, vyzkoušejte následující řešení:

1. Chvíli počkejte, jestli se něco nezmění. Chyba může být dočasná.
2. Restartujte zařízení a vyčkejte chvíli, než se načte Bitdefender. Otevřete produkt Bitdefender a zjistěte, jestli chyba přetrvává. Restart zařízení obvykle problém vyřeší.
3. Zkontrolujte, zda není nainstalované jiné řešení zabezpečení, což může narušit normální provoz produktu Bitdefender. Pokud je tomu tak, doporučujeme odebrat všechna ostatní řešení zabezpečení a poté produkt Bitdefender přeinstalovat.

   Další informace viz *„Jak odinstalovat jiná řešení zabezpečení?“* (str. 75).

Pokud problém přetrvává, požádejte o pomoc zástupce podpory dle popisu v části *„Žádost o pomoc“* (str. 206).

30.10. Antispamový filtr nefunguje správně

Tento článek vám pomůže vyřešit následující problémy s činností antispamového filtrování produktu Bitdefender:

- Několik legitimních emailových zpráv je označeno jako [spam].
- Mnoho spamových zpráv není antispamovým filtrem náležitě označeno.

- Antispamový filtr nedetekuje žádné spamové zprávy.

30.10.1. Legitimní zprávy jsou označeny jako [spam]

Legitimní zprávy jsou označovány jako [spam] jednoduše proto, že se antispamovému filtru produktu Bitdefender jeví jako spam. Tento problém lze normálně vyřešit adekvátní konfigurací antispamového filtru.

Produkt Bitdefender automaticky přidává příjemce vašich emailových zpráv do seznamu přátel. Emailové zprávy přijaté od kontaktů v seznamu přátel jsou považovány za legitimní. Nejsou antispamovým filtrem ověřovány, a proto nejsou nikdy označeny jako [spam].

Automatická konfigurace seznamu přátel nezabrání chybám detekce, ke kterým může docházet v následujících situacích:

- Přijímáte velké množství vyžádané komerční pošty v důsledku registrací na různých webových stránkách. V tomto případě je řešením přidat emailové adresy, ze kterých tyto emailové zprávy přijímáte, do seznamu přátel.
- Značná část legitimní pošty je od lidí, kterým jste nikdy nepsali, jako zákazníci, potenciální obchodní partneři a další. V tomto případě jsou vyžadována jiná řešení.

  Pokud používáte jednoho z poštovních klientů, do kterých se produkt Bitdefender integruje, označujte chyby detekce.

> **Poznámka**
> Produkt Bitdefender se integruje do nejčastěji používaných poštovních klientů ve formě snadno ovladatelné antispamové lišty nástrojů. Úplný seznam podporovaných poštovních klientů najdete zde *„Podporovaní emailoví klienti a protokoly“* (str. 107).

Přidání kontaktů do seznamu přátel

Jestliže používáte podporovaného poštovního klienta, můžete snadno přidat odesílatele legitimních zpráv do seznamu přátel. Postupujte následovně:

1. V poštovním klientovi vyberte emailovou zprávu od odesílatele, kterého chcete přidat do seznamu přátel.
2. Klikněte na tlačítko **Přidat přítele** na liště antispamových nástrojů produktu Bitdefender.

3. Můžete být vyzváni k potvrzení adres přidaných do seznamu přátel. Vyberte možnost **Nezobrazovat znovu tuto zprávu** a klikněte na tlačítko **OK**.

E-mailové zprávy z této adresy obdržíte vždy, bez ohledu na jejich obsah.

Pokud používáte jiného poštovního klienta, můžete kontakty do seznamu přátel přidat v rozhraní produktu Bitdefender. Postupujte následovně:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTISPAM** klikněte na **Spravovat přátele**.

   Zobrazí se konfigurační okno.
3. Zadejte emailovou adresu, ze které chcete vždy přijímat emailové zprávy, a poté klikněte na tlačítko **PŘIDAT**. Můžete přidat libovolný počet emailových adres.
4. Kliknutím na tlačítko **OK** uložte změny a zavřete okno.

Indikované chyby

Jestliže používáte podporovaného poštovního klienta, můžete snadno opravovat antispamový filtr (indikací emailových zpráv, které by neměly být označeny jako [spam]). Tím zlepšíte účinnost antispamového filtru. Postupujte následovně:

1. Otevřete poštovního klienta.
2. Přejděte do složky nevyžádané pošty, kam jsou přesouvány spamové zprávy.
3. Vyberte legitimní zprávu nesprávně označenou produktem Bitdefender jako [spam].
4. Kliknutím na tlačítko **Přidat přítele** na liště antispamových nástrojů produktu Bitdefender přidáte odesílatele do seznamu přátel. Může být nutné potvrzení tlačítkem **OK**. E-mailové zprávy z této adresy obdržíte vždy, bez ohledu na jejich obsah.
5. Klikněte na tlačítko **Není spam** na liště antispamových nástrojů produktu Bitdefender (obvykle se nachází v horní části okna poštovního klienta). Emailová zpráva bude přesunuta do složky přijaté pošty.

30.10.2. Mnoho spamových zpráv není detekováno

Pokud přijímáte mnoho spamových zpráv, které nejsou označeny jako [spam], je třeba nakonfigurovat autospamový filtr produktu Bitdefender, aby se zlepšila jeho účinnost.

Vyzkoušejte následující řešení:

1. Pokud používáte jednoho z poštovních klientů, do kterých se produkt Bitdefender integruje, označujte nedetekované spamové zprávy.

   > **Poznámka**
   >
   > Produkt Bitdefender se integruje do nejčastěji používaných poštovních klientů ve formě snadno ovladatelné antispamové lišty nástrojů. Úplný seznam podporovaných poštovních klientů najdete zde *„Podporovaní emailoví klienti a protokoly“* (str. 107).

2. Přidejte spamery do seznamu spamerů. Emailové zprávy přijaté z adres v seznamu spamerů budou automaticky označeny jako [spam].

Indikace nedetekovaných spamových zpráv

Jestliže používáte podporovaného poštovního klienta, můžete označit, které emailové zprávy měly být detekovány jako spam. Tím zlepšíte účinnost antispamového filtru. Postupujte následovně:

1. Otevřete poštovního klienta.
2. Přejděte do složky přijaté pošty.
3. Vyberte nedetekované spamové zprávy.
4. Klikněte na tlačítko **Je spam** na liště antispamových nástrojů produktu Bitdefender (obvykle se nachází v horní části okna poštovního klienta). Okamžitě se označí jako [spam] a budou přesunuty do složky nevyžádané pošty.

Přidání spamerů do seznamu spamerů

Jestliže používáte podporovaného poštovního klienta, můžete snadno přidat odesílatele spamových zpráv do seznamu spamerů. Postupujte následovně:

1. Otevřete poštovního klienta.

2. Přejděte do složky nevyžádané pošty, kam jsou přesouvány spamové zprávy.
3. Vyberte zprávy označené produktem Bitdefender jako [spam].
4. Klikněte na tlačítko **Přidat spamera** na liště antispamových nástrojů produktu Bitdefender.
5. Můžete být vyzváni k potvrzení adres přidaných do seznamu spamerů. Vyberte možnost **Nezobrazovat znovu tuto zprávu** a klikněte na tlačítko **OK**.

Pokud používáte jiného poštovního klienta, můžete spamery do seznamu spamerů přidat v rozhraní produktu Bitdefender. To je vhodné provést pouze v případě, že jste obdrželi několik spamových zpráv ze stejné emailové adresy. Postupujte následovně:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTISPAM** klikněte na **Nastavení**.
3. Přejděte do okna **Spravovat spammery** .
4. Zadejte emailovou adresu spamera a poté klikněte na tlačítko **Přidat**. Můžete přidat libovolný počet emailových adres.
5. Kliknutím na tlačítko **OK** uložte změny a zavřete okno.

30.10.3. Antispamový filtr nedetekuje žádné spamové zprávy

Pokud nejsou žádné spamové zprávy označovány jako [spam], může být problém s antispamovým filtrem produktu Bitdefender. Před řešením tohoto problému se ujistěte, že není způsoben jednou z následujících podmínek:

- Antispamová ochrana může být vypnutá. Pro ověření stavu ochrany proti spamu klikněte na **Ochrana** v nabídce v rozhraní Bitdefender. Podívejte se na panel **Antispam** a zkontrolujte, zda je modul zapnutý.

  Pokud je antispamová ochrana vypnutá, je problém způsoben tímto nastavením. Kliknutím na odpovídající přepínač zapněte antispamovou ochranu.

- Antispamová ochrana produktu Bitdefender je k dispozici pouze pro emailové klienty nakonfigurované pro příjem emailových zpráv prostřednictvím protokolu POP3. Znamená to následující:

- Emailové zprávy přijímané webovými emailovými službami (jako Post, Gmail, Centrum a další) nejsou filtrovány antispamovou ochranou produktu Bitdefender.
- Pokud je váš emailový klient nakonfigurován na příjem emailových zpráv jiným protokolem než POP3 (např. IMAP4), antispamový filtr produktu Bitdefender nekontroluje přítomnost spamu v nich.

> **Poznámka**
>
> POP3 je jedním z nejčastěji používaných protokolů pro stahování emailových zpráv z poštovního serveru. Jestliže nevíte, jaký protokol váš emailový klient používá ke stahování emailových zpráv, zeptejte se osoby, která vašeho emailového klienta nakonfigurovala.

- Produkt Bitdefender Internet Security neskenuje POP3 provoz aplikace Lotus Notes.

Možným řešením je opravit nebo přeinstalovat produkt. Může však být vhodné místo toho kontaktovat podporu společnosti Bitdefender dlr popisu v části *„Žádost o pomoc“* (str. 206).

30.11. Funkce automatického vyplňování v mé portmonce nefunguje

Uložili jste své přihlašovací údaje do portmonky produktu Bitdefender a zjistili jste, že automatické vyplňování nefunguje. Tento problém obvykle nastane, když ve vašem prohlížeči není nainstalované rozšíření Správce hesel produktu Bitdefender.

Tuto situaci opravíte následujícím postupem:

- V prohlížeči **Internet Explorer:**
  1. Otevřete prohlížeč Internet Explorer.
  2. Klikněte na nabídku Nástroje.
  3. Klikněte na položku Spravovat doplňky.
  4. Klikněte na položku Panely nástrojů a rozšíření.
  5. Ukažte na **Bitdefender Portmonku** a klikněte **Povolit**.
- V prohlížeči **Mozilla Firefox:**
  1. Otevřete prohlížeč Mozilla Firefox.

2. Klikněte na tlačítko **Otevřít nabídku** v pravém horním rohu obrazovky.
3. Klikněte na Doplňky.
4. Klikněte na Rozšíření.
5. Přejděte na **[Peněženka Bitdefender** a klikněte na přepínač vedle ní.

- V prohlížeči **Google Chrome:**
  1. Otevřete prohlížeč Google Chrome.
  2. Přejděte k ikoně Nabídka.
  3. Klikněte na Další nástroje.
  4. Klikněte na Rozšíření.
  5. Přejděte na **Bitdefender Peněženka** a klikněte na příslušný přepínač.

Poznámka
Doplněk bude povolen po restartu webového prohlížeče.

Nyní zkontrolujte, zda funkce automatického vyplňování v portmonce u vašich online účtů funguje.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

30.12. Odebrání produktu Bitdefender se nezdařilo

Pokud chcete produkt Bitdefender odebrat a zjistíte, že se proces zastaví nebo systém přestane reagovat, kliknutím na tlačítko **Storno** akci zrušte. Pokud to nefunguje, restartujte systém.

Pokud se odebrání nezdaří, některé klíče registru a soubory produktu Bitdefender mohou v systému zůstat. Tyto pozůstatky mohou znemožnit novou instalaci produktu Bitdefender. Rovněž mohou ovlivňovat výkon a stabilitu systému.

Pro kompletní odstranění Bitdefender ze systému:

- V systému **Windows 7**:
  1. Klikněte na nabídku **Start**, přejděte do **Ovládacích panelů** a dvakrát klikněte na položku **Programy a funkce**.
  2. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.

3. V okně, které se zobrazí, klikněte na **ODSTRANIT**.
4. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

- V systémech **Windows 8 a Windows 8.1**:
  1. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
  2. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
  3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
  4. V okně, které se zobrazí, klikněte na **ODSTRANIT**.
  5. Počkejte na dokončení procesu odinstalace a poté restartujte systém.
- V systému **Windows 10**:
  1. Klikněte na nabídku **Start** a poté na položku Nastavení.
  2. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Nainstalované aplikace**.
  3. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
  4. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.
  5. V okně, které se zobrazí, klikněte na **ODSTRANIT**.
  6. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

30.13. Po instalaci produktu Bitdefender se můj systém nespustí

Pokud jste právě nainstalovali produkt Bitdefender a nemůžete již restartovat systém v normálním režimu, může to být způsobeno několika příčinami.

S největší pravděpodobností je to způsobeno předchozí instalací produktu Bitdefender, která nebyla správně odinstalovaná, nebo přítomností jiného řešení zabezpečení v systému.

Každou takovou situaci můžete vyřešit následujícím způsobem:

- **Již jste Bitdefender používali a neodebrali jste ho správně.**

  Pro vyřešení:

1. Restartujte systém a spusťte ho v nouzovém režimu. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak mám restartovat do nouzového režimu?“* (str. 76).
2. Odeberte produkt Bitdefender ze systému:
   - V systému **Windows 7**:
     a. Klikněte na nabídku **Start**, přejděte do **Ovládacích panelů** a dvakrát klikněte na položku **Programy a funkce**.
     b. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
     c. V okně, které se zobrazí, klikněte na **ODSTRANIT**.
     d. Počkejte na dokončení procesu odinstalace a poté restartujte systém.
     e. Restartujte systém v normálním režimu.
   - V systémech **Windows 8 a Windows 8.1**:
     a. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
     b. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
     c. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
     d. V okně, které se zobrazí, klikněte na **ODSTRANIT**.
     e. Počkejte na dokončení procesu odinstalace a poté restartujte systém.
     f. Restartujte systém v normálním režimu.
   - V systému **Windows 10**:
     a. Klikněte na nabídku **Start** a poté na položku Nastavení.
     b. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Nainstalované aplikace**.
     c. Vyhledejte položku **Bitdefender Internet Security** a vyberte možnost **Odinstalovat**.
     d. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.

e. V okně, které se zobrazí, klikněte na **ODSTRANIT**.

f. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

g. Restartujte systém v normálním režimu.

3. Přeinstalujte produkt Bitdefender.

- **Dříve jste používali jiné řešení zabezpečení a neodebrali jste ho správně.**

  Pro vyřešení:

  1. Restartujte systém a spusťte ho v nouzovém režimu. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak mám restartovat do nouzového režimu?“* (str. 76).
  2. Odeberte druhé řešení zabezpečení ze systému:
     - V systému **Windows 7**:
       a. Klikněte na nabídku **Start**, přejděte do **Ovládacích panelů** a dvakrát klikněte na položku **Programy a funkce**.
       b. Najděte název programu, který chcete odebrat, a vyberte položku **Odebrat**.
       c. Počkejte na dokončení procesu odinstalace a poté restartujte systém.
     - V systémech **Windows 8 a Windows 8.1**:
       a. Na úvodní obrazovce systému Windows vyhledejte položku **Ovládací panely** (můžete např. začít psát „ovládací panel“ přímo na úvodní obrazovce) a poté klikněte na její ikonu.
       b. Klikněte na položku **Odinstalovat program** nebo **Programy a funkce**.
       c. Najděte název programu, který chcete odebrat, a vyberte položku **Odebrat**.
       d. Počkejte na dokončení procesu odinstalace a poté restartujte systém.
     - V systému **Windows 10**:
       a. Klikněte na nabídku **Start** a poté na položku Nastavení.
       b. Klikněte na ikonu **Systém** v oblasti Nastavení a poté vyberte položku **Nainstalované aplikace**.

c. Najděte název programu, který chcete odebrat, a vyberte položku **Odinstalovat**.

d. Počkejte na dokončení procesu odinstalace a poté restartujte systém.

Abyste druhý software korektně odinstalovali, přejděte na jeho webovou stránku a spusťte nástroj pro jeho odinstalování nebo přímo kontaktujte dodavatele, aby vám poskytl pokyny k odinstalování.

3. Restartujte systém v normálním režimu a přeinstalujte produkt Bitdefender.

Již jste provedli výše uvedený postup a situace není vyřešená.

Pro vyřešení:

1. Restartujte systém a spusťte ho v nouzovém režimu. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak mám restartovat do nouzového režimu?“* (str. 76).
2. Pomocí možnosti Obnovení systému z Windows obnovte zařízení na dřívější datum před instalací produktu Bitdefender.
3. Restartujte systém v normálním režimu a požádejte o pomoc zástupce podpory dle popisu v části *„Žádost o pomoc“* (str. 206).

31. ODSTRANĚNÍ HROZEB Z VAŠEHO SYSTÉMU

Hrozby mohou váš systém ovlivňovat mnoha různými způsoby a přístup produktu Bitdefender závisí na druhu ohrožení. Protože hrozby často mění své chování, je obtížné zjistit vzorec jejich chování a jejich činnosti.

V některých situacích produkt Bitdefender nedokáže automaticky odstranit infekční hrozby ze systému. V takových případech bude nutný váš zásah.

- *„Rescue Environment“* (str. 198)
- *„Co dělat, když Bitdefender najde na vašem zařízení hrozby?“* (str. 199)
- *„Jak vyčistím virus v archivu?“* (str. 200)
- *„Jak vyčistím hrozbu v emailovém archivu?“* (str. 201)
- *„Co mám provést, pokud mám podezření na nebezpečný soubor?“* (str. 202)
- *„Co znamenají heslem chráněné soubory v protokolu skenu?“* (str. 203)
- *„Co znamenají přeskočené položky v protokolu skenu?“* (str. 203)
- *„Co znamenají překomprimované soubory v protokolu skenu?“* (str. 203)
- *„Proč produkt Bitdefender automaticky odstranil infikovaný soubor?“* (str. 204)

Pokud zde svůj problém nemůžete najít nebo ho navrhovaná řešení neodstraní, můžete kontaktovat zástupce technické podpory společnosti Bitdefender dle postupu uvedeného v kapitole *„Žádost o pomoc“* (str. 206).

31.1. Rescue Environment

Záchranné prostředí je funkce Bitdefender, která umožňuje skenovat a dezinfikovat všechny stávající oddíly pevného disku uvnitř i vně vašeho operačního systému.

Bitdefender Rescue Environment je integrován s Windows RE,

Spuštění systému v Záchranném prostředí

Přístup k Záchrannému prostředí je možný pouze z Vašeho produktu Bitdefender, dle následujících kroků:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V podokně **ANTIVIRUS** klikněte na **Otevřít** .

3. Klikněte na **Otevřít** vedle **záchranného prostředí** .
4. V zobrazeném okně klikněte na **REBOOT** .

   Záchranné prostředí Bitdefender se za několik okamžiků načte.

Skenování systému v záchranném prostředí

Prohledání záchranného prostředí systému:

1. Vstupte do Záchranného prostředí dle popisu v „Spuštění systému v Záchranném prostředí“ (str. 198).
2. Proces skenování Bitdefender začne automaticky, jakmile bude systém načten v Záchranném prostředí.
3. Počkejte na dokončení skenu. Při nalezení jakékoli hrozby následujte pokyny pro její odstranění.
4. Záchranné prostředí ukončíte kliknutím na tlačítko **Zavřít** v okně s výsledky kontroly.

31.2. Co dělat, když Bitdefender najde na vašem zařízení hrozby?

Zjistíte, že na vašem zařízení existuje hrozba jedním z těchto způsobů:

- Prohledali jste zařízení a Bitdefender na něm našel infikované položky.
- Upozornění na hrozbu vás informuje, že Bitdefender zablokoval na vašem zařízení jednu nebo více hrozeb.

V takových situacích produkt Bitdefender aktualizujte, abyste měli nejnovější informace o hrozbách, a spusťte kompletní sken, aby systém analyzoval.

Jakmile je kompletní sken dokončený, vyberte pro infikované položky požadovanou akci (Dezinfikovat, Odstranit, Přesunout do karantény).

Varování

Pokud máte podezření, že je soubor součástí operačního systému Windows, nebo že není infikovaný, neprovádějte tento postup a co nejdříve se obraťte na zákaznickou podporu produktu Bitdefender.

Pokud zvolenou akci nebylo možné provést a protokol skenu odhalí infekci, kterou nebylo možné odstranit, může být třeba odstranit soubor nebo soubory ručně:

První způsob lze použít v normálním režimu:

1. Vypněte antivirovou ochranu produktu Bitdefender v reálném čase:
   a. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
   b. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
   c. V okně **Pokročilé** vypněte **Bitdefender Štít** .
2. Zobrazení skrytých objektů v systému Windows. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak zobrazím skryté objekty v systému Windows?“* (str. 74).
3. Přejděte do umístění infikovaného souboru (podívejte se na protokol skenu) a odstraňte ho.
4. Zapněte antivirovou ochranu produktu Bitdefender v reálném čase.

V případě, že se první metodou nepodařilo odstranit infekci:

1. Restartujte systém a spusťte ho v nouzovém režimu. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak mám restartovat do nouzového režimu?“* (str. 76).
2. Zobrazení skrytých objektů v systému Windows. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak zobrazím skryté objekty v systému Windows?“* (str. 74).
3. Přejděte do umístění infikovaného souboru (podívejte se na protokol skenu) a odstraňte ho.
4. Restartujte systém a spusťte ho v normálním režimu.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

31.3. Jak vyčistím virus v archivu?

Archiv je soubor nebo sada souborů zkomprimovaných do speciálního formátu za účelem zmenšení obsazeného místa na disku.

Některé z těchto formátů jsou otevřené, takže produktu Bitdefender umožňují skenovat obsah archivů a poté pomocí vhodného postupu odstranit infekci.

Jiné formáty archivů jsou částečně nebo zcela uzavřené a produkt Bitdefender dokáže pouze zjistit přítomnost ohrožení uvnitř, ale nemůže provést žádnou jinou akci.

Pokud vás produkt Bitdefender upozorní, že uvnitř archivu byla nalezena hrozba a není k dispozici žádná akce, znamená to, že její odstranění není možné kvůli omezenému nastavení oprávnění archivu.

Hrozbu uloženou v archivu lze odstranit následujícím způsobem:

1. Zjistěte, ve kterém archivu se hrozba nachází provedením kompletního skenu systému.
2. Vypněte antivirovou ochranu produktu Bitdefender v reálném čase:
   a. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
   b. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
   c. V okně **Pokročilé** vypněte **Bitdefender Štít** .
3. Přejděte do umístění archivu a dekomprimujte ho pomocí archivační aplikace, jako WinZip.
4. Identifikuje infikovaný soubor a odstraňte ho.
5. Smažte původní archiv, aby byla infekce zcela odstraněná.
6. Znovu zkomprimujte soubory do nového archivu pomocí archivační aplikace, např. WinZip.
7. Zapněte antivirovou ochranu produktu Bitdefender v reálném čase a proveďte kompletní sken systému, abyste se ujistili, že v něm není žádná další infekce.

Poznámka
Je důležité mít na paměti, že hrozba uložená v archivu nepředstavuje pro váš systém bezprostřední hrozbu, protože aby mohla infikovat systém, archiv musí být dekomprimován a spuštěn.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

31.4. Jak vyčistím hrozbu v emailovém archivu?

Produkt Bitdefender dokáže identifikovat také hrozby v emailových databázích a emailových archivech uložených na disku.

Někdy je nutné identifikovat infikovanou zprávu pomocí informací uvedených ve zprávě o skenu a odstranit ji ručně.

Hrozbu uloženou v emailovém archivu lze odstranit následujícím způsobem:

1. Oskenujte emailovou databázi produktem Bitdefender.
2. Vypněte antivirovou ochranu produktu Bitdefender v reálném čase:
   a. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
   b. V podokně **ANTIVIRUS** klikněte na **Otevřít** .
   c. V okně **Pokročilé** vypněte **Bitdefender Štít** .
3. Otevřete zprávu o skenu a pomocí identifikačních údajů (Předmět, Od, Komu) najděte infikované zprávy v emailovém klientovi.
4. Odstraňte infikované zprávy. Většina emailových klientů také přesouvá odstraněné zprávy do obnovitelné složky, odkud je lze obnovit. Měli byste se ujistit, že je zpráva odstraněna také z této obnovovací složky.
5. Zkomprimujte složku, ve které byla infikovaná zpráva uložena.
   - V aplikaci Microsoft Outlook 2007: V nabídce Soubor klikněte na položku Správa datových souborů. Vyberte soubory osobních složek (.pst), které chcete zkomprimovat, a klikněte na položku Nastavení. Klikněte na položku Komprese.
   - V aplikaci Microsoft Outlook 2010 / 2013/ 2016: V nabídce Soubor klikněte na položku Informace a poté na možnost Nastavení účtu (změny a odebírání účtů nebo změna stávajících nastavení připojení). Poté klikněte na datový soubor, vyberte soubory osobních složek (.pst), které chcete zkomprimovat, a klikněte na položku Nastavení. Klikněte na položku Komprese.
6. Zapněte antivirovou ochranu produktu Bitdefender v reálném čase.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Žádost o pomoc“* (str. 206).

31.5. Co mám provést, pokud mám podezření na nebezpečný soubor?

Může se stát, že nějaký soubor ve vašem systému budete považovat za nebezpečný, i když ho produkt Bitdefender nedetekoval.

Pro ujištění, že je Váš systém chráněn:

1. Proveďte v produktu Bitdefender **Kompletní sken**. Chcete-li zjistit, jak to udělat, obraťte se na *„Jak mám provést sken systému?“* (str. 54).

2. Pokud výsledky skenu vypadají v pořádku, ale stále jste na pochybách a chcete se o souboru ujistit, obraťte se na zástupce naší podpory, abychom vám mohli pomoci.

   Pokud chcete zjistit jak to udělat, obraťte se na *„Žádost o pomoc“* (str. 206).

31.6. Co znamenají heslem chráněné soubory v protokolu skenu?

Jedná se pouze o oznámení, které indikuje, že produkt Bitdefender detekoval, že tyto soubory jsou chráněny heslem nebo nějakou formou šifrování.

Nejčastěji jsou heslem chráněné následující položky:

- Soubory patřící jinému řešení zabezpečení.
- Soubory patřící operačnímu systému.

Abyste skutečně oskenovali jejich obsah, musely by být tyto soubory buď dekomprimovány, nebo jinak dešifrovány.

Pokud by byl tento obsah extrahován, skener v reálném čase Bitdefender by je automaticky prohledal, aby byl váš přístroj chráněn. Pokud chcete tyto soubory produktem Bitdefender oskenovat, je třeba kontaktovat výrobce produktu, aby vám poskytl další podrobnosti o těchto souborech.

Naším doporučením je tyto soubory ignorovat, protože pro váš systém nepředstavují hrozbu.

31.7. Co znamenají přeskočené položky v protokolu skenu?

Všechny soubory, které se ve zprávě o skenu zobrazují jako přeskočené, jsou čisté.

Z důvodu vyššího výkonu produkt Bitdefender neskenuje soubory, které se od minulého skenu nezměnily.

31.8. Co znamenají překomprimované soubory v protokolu skenu?

Překomprimované položky jsou prvky, které skenovací jádro nemohlo extrahovat, nebo prvky, u nichž by doba dešifrování byla příliš dlouhá, což by způsobilo nestabilitu systému.

Překomprimování znamená, že produkt Bitdefender přeskočil skenování v příslušném archivu, protože se ukázalo, že jeho dekomprimace by spotřebovala příliš mnoho systémových prostředků. Obsah bude v případě potřeby oskenován při přístupu v reálném čase.

31.9. Proč produkt Bitdefender automaticky odstranil infikovaný soubor?

Pokud je detekován infikovaný soubor, produkt Bitdefender se ho automaticky pokusí dezinfikovat. Pokud se dezinfekce nezdaří, soubor je přesunut do karantény, která infekci zadrží.

V případě některých druhů hrozeb není dezinfekce možná, protože detekovaný soubor je celý škodlivý. V takových případech bude infikovaný soubor z disku odstraněn.

K tomu obvykle dojde u instalačních souborů, které byly staženy z nedůvěryhodných webových stránek. Pokud se dostanete do takové situace, stáhněte instalační soubor z webových stránek výrobce nebo jiné důvěryhodné webové stránky.

CONTACT US

32. ŽÁDOST O POMOC

Produkt Bitdefender poskytuje svým zákazníkům bezkonkurenčně rychlou a přesnou podporu. Pokud se setkáte s problémem nebo máte otázky ohledně produktu Bitdefender, můžete použít několik online zdrojů k nalezení řešení nebo odpovědi. Současně můžete kontaktovat tým zákaznické podpory produktu Bitdefender. Naši zástupci podpory pohotově zodpoví vaše dotazy a poskytnou vám potřebnou pomoc.

V části *„Řešení běžných problémů“* (str. 177) najdete potřebné informace ohledně nejčastějších problémů, se kterými se můžete setkat při používání tohoto produktu.

Pokud nenajdete odpověď na svou otázku v uvedených zdrojích, můžete nás kontaktovat přímo:

- „Kontaktujte nás přímo z Bitdefender Internet Security“ (str. 206)
- „Kontaktujte nás prostřednictvím našeho centra podpory online“ (str. 207)

Kontaktujte nás přímo z Bitdefender Internet Security

Pokud máte funkční připojení k Internetu, můžete požádat podporu produktu Bitdefender o pomoc přímo z rozhraní produktu.

Postupujte následovně:

1. Klikněte na tlačítko **Podpora** , reprezentované **otazníkem** , v horní části Bitdefender Rozhraní .
2. K dispozici jsou následující možnosti:
   - **UŽIVATELSKÁ PŘÍRUČKA**

     Přístup k naší databázi a vyhledávání potřebných informací.
   - **CENTRUM PODPORY**

     Prohlížejte naše online články a video návody.
   - **PODPORA**

     Tlačítkem **Kontaktování podpory** spustíte nástroj Bitdefender - Průvodce nahlášením problému a kontaktujete Oddělení zákaznické péče.

     a. Vyplňte do formuláře k odeslání potřebné údaje:

        i. Vyberte typ problému, který chcete nahlásit.

ii. Zadejte popis problému, se kterým jste se setkali.

iii. Klikněte na **Pokusit se o opětovné vyvolání problému** v případě, že máte problém s produktem. Znovu vyvolejte problém a poté klikněte na **DOKONČIT** v okně OPĚTOVNÉ VYVOLÁNÍ PROBLÉMU.

iv. Klikněte na **Potvrdit lístek**.

b. Pokračujte vyplněním podacího formuláře nezbytnými údaji:

i. Zadejte své celé jméno.

ii. Zadejte svou emailovou adresu.

iii. Zaškrtněte políčko se souhlasem.

iv. Klikněte na **VYTVOŘIT LADICÍ BALÍČEK**.

Počkejte několik minut, než produkt Bitdefender nashromáždí související informace. Tyto informace pomohou našim technikům najít řešení vašeho problému.

c. Kliknutím na tlačítko **Zavřít** ukončíte průvodce. V nejbližší možné době budete kontaktováni jedním z našich zástupců.

Kontaktujte nás prostřednictvím našeho centra podpory online

Pokud prostřednictvím produktu Bitdefender nemáte přístup k potřebným informacím, použijte naše centrum podpory online:

1. Přejděte na web https://www.bitdef.cz/podpora/.

   Centrum podpory Bitdefender obsahuje velké množství článků, které popisují řešení problémů souvisejících s produktem Bitdefender.

2. Pomocí vyhledávacího pole v horní části okna hledejte články, které mohou nabízet řešení vašeho problému. Při hledání stačí napsat termín do pole vyhledávání a kliknout na tlačítko **Search**.

3. Přečtěte si příslušné články nebo dokumenty a vyzkoušejte navrhovaná řešení.

4. Pokud zde řešení všeho problému nenajdete, přejděte na

   https://www.bitdef.cz/kontakt/a kontaktujte zástupce podpory.

33. ONLINE ZDROJE

K dispozici je několik online zdrojů, které vám pomohou vyřešit vaše problémy a otázky související s produktem Bitdefender.

- Centrum podpory produktu Bitdefender:

  https://www.bitdef.cz/podpora/

- Fórum podpory produktu Bitdefender:

  http://forum.bitdefender.com

- Portál počítačového zabezpečení HOTforSecurity:

  http://www.hotforsecurity.com

Můžete také použít svůj oblíbený vyhledávač k nalezení dalších informací o počítačovém zabezpečení, produktech Bitdefender a společnosti.

33.1. Centrum podpory produktu Bitdefender

Centrum podpory produktu Bitdefender je online úložiště informací o produktech Bitdefender. Uchovává v snadno přístupném formátu zprávy o výsledcích probíhající technické podpory a činnostech opravy chyb týmů podpory a vývoje produktu Bitdefender, spolu s obecnějšími články o virové prevenci, správě řešení produktů Bitdefender s podrobnými vysvětleními a mnoha dalšími články.

Centrum podpory produktu Bitdefender je přístupné veřejnosti a lze ho volně prohledávat. Rozsáhlé informace, které obsahuje, jsou dalším prostředkem poskytování potřebných technických znalostí zákazníkům produktu Bitdefender. Všechny platné žádosti o informace nebo hlášení chyb od klientů produktu Bitdefender se časem dostanou do centra podpory produktu Bitdefender jako hlášení o opravách chyb, taháky pro obcházení problémů nebo informativní články doplňující soubory nápovědy produktu.

Centrum podpory produktu Bitdefender je kdykoli k dispozici na adrese

https://www.bitdef.cz/podpora/.

33.2. Fórum podpory produktu Bitdefender

Fórum podpory produktu Bitdefender poskytuje uživatelům produktu Bitdefender snadný způsob, jak získat pomoc a pomoci ostatním.

Pokud váš produkt Bitdefender nefunguje dobře nebo nedokáže z vašeho počítače odstranit určité viry, nebo pokud máte dotazy k jeho fungování, zveřejněte váš problém nebo otázku na fóru.

Technici podpory produktu Bitdefender sledují nové příspěvky a fóru, aby vám pomohli. Odpověď nebo řešení můžete rovněž získat od zkušenějšího uživatele produktu Bitdefender.

Před zveřejněním problému nebo otázky prohledejte fórum, jestli se na něm nenachází podobné nebo související téma.

Fórum podpory produktu Bitdefender je k dispozici na adrese http://forum.bitdefender.com v 5 různých jazycích: v angličtině, němčině, francouzštině, španělštině a rumunštině. Kliknutím na odkaz **Home & Home Office Protection** přejdete do části věnované spotřebitelským produktům.

33.3. Portál HOTforSecurity

HOTforSecurity je bohatý zdroj informací o počítačovém zabezpečení. Zde se dozvíte o různých hrozbách, kterým je zařízení při připojení k internetu vystaveno (malware, phishing, spam, počítačoví zločinci).

Pravidelně jsou zveřejňovány nové stránky o nejnovějších objevených hrozbách, aktuálních bezpečnostních trendech a další informace o oblasti počítačového zabezpečení.

Webová stránka HOTforSecurity je k dispozici na http://www.hotforsecurity.com.

34. CONTACT INFORMATION

Účinná komunikace je klíčem k úspěšnému obchodu. Od roku 2001 si BITDEFENDER vybudoval nezpochybnitelnou pověst díky neustálému usilování o lepší komunikaci s cílem překonat očekávání našich klientů a partnerů. V případě dotazů nás bez váhání kontaktujte.

34.1. Webové adresy

Prodejní oddělení: sales@bitdefender.com
Centrum podpory:https://www.bitdef.cz/podpora/
Dokumentace: documentation@bitdefender.com
Lokální distributoři: http://www.bitdefender.com/partners
Partnerský program: partners@bitdefender.com
Vztahy s médii: pr@bitdefender.com
Pracovní nabídky: jobs@bitdefender.com
Zasílání virů: virus_submission@bitdefender.com
Zasílání spamu: spam_submission@bitdefender.com
Oznámení zneužívání produktu: abuse@bitdefender.com
Webová stránka:https://www.bitdef.cz/

34.2. Lokální distributoři

Lokální distributoři produktu Bitdefender jsou připraveni zodpovědět jakékoli dotazy ohledně své oblasti působnosti jak v komerčních, tak v obecných záležitostech.

Chcete-li najít distributora produktu Bitdefender ve vaší zemi:

1. Přejděte na web http://www.bitdefender.com/partners/partner-locator.html.
2. Vyberte vaši zemi a město pomocí příslušných možností.
3. Pokud nenajdete distributora produktu Bitdefender ve vaší zemi, kontaktujte nás emailem na adrese sales@bitdefender.com. Email napište v angličtině, abychom vám mohli rychle pomoci.

34.3. Pobočky produktu Bitdefender

Pobočky produktu Bitdefender jsou připraveny zodpovědět jakékoli dotazy ohledně své oblasti působnosti jak v komerčních, tak v obecných záležitostech. Jejich příslušné adresy a kontakty jsou uvedeny níže.

USA

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefon (pobočka a prodej): 1-954-776-6262
Prodej: sales@bitdefender.com
Technická podpora: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

Velká Británie a Irsko

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
Email: info@bitdefender.co.uk
Phone: (+44) 2036 080 456
Prodej: sales@bitdefender.co.uk
Technická podpora: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Německo

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Pobočka: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Prodej: vertrieb@bitdefender.de
Technická podpora: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Dánsko

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Pobočka: +45 7020 2282
Technická podpora: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Španělsko

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Phone: +34 902 19 07 65
Prodej: comercial@bitdefender.es
Technická podpora: https://www.bitdefender.es/support/consumer.html
Webová stránka: https://www.bitdefender.es

Rumunsko

BITDEFENDER SRL
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 6
Bucharest
Fax: +40 21 2641799
Telefon pro prodej: +40 21 2063470
Email pro prodej: sales@bitdefender.ro
Technická podpora: https://www.bitdefender.ro/support/consumer.html
Webová stránka: https://www.bitdefender.ro

Spojené arabské emiráty

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefon pro prodej: 00971-4-4588935 / 00971-4-4589186
Email pro prodej: mena-sales@bitdefender.com
Technická podpora: https://www.bitdefender.com/support/consumer.html
Webová stránka: https://www.bitdefender.com

Významový slovník

ActiveX

Active X je šablona pro psaní programů tak, aby je ostatní programy a operační systém mohly volat. Technologii Active X používá prohlížeč Microsoft Internet Explorerem pro tvorbu interaktivních webových stránek, které vypadají a chovají se spíše jako počítačové programy, než statické stránky. Pomocí technologie Active X mohou uživatelé klást otázky a odpovídat na ně, používat tlačítka a různými způsoby interaktivně komunikovat s webovými stránkami. Ovladače Active X jsou často psány v jazyce Visual Basic.

Technologie ActiveX se vyznačuje naprostým nedostatkem bezpečnostních prvků; odborníci v oblasti počítačového zabezpečení zrazují od jejího používání na Internetu.

Advanced persistent threat

Advanced persistent threat (APT) zneužívá zranitelností systému ke zcizení důležitých informací a jejich doručení ke zdroji. Cílem tohoto viru jsou velké skupiny, jako organizace, společnosti nebo státní správa.

Cílem útoku typu advanced persistent threat je zůstat po dlouhou dobu nezjištěný a moci sledovat a shromažďovat informace bez poškození cílových počítačů. Virus je zanesen do síte prostřednictvím souboru PDF nebo dokumentu sady Office, který vypadá neškodně, takže ho mohou používat všichni uživatelé.

Adware

Adware je často kombinován s hostitelskou aplikací, která je bezplatně poskytována, pokud uživatel souhlasí s přijetím adware. Vzhledem k tomu, že aplikace adwaru se obvykle instalují poté, co uživatel souhlasí s licenční smlouvou, která uvádí účel aplikace, nedošlo k žádnému přestupku.

Přesto mohou být vyskakovací reklamy obtěžující a v některých případech snižují výkon systému. Také informace, které některé z těchto aplikací shromažďují, mohou způsobit obavy o ochranu osobních údajů u uživatelů, kteří si plně nevěděli, jaké jsou podmínky licenční smlouvy.

Aktivační kód

Jedná se o unikátní klíč, který můžete zakoupit v maloobchodě a použít k aktivaci konkrétního produktu nebo služby. Aktivační kód umožňuje aktivaci platného předplatného na určité časové období a počet zařízení a rovněž ho lze použít k prodloužení předplatného, pokud byl vygenerován pro stejný produkt nebo službu.

Aktualizace

Nová verze softwarového nebo hardwarového produktu vyvinutá za účelem nahradit starší verzi téhož produktu. Navíc se při instalaci aktualizací často zjišťuje, zda již je ve vašem počítači nainstalovaná starší verze, a pokud ne, nemůžete aktualizaci instalovat.

Bitdefender má svůj vlastní modul pro aktualizace, který Vám umožňuje aktualizace produktu kontrolovat ručně nebo produkt nechat aktualizovat automaticky.

Aktualizace informací o hrozbách

Binární vzorec hrozby, který řešení zabezpečení použije k jejímu nalezení a eliminaci.

Aplet v jazyce Java

Program v jazyce Java, který je navržen výhradně pro běh na webové stránce. Pro použití apletu na webové stránce je třeba specifikovat název apletu a velikost (délku a šířku v pixelech), kterou aplet může použít. Když vstoupíte na webovou stránku, prohlížeč stáhne aplet ze serveru a spustí ho na počítači uživatele (klientovi). Aplety se od aplikací liší v tom, že se řídí přísným bezpečnostním protokolem.

Příklad: přestože se aplety spouštějí na klientovi, nemohou z klientského počítače číst data ani je zapisovat. Aplety jsou dále omezeny tím, že mohou číst a zapisovat data pouze na doméně, z níž jsou poskytovány.

Archiv

Disk, páska nebo adresář obsahující soubory, které byly zálohovány.

Soubor, který obsahuje jeden nebo více souborů v komprimovaném formátu.

Boot sector

Sektor na začátku každého disku, který identifikuje architekturu disku (velikost sektoru, velikost clusteru atd.). U startovacích disků obsahuje spouštěcí sektor rovněž program, který načítá operační systém.

Boot vir

Virus, který infikuje spouštěcí sektor pevného disku nebo diskety. Pokus o spuštění z diskety infikované boot virem zapříčiní, že se virus v paměti aktivuje. Pokaždé, když zavedete systém z tohoto místa, budete mít aktivní virus v paměti.

Botnet

Termín "botnet" se skládá ze slov "robot" a "network" ("síť"). Botnety jsou zařízení připojená k internetu, která jsou nakažená viry a mohou být využita k odesílání emailů se spamem, ke kradení dat, k dálkovému ovládání zranitelných zařízení, nebo k šíření spywaru, ransomwaru a dalších druhů hrozeb. Jejich cílem je infikovat co nejvíce k internetu připojených zařízení, jako jsou počítače, servery, mobilní zařízení nebo zařízení s IoT patřící velkým firmám nebo průmyslům.

Červ

Program, který se sám šíří po síti a přitom se reprodukuje. Neumí se sám připojit k jiným programům.

Cesta

Přesné nasměrování k souboru v počítači. Tato nasměrování jsou obvykle popisována pomocí hierarchického souborového systému od nejvyšší úrovně dolů.

Trasa mezi dvěma body, jako je např. komunikační kanál mezi dvěma počítači.

Cookie

V internetovém žargonu jsou cookie popisovány jako malé soubory, obsahující informace o jednotlivých počítačích, které mohou být analyzovány a použity inzerenty pro vysledování vašich internetových zájmů a zálib. V této oblasti se technologie cookie stále ještě rozvíjí se záměrem cílit reklamu přímo na zájmy, které jste uvedli. Na jednu stranu se pro mnoho lidí jedná o dvousečný meč, který je účinný a relevantní, protože vidíte pouze reklamy, o které se zajímáte. Na stranu druhou ve skutečnosti „stopuje“ a „pronásleduje“, kam chodíte a na co kliknete. Je

pochopitelné, že to vyvolalo debatu o soukromí a mnoho lidí se cítí dotčeno představou, že je na ně nazíráno jako na „číslo SKU“ (určitě znáte čárový kód na zadní straně obalů, které jsou skenovány v obchodě u pokladny). Jakkoliv se může zdát tento názor extrémní, v některých případech odpovídá realitě.

Dictionary Attack - pokus o získání nedovoleného přístupu k systému počítače pomocí velké slovní zásoby pro generování potenciálních hesel.

Útoky pro odhalení hesla (Password guessing attacks) používané k proniknutí do počítačového systému zadáním kombinace běžných slov pro generování potenciálních hesel. Stejná metoda se používá k odhalení dešifrovacích klíčů zašifrovaných zpráv nebo dokumentů. Útoky pro odhalení hesla (Dictionary attacks) jsou úspěšné, protože mnoho lidí se snaží vybrat krátká a jednoduchá hesla, která lze snadno uhdnout.

Disková jednotka

Jedná se o zařízení, které čte data z disku a zapisuje je na něj.

Jednotka pevného disku čte a zapisuje na pevné disky.

Disketová jednotka přistupuje na diskety.

Diskové jednotky mohou být buďto interní (umístěné uvnitř počítače), nebo externí (umístěné v samostatné krabici, která se připojuje k počítači).

E-mail

Elektronická pošta. Služba, která zasílá zprávy na počítače prostřednictvím místních nebo globálních sítí.

E-mailový klient

Emailový klient je aplikace, která umožňuje posílat a přijímat emaily.

Exploity

Způsob, jak využít různých chyb nebo chyb zabezpečení, které jsou v počítači (software nebo hardware). Hackeři tak mohou získat kontrolu nad počítači nebo sítí.

Falešná detekce

Objeví se, když sken rozpozná soubor jako infikovaný, ačkoliv ve skutečnosti není.

Heuristika

Na pravidlech založená metoda identifikace nových virů. Tento způsob skenování je nezávislý na konkrétní databázi s informacemi o hrozbách. Výhodou heuristického skenování je, že se nenechá ošálit novou variantou existujícího viru. Nicméně občas se může stát, že ohlásí podezřelý kód u normálních programů – pak hovoříme o „falešné detekci".

Honeypot

Speciálně upravené počítačové systémy, sloužící jako návnada pro hackerské útoky, k tomu aby během incidentu a po incidentech umožnilo bezpečnostním odborníkům studovat jejich postupy a metody, které používají ke sběru systémových informací. Společnosti a korporace se zajímají o implementaci a používání honeypots pro vylepšení jejich celkové úrovně zabezpečení.

Hrozba

Program, nebo kus kódu, který je načten do Vašeho počítače bez vašeho vědomí a pracuje proti vaší vůli. Většina virů se může také replikovat. Všechny počítačové viry jsou dílem člověka. Je relativně snadné vyrobit jednoduchý virus, který se neustále kopíruje. Dokonce i tak jednoduchý vir je nebezpečný, protože rychle spotřebuje veškerou dostupnou paměť a způsobí kolaps systému. Mnohem nebezpečnějším druhem virů jsou takové, které jsou schopné se přenášet po sítích a obcházet bezpečnostní systémy.

IP

Internetový protokol - směrovací protokol v sadě protokolů TCP/IP, který je zodpovědný za adresování v sítích IP, směrování a fragmentaci a skládání paketů IP.

Keylogger

Keylogger je aplikace, která zaznamenává vše co píšete.

Keyloggery jsou ze své povahy škodlivé. Lze je použít k legitimním účelům, jako sledování aktivity zaměstnanců nebo dětí. Stále častěji je však používají počítačoví piráti k zlomyslným účelům (např. ke shromažďování soukromých dat, jako přihlašovací údaje a čísla sociálního pojištění).

Kyberšikana

Když kolegové nebo cizinci páchají násilné činy proti dětem záměrně, aby je fyzicky zranili. Aby mohli útočníci emocionálně škodit, vysílají běžné zprávy nebo nelichotivé fotografie, čímž se jejich oběti oddělují od ostatních nebo se cítí frustrované.

Makro virus

Druh počítačového viru, který je zakódovaný jako makro začleněné do dokumentu. Mnoho aplikací, jako např. Microsoft Word a Excel, podporuje výkonné jazyky maker.

Tyto aplikace umožňují vložit makro do dokumentu a nechat ho provést při každém otevření dokumentu.

Neheuristický

Tento způsob skenování je závislý na konkrétní databázi s informacemi o hrozbách. Výhodou neheuristického skenování je, že se nedá zmást domnělým virem a nespouští falešný poplach.

Online útočník

Jednotlivci, kteří usilují o nalákaní nezletilých nebo dospívajících do rozhovorů za účelem jejich zapojení se do nezákonných sexuálních aktivit. Sociální sítě jsou ideálním místem, kde mohou být zranitelné děti snadno loveny a sváděny ke spáchání sexuálních aktivit, online nebo tváří v tvář.

Paměť

Vnitřní paměťové oblasti v počítači. Termín paměť označuje datové úložiště ve formě čipů a slovo úložiště se používá pro paměť, která se nachází na páskách nebo discích. Každý počítač disponuje určitým množstvím fyzické paměti, obvykle označované jako hlavní paměť nebo RAM.

Phishing

Jedná se o rozesílání podvržených emailových zpráv, které se tváří jako legitimní, s cílem, aby uživatel poskytl soukromé informace, které budou následně použity ke krádeži identity. Email obvykle nasměruje uživatele na webovou stránku, kde má aktualizovat své osobní informace, jako hesla, údaje o kreditní kartě, číslo sociálního pojištění a čísla bankovních účtů apod., která již legitimní organizace má. Webová stránka je však falešná a vytvořená s cílem zcizit informace uživatele.

Photon

Photon je inovativní neobtěžující technologie společnosti Bitdefender, navržená k minimalizaci výkonnostního dopadu antivirové ochrany. Sledováním činnosti vašeho počítače na pozadí rozpoznává návyky používání, které pomáhají optimalizovat procesy spouštění a skenování.

Položky Po spuštění

Veškeré soubory uložené v této složce se po startu počítače spustí. Například obrazovka při startu, zvukový soubor, který se přehraje, když je počítač poprvé spuštěn, kalendář s upomínkami nebo různé aplikace. Obvykle je v této složce uložen jen odkaz na soubor, nikoliv soubor samotný.

Polymorfní virus

Virus, který mění svoji formu v každém souboru, který infikuje. Jelikož takové viry nemají konzistentní binární vzorec, je těžké je identifikovat.

Port

Rozhraní v počítači, ke kterému můžete připojit zařízení. Osobní počítače mají různé druhy portů. Uvnitř je celá řada portů pro připojení diskových jednotek, displejů a klávesnic. Vně mají osobní počítače porty pro připojení modemů, tiskáren, myší a dalších periferních zařízení.

V sítích TCP/IP a UDP je to konečný bod logického propojení. Číslo portu udává, o jaký typ portu jde. Např. port 80 je používán pro HTTP provoz.

Předplatné

Kupní smlouva, která uživateli poskytuje právo užívat konkrétní produkt nebo službu na určitém počtu zařízení a po určitou dobu. Prošlé předplatné lze automaticky obnovit pomocí informací poskytnutých uživatelem při prvním nákupu.

Příkazový řádek

V rozhraní příkazového řádku píše uživatel příkazy do prostoru přímo na obrazovce s použitím jazyka příkazového řádku.

Přípona názvu souboru

Součást názvu souboru, nacházející se za tečkou, která indikuje druh dat uložených v souboru.

Mnohé operační systémy používají přípony názvů souborů, např. Unix, VMS a MS-DOS. Skládají se obvykle z 1-3 písmen (některé staré operační

systémy nepodporují více než tři). Jako příklad poslouží „c“ jako zdrojový kód v jazyce C, „ps“ jako PostScript, „txt“ pro libovolný text.

Prohlížeč

Krátké pro webový prohlížeč, softwarovou aplikaci určenou k vyhledání a zobrazení webových stránek. Mezi oblíbené prohlížeče patří Microsoft Internet Explorer, Mozilla Firefox a Google Chrome. Jedná se o grafické prohlížeče, což znamená, že umějí zobrazit grafiku i text. Navíc, většina nejmodernějších prohlížečů umí prezentovat multimediální informace, včetně zvuku a videa, ačkoliv pro některé formáty vyžadují moduly plug-in.

Ransomware

Ransomware je škodlivý program, který se snaží získávat peníze od uživatelů tím, že uzamkne jejich zranitelné systémy. Mezi varianty, které napadají osobní systémy uživatelů, patří CryptoLocker, CryptoWall a TeslaWall.

Infekce se může šířit přístupem k nevyžádanému emailu, stažením emailových příloh nebo instalací aplikací bez informování uživatele o dění v systému. Uživatelé a společnosti jsou denně ohrožováni hackery používajícími ransomware.

Rootkit

Rootkit je sada softwarových nástrojů, které nabízejí přístup k systému na úrovni správce. Termín byl poprvé použit pro UNIXové operační systémy a označoval překompilované nástroje, které vetřelci poskytovaly administrátorská práva, umožňující utajit jeho přítomnost i před samotnými správci systému.

Hlavní úlohou rootkitů je maskovat procesy, soubory, přihlašování a protokoly. Rovněž mohou zachytávat data z terminálů, síťových připojení nebo periferií, pokud se včlení do příslušného softwaru.

Rootkity nejsou ve skutečnosti nebezpečné. Například systémy a dokonce některé aplikace skrývají kritické soubory používající rootkity. Nicméně jsou většinou používány ke skrývání hrozeb nebo maskování přítomnosti vetřelce v systému. V kombinaci s viry představují rootkity velkou hrozbu pro integritu a bezpečnost systému. Mohou monitorovat síťový provoz, vytvořit zadní vrátka do systému, modifikovat soubory a protokoly, a zabránit tak své detekci.

Skript

Jiný termín pro makro nebo pro dávkový soubor; skript je seznam příkazů, které mohou být vykonány bez uživatelovy interakce.

Soubor se zprávou

Soubor, který obsahuje seznam akcí, ke kterým došlo. Produkt Bitdefender uchovává soubor se zprávou, ve které jsou uvedeny skenované cesty, složky, počet skenovaných archivů a souborů, počet nalezených infikovaných a podezřelých souborů.

Spam

Nevyžádaná pošta nebo nevyžádané příspěvky v diskuzních skupinách. Obecně jsou označovány jako nevyžádané emaily.

Spyware

Jakýkoli software, který tajně shromažďuje informace o uživateli prostřednictvím internetového připojení bez jeho vědomí, obvykle pro reklamní účely. Spywarové aplikace jsou většinou skrytou součástí freewarových nebo sharewarových programů, volně přístupných na Internetu; nicméně je třeba poznamenat, že většina freewarových a sharewarových aplikací spyware neobsahuje. Pokud je spyware nainstalován, monitoruje aktivitu uživatele na internetu a na pozadí odesílá tyto informace někomu jinému. Spyware také může shromažďovat informace o emailových adresách a dokonce i hesla a čísla kreditních karet.

Spyware je obdobná hrozba jako Trojský kůň, uživatelé nechtěně nainstalují produkt, když instalují něco jiného. Nejobvyklejším způsobem, jak se stát obětí spywaru, je stahování některých v současnosti dostupných produktů pro výměnu souborů metodou peer-to-peer.

Vedle otázky etiky a porušování soukromí spyware zabírá také paměťové prostředky počítače a přenosové pásmo, když odesílá informace zpět na svou domovskou základnu prostřednictvím internetového připojení uživatele. Protože spyware využívá paměť a systémové prostředky, aplikace běžící na pozadí mohou vést až k pádu systému a jeho obecné nestabilitě.

Stahování

Znamená kopírování dat (obyčejně celého souboru) z hlavního zdroje na periferní zařízení. Tento termín je obvykle používán pro popis procesu

kopírování souboru z online služby na vlastní počítač. Stahování může často znamenat kopírování souboru ze síťového souborového serveru na počítač v síti.

Systémová lišta

Systémová lišta, uvedená se systémem Windows 95, se nachází na hlavním panelu systému Windows (obvykle dole vedle hodin) a obsahuje miniaturní ikony pro snadný přístup k systémovým funkcím, jako je fax, tiskárna, modem, hlasitost atd. Dvojím kliknutím nebo kliknutím pravým tlačítkem na ikonu zobrazíte a získáte přístup k podrobnostem a ovládacím prvkům.

TCP/IP

Transmission Control Protocol/Internet Protocol - sada síťových protokolů široce používaných na Internetu, které zajišťují komunikaci mezi propojenými sítěmi počítačů s různorodou hardwarovou architekturou a rozličnými operačními systémy. Protokol TCP/IP obsahuje standardy pro komunikaci počítačů a konvence pro propojení sítí a směrování provozu.

Trójský kůň

Destruktivní program, který se maskuje jako neškodná aplikace. Na rozdíl o škodlivého softwaru a červů se trojské koně nereplikují, ale mohou být stejně tak ničivé. Jedním z nejzákeřnějších typů trojského koně je program, který slibuje odstranění virů z Vašeho počítače, ale namísto toho do počítače viry zavede.

Termín pochází z příběhu Homérovy Illiady, v němž Řekové darují obrovského dřevěného koně svému nepříteli, Trójanům, jako symbol míru. Jakmile však Trójané dovlečou koně dovnitř městských hradeb, řečtí vojáci vylezou z dutých útrob koně a otevřou městské brány, aby tak umožnili svým spolubojovníkům proniknout dovnitř a zmocnit se Tróje.

Události

Akce nebo událost odhalená programem. Událostmi mohou být aktivity uživatele, jako např. kliknutí tlačítkem myši nebo stisk klávesy, nebo systémové události, jako např. zaplnění paměti.

Útok hrubou silou

Útok pro odhalení hesla (Password guessing attack) se používá ke vstupu do systému počítače, zadáním možných kombinací hesel, většinou počínaje nejjednodušším heslem.

Virtuální Privátní Síť (VPN)

Je to technologie, která umožňuje dočasné šifrované spojení k určité síti přes méně zabezpečenou síť. Touto cestou je posílání a přijímání dat bezpečné a šifrované. Slídilové tuto komunikaci těžko odchytí. Důkazem bezpečnosti je autentizace, což lze provést pouze pomocí uživatelského jména a hesla.

Zadní vrátka

Díra v zabezpečení systému, kterou návrháři nebo údržbáři úmyslně zanechali. Nemusí se vždy jednat o zlý úmysl; některé operační systémy, např. počítají s privilegovanými účty zamýšlenými pro používání terénními servisními techniky nebo programátory údržby dodavatele.

Zkomprimované programy

Soubor v komprimovaném formátu. Mnoho operačních systémů a aplikací obsahuje příkazy, které Vám umožní zkomprimovat soubor tak, aby zabíral méně paměti. Například předpokládejme, že máte textový soubor obsahující deset mezer za sebou. Normálně by takový soubor vyžadoval deset bajtů paměti.

Program, který komprimuje soubory, však nahradí mezery speciálním znakem pro řadu mezer a číslem udávajícím počet mezer, které byly nahrazeny. V tomto případě pak deset mezer potřebuje pouze dva bajty. Tohle je pouze jedna z komprimačních metod, ale existuje jich mnohem více.