Bitdefender ANTIVIRUS PLUS

UŽIVATELSKÁ PŘÍRUČKA

Bitdefender Antivirus Plus
Uživatelská příručka

Datum vydání 07. srpna 2018

Copyright© 2018 Bitdefender

Právní oznámení

Všechna práva vyhrazena. Žádná část tohoto dokumentu nemůže být reprodukována ani šířena dál v jakékoli formě a jakýmikoli prostředky, elektronicky ani mechanicky, včetně kopírování, záznamu nebo jakéhokoli systému pro uchovávání a sběr informací, bez písemného souhlasu oprávněného zástupce společnosti Bitdefender. Začlenění krátkých citací do recenzí je možné pouze s uvedením citovaného zdroje. Obsah nesmí být žádným způsobem modifikován.

Varování a odmítnutí odpovědnosti. Tento produkt a jeho dokumentace jsou chráněny autorským právem. Informace v tomto dokumentu jsou poskytovány „tak, jak jsou“, bez záruky. I když byla během přípravy tohoto dokumentu učiněna veškerá opatření, autoři se žádné osobě ani subjektu nezodpovídají za ztrátu nebo škodu přímo či nepřímo způsobenou nebo údajně způsobenou použitím informace z tohoto dokumentu.

Tato kniha obsahuje odkazy na webové stránky třetích stran, které nejsou pod kontrolou společnosti Bitdefender. Proto společnost Bitdefender neodpovídá za obsah žádné odkazované stránky. Pokud navštívíte webovou stránku třetí strany uvedenou v tomto dokumentu, činíte tak na vlastní nebezpečí. Společnost Bitdefender poskytuje tyto odkazy pouze z praktických důvodů a začlenění těchto odkazů neznamená, že společnost Bitdefender podporuje nebo přijímá jakoukoli odpovědnost za obsah stránek třetích stran.

Ochranné známky. V tomto dokumentu mohou být použity názvy ochranných známek. Všechny registrované i neregistrované ochranné známky jsou majetkem příslušných vlastníků a jsou náležitě uznávány.

Bitdefender

Obsah

Instalace ... 1

1. Příprava na instalaci ... 2

2. Požadavky na systém ... 3
2.1. Minimální požadavky na systém ... 3
2.2. Doporučené požadavky na systém ... 3
2.3. Softwarové požadavky ... 4

3. Instalace produktu Bitdefender ... 5
3.1. Instaluj z Bitdefender Central ... 5
3.2. Instalace z instalačního disku ... 7

Začínáme ... 12

4. Základy ... 13
4.1. Otevření okna produktu Bitdefender ... 14
4.2. Upozornění ... 15
4.3. Profily ... 16
4.3.1. Nastavte automatickou aktivaci profilů ... 16
4.4. Ochrana nastavení produktu Bitdefender heslem ... 17
4.5. Produktová hlášení ... 17
4.6. Oznámení o speciálních nabídkách ... 18
4.7. Služba Antimalwarového skenování ... 18

5. Rozhraní produktu Bitdefender ... 19
5.1. Ikona oznamovací oblasti ... 19
5.2. Navigační menu ... 21
5.3. Kontrolní panel ... 21
5.3.1. Oblast stavu zabezpečení ... 22
5.3.2. Autopilot ... 23
5.3.3. Rychlé akce ... 23
5.4. Sekce Bitdefender ... 24
5.4.1. **Ochrana** ... 24
5.4.2. **Soukromí** ... 26
5.5. Bezpečnostní semafor ... 27
5.5.1. Skenování souborů a složek ... 28
5.5.2. Skrýt/Zobrazit bezpečnostní semafor ... 29

6. Bitdefender Central ... 30
6.1. Přistupuji na Bitdefender Central ... 30
6.2. Moje předplatná ... 31
6.2.1. Kontrola dostupných předplatných ... 31
6.2.2. Přidání nového zařízení ... 31
6.2.3. Obnovení předplatného ... 32
6.2.4. Aktivace předplatného ... 32
6.3. Moje zařízení ... 33
6.4. Můj účet ... 35

6.5. Upozornění 35

7. Aktualizace produktu Bitdefender 36
7.1. Kontrola aktuálnosti produktu Bitdefender 36
7.2. Provedení aktualizace 37
7.3. Zapnutí nebo vypnutí automatických aktualizací 37
7.4. Úprava nastavení aktualizací 38
7.5. Průběžné aktualizace 39

Doporučené postupy 40

8. Instalace 41
8.1. Jak nainstaluji produkt Bitdefender na druhý počítač? 41
8.2. Jak mohu přeinstalovat Bitdefender? 41
8.3. Odkud mohu stáhnout produkt Bitdefender? 42
8.4. Jak mohu změnit jazyk mého Bitdefender produktu? 43
8.5. Jak mohu použít předplatné produktu Bitdefender po upgradu systému Windows? 45
8.6. Jak mohu aktualizovat Bitdefender na nejnovější verzi? 47

9. Předplatná 49
9.1. Jak aktivuji předplatné produktu Bitdefender pomocí licenčního klíče? 49

10. Bitdefender Central 51
10.1. Jak se mohu přihlásit k účtu Bitdefender Central pomocí jiného online účtu? 51
10.2. Jak vypnout pomocné zprávy Bitdefender Central? 51
10.3. Zapoměl jsem heslo které jsem nastavil pro svůj účet Bitdefender. Jak jej resetovat? 52
10.4. Jak mohu spravovat přihlašovací relace spojené s mým Bitdefender účtem? 53

11. Skenování pomocí produktu Bitdefender 54
11.1. Jak provést sken souboru nebo složky? 54
11.2. Jak mám provést sken systému? 54
11.3. Jak mám naplánovat sken? 55
11.4. Jak mám vytvořit vlastní sken? 55
11.5. Jak mohu vyloučit složku ze skenování? 56
11.6. Co dělat, když produkt Bitdefender detekuje čistý soubor jako infikovaný? . . . 57
11.7. Jak zjistím, jaké viry produkt Bitdefender detekoval? 58

12. Kontrola soukromí 59
12.1. Jak se ujistím, že jsou moje online transakce zabezpečené? 59
12.2. Jak s pomocí produktu Bitdefender trvale odstraním soubor? 59
12.3. Jak mohu manuálně obnovit zašifrované soubory, když procesy obnovy selže? 60

13. Užitečné informace 61
13.1. Jak otestuji své řešení zabezpečení? 61
13.2. Jak odeberu produkt Bitdefender? 61
13.3. Jak odeberu Bitdefender VPN? 62
13.4. Jak automaticky vypnout počítač po dokončení skenu? 63

13.5. Jak nakonfigurovat produkt Bitdefender, aby používal připojení k Internetu pomocí proxy? . . . 64
13.6. Používám 32bitovou, nebo 64bitovou verzi systému Windows? . . . 65
13.7. Jak zobrazím skryté objekty v systému Windows? . . . 66
13.8. Jak odinstalovat jiná řešení zabezpečení? . . . 66
13.9. Jak mám restartovat do nouzového režimu? . . . 68

Správa vašeho zabezpečení . . . 70

14. Antivirová ochrana . . . 71
14.1. Skenování při přístupu (ochrana v reálném čase) . . . 72
14.1.1. Zapnutí nebo vypnutí ochrany v reálném čase . . . 72
14.1.2. Rozšířená nastavení konfigurace ochrany v reálném čase . . . 72
14.1.3. Obnovení výchozích nastavení . . . 76
14.2. Manuální skenování . . . 76
14.2.1. Skenování na hrozby v souboru nebo složce . . . 76
14.2.2. Provedení rychlého skenu . . . 77
14.2.3. Provedení kompletního skenu . . . 77
14.2.4. Konfigurace vlastního skenu . . . 78
14.2.5. Průvodce antivirovým skenem . . . 81
14.2.6. Kontrola protokolů skenů . . . 84
14.3. Automatický sken vyjímatelných médií . . . 85
14.3.1. Jak to funguje? . . . 85
14.3.2. Správa skenů vyjímatelných médií . . . 86
14.4. Skenovat soubor hosts . . . 86
14.5. Konfigurace výjimek skenování . . . 87
14.5.1. Vyloučení souborů a složek ze skenování . . . 87
14.5.2. Vyloučení přípon souborů ze skenování . . . 88
14.5.3. Správa výjimek ze skenování . . . 89
14.6. Správa souborů v karanténě . . . 89

15. Pokročilá Ochrana . . . 91
15.1. Zapnutí/vypnutí Pokročilé ochrany před hrozbami . . . 91
15.2. Kontrola detekovaných škodlivých útoků . . . 91
15.3. Přidávání procesů mezi výjimky . . . 92

16. Prevence online hrozeb . . . 93
16.1. Výstrahy produktu Bitdefender v prohlížeči . . . 94

17. Zranitelnosti . . . 96
17.1. Skenování zranitelností systému . . . 96
17.2. Používání automatického sledování zranitelností . . . 97
17.3. Wi-Fi Bezpečnostní Poradce . . . 100
17.3.1. Zapnutí nebo vypnutí notifikací Wi-Fi Poradce bezpečnosti . . . 100
17.3.2. Konfigurace domácí Wi-Fi sítě . . . 100
17.3.3. Veřejná Wi-Fi . . . 101
17.3.4. Kontroluji informace o síti Wi-Fi . . . 101

18. Bezpečné Soubory . . . 103
18.1. Zapnutí/vypnutí Bezpečných souborů . . . 103
18.2. Chraňte osobní soubory před ransomwarovými útoky . . . 104

18.3. Konfigurace přístupu k aplikacím 104
18.4. Ochrana při bootu 105

19. Odstranění Ramsomware 106
19.1. Zapnutí nebo vypnutí ochrany před ransomwarem 106
19.2. Zapínání a vypínaní automatické obnovy 106
19.3. Zobrazování souborů, které byly automaticky obnoveny 106
19.4. Ruční obnovení zašifrovaných souborů 107
19.5. Přidávání aplikací do výjimek 107

20. Ochrana vašich osobních dat správcem hesel 109
20.1. Vytvoření nové portmonkové databáze 110
20.2. Importovat existující databázi 110
20.3. Export portmonkové databáze 111
20.4. Synchronizace vašich portmonek do cloudu 111
20.5. Správa přihlašovacích údajů v Portmonce 112
20.6. Zapnutí nebo vypnutí ochrany Správcem hesel 112
20.7. Správa nastavení Správce hesel 112

21. VPN 116
21.1. Instalace VPN 116
21.2. Otevírám VPN 117
21.3. Rozhraní VPN 117
21.4. Předplatná 118

22. Zabezpečení Safepay pro online transakce 119
22.1. Použití prohlížeče Bitdefender Safepay™ 119
22.2. Konfigurace nastavení 121
22.3. Správa záložek 122
22.4. Vypnutí upozornění Safepay 123
22.5. Používání VPN se Safepay 123

23. Ochrana dat 124
23.1. Trvalé odstranění souborů 124

24. USB imunizátor 126

Optimalizace systému 127

25. Profily 128
25.1. Pracovní profil 129
25.2. Filmový profil 130
25.3. Herní profil 131
25.4. Profil Veřejná Wi-Fi 132
25.5. Profil režimu baterie 133
25.6. Optimalizace v reálném čase 134

Řešení problémů 135

26. Řešení běžných problémů 136
26.1. Systém je pomalý 136
26.2. Sken se nespustí 137

26.3. Nemůžete používat aplikaci 140
26.4. Co dělat, když produkt Bitdefender blokuje bezpečnou webovou stránku nebo online aplikaci 141
26.5. Co dělat pokud Bitdefender detekuje bezpečnou aplikaci jako ransomware . . . 141
26.6. Jak aktualizovat produkt Bitdefender na pomalém připojení k Internetu 142
26.7. Služby produktu Bitdefender neodpovídají 142
26.8. Funkce automatického vyplňování v mé portmonce nefunguje 143
26.9. Odebrání produktu Bitdefender se nezdařilo 144
26.10. Po instalaci produktu Bitdefender se můj systém nespustí 145

27. Odstranění hrozeb z vašeho systému 149
27.1. Bitdefender Záchranný režim (Záchranné prostředí ve Windows 10) 149
27.2. Co dělat, když produkt Bitdefender ve vašem počítači najde viry? 153
27.3. Jak vyčistím virus v archivu? 154
27.4. Jak vyčistím hrozbu v emailovém archivu? 155
27.5. Co mám provést, pokud mám podezření na nebezpečný soubor? 156
27.6. Co znamenají heslem chráněné soubory v protokolu skenu? 157
27.7. Co znamenají přeskočené položky v protokolu skenu? 157
27.8. Co znamenají překomprimované soubory v protokolu skenu? 158
27.9. Proč produkt Bitdefender automaticky odstranil infikovaný soubor? 158

Kontaktujte nás 159

28. Požádání o pomoc 160

29. Online zdroje 162
29.1. Centrum podpory produktu Bitdefender 162
29.2. Fórum podpory produktu Bitdefender 162
29.3. Portál HOTforSecurity 163

30. Kontaktní informace 164
30.1. Webové adresy 164
30.2. Lokální distributoři 164
30.3. Pobočky produktu Bitdefender 164

Významový slovník 167

INSTALACE

1. PŘÍPRAVA NA INSTALACI

Před instalací produktu Bitdefender Antivirus Plus proveďte následující přípravy, abyste zajistili hladký průběh instalace:

- Ujistěte se, že počítač, na který chcete produkt Bitdefender nainstalovat, splňuje minimální požadavky na systém. Pokud počítač všechny minimální požadavky na systém nesplňuje, produkt Bitdefender se nenainstaluje, nebo v případě, že se nainstaluje, nebude fungovat správně a bude způsobovat zpomalení a nestabilitu systému. Úplný seznam požadavků na systém najdete zde *„Požadavky na systém“* (str. 3).
- Přihlaste se k počítači pomocí účtu správce.
- Odinstalujte z počítače jiné podobné aplikace. 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.
- Doporučujeme připojit počítač během instalace k internetu, i v případě instalace z disku 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

Produkt Bitdefender Antivirus Plus lze nainstalovat pouze na počítače s následujícími operačními systémy:

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

Před instalací se ujistěte, že váš počítač splňuje minimální požadavky na systém.

Poznámka

Pokud chcete zjistit, jaký operační systém Windows váš počítač používá, a informace o hardwaru, postupujte následovně:

- 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. Minimální požadavky na systém

- 2 GB volného místa na pevném disku
- Procesor Dual Core 1.6 GHz
- 1 GB paměti (RAM)

2.2. Doporučené požadavky na systém

- 2,5 GB volného místa na pevném disku (nejméně 800 MB na systémové jednotce)
- Procesor Intel CORE Duo (2 GHz) nebo ekvivalentní
- 2 GB paměti (RAM)

2.3. Softwarové požadavky

Aby bylo možné používat produkt Bitdefender a všechny jeho funkce, váš počítač 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

3. INSTALACE PRODUKTU BITDEFENDER

Produkt Bitdefender lze nainstalovat z instalačního disku nebo pomocí webového instalačního programu, který můžete stáhnout do počítače z platformy Bitdefender Central.

Jestliže váš nákup zahrnuje licence pro více než jeden počítač (for např. pokud jste produkt Bitdefender Antivirus Plus zakoupili pro 3 počítače), opakujte postup instalace a aktivujte produkt na všech počítačích pomocí stejného účtu. 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 Antivirus Plus aktivován.

Pro stáhnutí Bitdefender Antivirus Plus 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 uložte instalační soubor.
   - **Chránit další zařízení**

     Vyberte tuto možnost a poté klikněte na **ODESLAT ODKAZ KE STAŽENÍ**. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Zapamatujte si, 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.

Ověření instalace

Bitdefender nejprve zkontroluje systém z důvodu ověření instalace.

Pokud systém nesplňuje minimální požadavky na instalaci produktu 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. Pro dokončení odebrání nalezených antivirových programů může být nutné restartovat počítač.

Instalační balíček produktu Bitdefender Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus.

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.

Proběhne antivirový sken kritických oblastí systému, stáhnou a nainstalují se nejnovější verze souborů aplikace a budou spuštěny služby produktu Bitdefender. Tento krok může trvat několik minut. Pokud chcete svůj systém skenovat později, klikněte na **Přeskočit sken**. Další informace o spuštění skenování systému naleznete na *„Provedení kompletního skenu“* (str. 77).

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. Pro pokračování klikněte na **ZAČÍT POUŽÍVAT Bitdefender**.

4. krok - začínáme

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

Klikněte na tlačítko **Dokončit** a přejdete do rozhraní produktu Bitdefender Antivirus Plus.

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 produktu 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. Pro dokončení odebrání nalezených antivirových programů může být nutné restartovat počítač.

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 Antivirus Plus 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 Antivirus Plus.

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.

Kritické oblasti vašeho systému jsou skenovány proti hrozbám a služby Bitdefender jsou spuštěny. Tento krok může trvat několik minut. Pokud

chcete svůj systém skenovat později, klikněte na **Přeskočit sken**. Další informace o spuštění skenování systému naleznete na *„Provedení kompletního skenu“* (str. 77).

3. krok - dokončení instalace

Zobrazí se shrnutí instalace. Pokud byla během instalace nalezena a odstraněna aktivní hrozba, může být nutný restart systému. Pro pokračování klikněte na **ZAČÍT POUŽÍVAT Bitdefender**.

Krok 4 - Bitdefender účet

Po dokončení počátečního nastavení se zobrazí okno 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 alespoň 8 znaků a obsahovat číslici.
  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**, a pak napište svojí emailovou adresu a heslo Vašeho Bitdefender účtu.

   Pro pokračování klikněte na **Přihlásit se**.

2. V případě, že jste zapomněli heslo k vašemu účtu nebo jej chcete resetovat, vyberte možnost **Zapomenuté heslo** . Zadejte svou e-mailovou adresu a klikněte na tlačítko **ZAPOMENUTÉ HESLO**. Zkontrolujte váš emailový účet a řiďte se instrukcemi pro nastavení nového hesla pro váš Bitdefender účet.

   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 5 - Aktivace vašeho produktu

Poznámka
Tento krok se objeví, pokud jste vybrali vytvoření nového Bitdefender účtu během předešlého kroku, nebo pokud jste přihlášeni na účet s vypršeným předplatným.

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 od 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 testovacího období vyberte **Nemám předplatné, chci testovat produkt zdarma**, a poté klikněte na **POKRAČOVAT**.

6. krok - začínáme

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

Klikněte na tlačítko **Dokončit** a přejdete do rozhraní produktu Bitdefender Antivirus Plus.

ZAČÍNÁME

4. ZÁKLADY

Po instalaci produktu Bitdefender Antivirus Plus je váš počítač chráněn před všemi druhy malwaru (jako viry, spyware, ransomware, pokusy o zneužití, botnety a trojské koně).

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. 116).

Můžete mít přehled o svých heslech a online uživatelských účtech tak, že je uložíte *„Ochrana vašich osobních dat správcem hesel“* (str. 109) do peněženky. Používáním jediného hlavního hesla máte možnost chránit své soukromí před vetřelci, kteří by se mohli pokusit obrat Vás o peníze.

Aby jste byli chráněni proti případným špionům a slídilům, když je Vaše zařízení připojeno k nezabezpečené bezdrátové síti, Bitdefender analyzuje její úroveň zabezpečení a když je potřeba, navrhne doporučené možnosti pro zvýšení bezpečnosti Vašich online aktivit. Pro pokyny, jak udržet svá soukromá data v bezpečí, prosím odkažte se na *„ Wi-Fi Bezpečnostní Poradce“* (str. 100).

Vaše osobní soubory, uložené lokálně, jako dokumenty, fotky nebo filmy, a také soubory uložené na cloudu, mohou nyní zůstat v bezpečí a daleko od hrozby dnešního nejnebezpečnějšího druhu malwaru, konkrétně před ransomwarem. Pro pokyny, jak vložit osobní soubory do úkrytu, prosím odkažte se na *„Bezpečné Soubory“* (str. 103).

Soubory zašifrované ransomwarem můžeme teď obnovit bez nutnosti zaplatit výkupné. Pro informace jak obnovit zašifrované soubory se obraťte na *„Odstranění Ramsomware“* (str. 106).

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. 128).

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. 15).

Čas od času je třeba otevřít Bitdefender a vyřešit jakékoliv existující problémy. Pro ochranu vašeho počítače a dat může být třeba nakonfigurovat určité součásti produktu Bitdefender nebo provést preventivní opatření.

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

V části „Doporučené postupy“ (str. 40) najdete postupy k provádění běžných úkonů. Pokud se během používání produktu Bitdefender setkáte s problémy, nahlédněte do části *„Řešení běžných problémů“* (str. 136), kde můžete najít případná řešení nejčastějších problémů.

4.1. Otevření okna produktu Bitdefender

Hlavní rozhraní produktu Bitdefender Antivirus Plus zobrazíte provedením následujícího postupu:

- 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 Antivirus Plus** 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. 19).

4.2. Upozornění

Produkt Bitdefender uchovává podrobný protokol událostí ohledně své činnosti na vašem počítači. 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 zjistit, jestli se úspěšně provedla aktualizace, zda byly v počítači nalezeny hrozby, 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.

Pro povolení Bitdefender aktivovat profily:

1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
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. Manuálně aktivován nemůže být víc než jeden profil současně.

Pro více informací o Profilech, obraťte se na„*Profily*“ (str. 128)

4.4. Ochrana nastavení produktu Bitdefender heslem

Pokud nejste jedinou osobou s právy správce, která používá tento počítač, je doporučeno chránit nastavení produktu 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.

4.7. Služba Antimalwarového skenování

Bitdefender je integrován s rozhraním Microsoft Antimalware Scan Interface (AMSI), který vám pomůže zůstat chráněni před škodlivým softwarem založeným na dynamickém skriptu a netradičním způsobem kyberatacků. AMSI je standard generického rozhraní, který umožňuje aplikacím a službám integrovat se s produkty Bitdefender.

Zapnutí nebo vypnutí integrace pomocí funkce Antimalware Scan Interface:

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

Integrace s rozhraním Antimalware Scan Interface je ve výchozím nastavení povolena a je k dispozici pouze v systému Windows 10.

5. ROZHRANÍ PRODUKTU BITDEFENDER

Produkt Bitdefender Antivirus Plus 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.

V navigačním menu na levé straně máte přístup ke svému Bitdefender účtu , oblasti nastavení, oznámení a sekcí Bitdefender pro podrobnou konfiguraci a pokročilé úpravy správy. Také nás můžete kontaktovat, v případě, že máte nějaké dotazy.

Pokud chcete mít neustálý přehled o podstatných informacích o zabezpečení a mít rychlý přístup k hlavním nastavením, přidejte si na plochu bezpečnostní semafor.

5.1. Ikona oznamovací oblasti

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

Poznámka

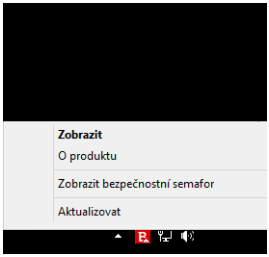
Ikona produktu Bitdefender nemusí být vždy vidět. Pro zobrazení ikony permanentně:

- 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. Klikněte pravým tlačítkem na hlavní panel a vyberte položku **Vlastnosti**.
  2. V okně hlavního panelu klikněte na položku **Přizpůsobit**.
  3. Klikněte na odkaz **Vyberte, které ikony se zobrazí na hlavním panelu** v okně **Oznámení a akce**.
  4. 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.



Ikona na hlavním panelu

- **Zobrazit** - otevře hlavní okno produktu Bitdefender.
- **About** - 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.
- **Skrýt/Zobrazit bezpečnostní semafor** - povolí/zakáže bezpečnostní semafor.
- **Aktualizovat** - spustí okamžitou aktualizaci. Stav aktualizace můžete sledovat v panelu Aktualizace hlavního okna produktu Bitdefender.

Ikona oznamovací oblasti produktu Bitdefender informuje o případných problémech ovlivňujících váš počítač nebo o činnosti produktu zobrazením speciálního symbolu, viz níže:

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 v rozhraní Bitdefender se nachází navigační menu, které vám umožňuje rychlý přístup k funkcím a nástrojům Bitdefender, které potřebujete k ovládání vašeho produktu. 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**. Odsud můžete spouštět a konfigurovat antivirové skeny, přistupovat k nastavení Firewall, chránit soubory a aplikace před ransomwarovými útoky, obnovit data v případě, že jsou zašifrována ransomwarem, a nastavit ochranu během surfování po internetu.
- **Soukromí**. Odsud můžete vytvářet správce hesel pro vaše online účty, chránit vaši webkameru před přístupem nežádaných očí, provádět online platby v bezpečném prostředí a otevírat aplikaci VPN.
- **Události**. Odtud máte přístup ke generovaným událostem.
- **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.
- **Nastavení**. Odtud máte přístup k obecným nastavením.
- **Podpora**. Odteď, kdykoliv budete potřebovat pomoc pří řešení problému s Bitdefender Antivirus Plus, můžete kontaktovat Bitdefender oddělení technické podpory.

5.3. Kontrolní 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 kontrolovat bezpečnostní stav vašeho počítače.

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

Produkt Bitdefender používá systém sledování problémů pro detekci a oznamování problémů, které mohou ovlivňovat zabezpečení vašeho počítače a dat. Zjištěné problémy zahrnují důležitá nastavení ochrany, která byla vypnuta, a jiné podmínky, které představují bezpečnostní riziko.

Kdykoli se vyskytnou problémy, které ohrozí bezpečnost vašeho počítače, stav zobrazený v horní části rozhraní Bitdefender změní barvu 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**. Spuštění rychlého skenu pro okamžitou detekci možných hrozeb, které se mohou vyskytovat ve vašem systému.
- **Systémový sken**. Spustit systémový sken, který zajistí, že se v počítači nenacházejí žádné hrozby.
- **Sken zranitelností**. Skenování zranitelností ve vašem počítači, aby bylo zajištěno, že všechny nainstalované aplikace i operační systém budou aktualizované a funkční.
- **Zkontrolovat zabezpečení Wi-Fi**. Otevřete Poradce zabezpečení Wi-Fi a pro kontrolu, zda je domácí bezdrátová síť ke které jste připojeni bezpečná, nebo ne, a pokud má slabá místa.
- **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 Likvidátor souborů pro odstranění zbytků citlivých dat z vašeho počítače.
-

Pro zahájení ochrany přidaných zařízení s Bitdefender:

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

   Budete přesměrováni na webovou stránku účtu Bitdefender. Přihlaste se pomocí svých přihlašovacích údajů.

2. Klikněte na **ODESLAT ODKAZ KE STAŽENI** v okně, které se objeví.

3. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Zapamatujte si, 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.

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

- Bitdefender Antivirus Plus 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 dvě oddíly rozdělenými na užitečné moduly, které Vám pomohou být chráněni při práci, prohlížení webu, hraní her nebo provádění online plateb.

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

5.4.1. Ochrana

V sekci Ochrana můžete konfigurovat pokročilá bezpečnostní nastavení, nastavit funkce Bezpečné soubory a Prevence online hrozeb, zkontrolovat

a opravit případné zranitelnosti systému a posoudit zabezpečení bezdrátových sítí, 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
- Záchranný režim (Záchranné prostředí ve Windows 10)

Další informace o činnostech skenování a konfiguraci antivirové ochrany viz *„Antivirová ochrana“* (str. 71).

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. 93).

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. 91).

ZRANITELNOST

Modul Zranitelnosti vám pomůže udržet operační systém a aplikace, které pravidelně užíváte, aktuální a k identifikaci nezabezpečených bezdrátových sítí.

Kliknutím na **Sken zranitelností** v modulu Zranitelnosti spustíte kontrolu kritických aktualizací systému Windows, aktualizací aplikací, slabých hesel patřících k účtům systému Windows a nezabezpečených bezdrátových sítí.

Klikněte na **Wi-Fi poradce soukromí** k zobrazení seznamu bezdrátových sítí ke kterým se připojujete, kde najdete také naše posouzení reputace pro každou z nich a akce, které můžete uplatnit, aby jste zůstali v bezpečí před potenciálními slídilům.

Další informace o konfiguraci ochrany před zranitelnostmi viz *„Zranitelnosti“* (str. 96).

Bezpečné Soubory

Modul Bezpečné soubory zjišťuje zabezpečení pro Vaše osobní soubory proti útokům ransomwaru.

Další informace o konfiguraci Bezpečných souborů pro ochranu Vašich osobních souborů před ransomwarovými útoky naleznete v *„Bezpečné Soubory“* (str. 103).

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 *„Odstranění Ramsomware“* (str. 106).

5.4.2. Soukromí

V sekci Soukromí můžete otevřít aplikaci Bitdefender VNP, chránit své online transakce a zabezpečit procházení webu.

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. 116).

PENĚŽENKA

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. 109).

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. 119).

Ochrana dat

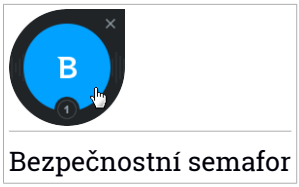
Modul Ochrana dat umožňuje trvalé odstranění souborů.
Kliknutím na **Likvidátor souborů** v modulu Ochrana dat spustíte průvodce, který umožňuje úplné odstranění souborů ze systému.

Další informace o konfiguraci modulu Ochrana dat viz *„Ochrana dat“* (str. 124).

5.5. Bezpečnostní semafor

Bezpečnostní semafor představuje rychlý a snadný způsob sledování a ovládání produktu Bitdefender Antivirus Plus. Po přidání této malé neobtěžující miniaplikace na plochu můžete kdykoli sledovat kritické informace a provádět klíčové činnosti:

- otevřete hlavní okno produktu Bitdefender.
- sledování činnosti skenování v reálném čase.
- sledování stavu zabezpečení vašeho systému a opravy případných problémů.
- sledování probíhající aktualizace.
- prohlížení oznámení a přístup k posledním událostem hlášeným produktem Bitdefender.
- skenování souborů nebo složek přetažením jedné nebo více položek na miniaplikaci.



Celkový stav zabezpečení vašeho počítače se zobrazuje **uprostřed** miniaplikace. Stav je indikován barvou a tvarem ikony zobrazené v této oblasti.

Zabezpečení vašeho systému ovlivňují kritické problémy.

Vyžadují vaši okamžitou pozornost a je třeba je odstranit co nejdřívě. Kliknutím na stavovou ikonu zahájíte opravu hlášených problémů.

Zabezpečení vašeho systému ovlivňují nekritické probémy. Až budete mít čas, měli byste je zkontrolovat a odstranit. Kliknutím na stavovou ikonu zahájíte opravu hlášených problémů.

Váš systém je chráněný.

Když probíhá úloha skenování na požádání, zobrazuje se tato animovaná ikona.

V případě hlášení problémů spustíte kliknutím na stavovou ikonu průvodce opravou problémů.

V **dolní části** miniaplikace se zobrazuje počítadlo nepřečtených událostí (počet nevyřízených událostí hlášených produktem Bitdefender, pokud nějaké nastaly). Kliknutím na počítadlo událostí, např. na 1 v případě jedné nepřečtené události, a otevře se okno Události. Další informace viz *„Upozornění“* (str. 15).

5.5.1. Skenování souborů a složek

Bezpečnostní semafor lze použít k rychlému skenování souborů a složek. Přetáhněte jakýkoli soubor nebo složku, které chcete skenovat, na **bezpečnostní semafor**.

Zobrazí se průvodce antivirovým skenem, který vás provede průběhem skenování. Možnosti skenování jsou předkonfigurovány pro nejlepší výsledky

detekce a nelze je měnit. V případě nalezení infikovaných souborů se produkt Bitdefender pokusí o jejich vyléčení (odstranění škodlivého kódu). Pokud se léčení nezdaří, průvodce antivirovým skenem vám umožní určit jiné činnosti, které se mají s infikovanými soubory provádět.

5.5.2. Skrýt/Zobrazit bezpečnostní semafor

Pokud již nechcete miniaplikaci zobrazit, klikněte na ⊗.

Bezpečnostní semafor obnovíte jedním z následujících způsobů:

- Z oznamovací oblasti:
  1. Klikněte pravým tlačítkem na ikonu Bitdefender v oznamovací oblasti.
  2. V zobrazené kontextové nabídce klikněte na položku **Zobrazit bezpečnostní semafor**.
- Z rozhraní produktu Bitdefender:
  1. Klikněte na **Nastavení** v navigačním menu v rozhraní Bitdefender.
  2. V okně **Obecné** zapněte **Bezpečnostní semafor**.

Widget Zabezpečení Bitdefender je deaktivovaný ve výchozím nastavení.

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. Můžete se přihlásit k vašemu Bitdefender účtu z kteréhokoliv připojeného k internetu přechodem na 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 Antivirus Plus
  - Antivirový program Bitdefender pro počítače Macintosh
  - Bitdefender Mobile Security pro Android
  - Bitdefender zabezpečení mobilních zařízení s operačním systémem iOS
- Spravovat a obnovovat předplatná produktu Bitdefender.
- Přidávat nová zařízení do vaší sítě a odkudkoli je spravovat.

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.

- Ze 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. Moje předplatná

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

6.2.1. 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).

6.2.2. Přidání nového zařízení

Pokud se vaše předplatné vztahuje k více než jednomu zařízení, můžete přidat nové zařízení a nainstalovat na ně produkt Bitdefender Antivirus Plus 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 uložte instalační soubor.

- **Chránit další zařízení**

  Vyberte tuto možnost a poté klikněte na **ODESLAT ODKAZ KE STAŽENÍ**. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Zapamatujte si, 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.

6.2.3. Obnovení předplatného

Pokud jste nezvolili automatické obnovení předplatného produktu 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.

6.2.4. 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.

6.3. 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 *„Provedení kompletního skenu“* (str. 77) a *„Provedení rychlého skenu“* (str. 77).
- **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. 96).

6.4. Můj účet

V části **Můj účet** můžete upravovat svůj profil, změnit heslo ke svému účtu, spravovat přihlašovací relace a Bitdefender Central pomocné zprávy.

Když kliknete na ikonu v pravé horní části obrazovky a zvolíte **Můj účet**, uvidíte následující karty:

- **Profil** - zde můžete přidávat a upravovat uživatelské údaje.
- **Změnit heslo** - zde můžete změnit heslo připojené k Vašemu účtu.
- **Řízení relací** - zde můžete sledovat a řídit nejnovější aktivní i neaktivní přihlašovací relace probíhající na zařízeních připojených k Vašemu účtu.
- **Nastavení** - zde můžete Zapnout/Vypnout Bitdefender Central pomocné zprávy a rozhodnout se, zda chcete být informováni v případě pořizovaní fotografií pomocí vašich zařízení Android.

6.5. 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 stavu se aktualizace kontrolují, když zapnete počítač, a poté každou **hodinu**. V případě, ze je aktualizace nalezena, automaticky se stáhne a nainstaluje do počítače.

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 váš počítač připojuje k Internetu pomocí proxy serveru, je třeba nakonfigurovat nastavení proxy dle popisu v části *„Jak nakonfigurovat produkt Bitdefender, aby používal připojení k Internetu pomocí proxy?“* (str. 64).
- Pokud jste k Internetu připojeni pomocí vytáčeného připojení, doporučujeme pravidelně aktualizovat produkt Bitdefender na žádost uživatele. Další informace viz *„Provedení aktualizace“* (str. 37).

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 nezbytné restartovat počítač. 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, trvale 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.

Ve výchozím stavu platí, že pokud aktualizace vyžaduje restart, produkt Bitdefender bude nadále pracovat se starými soubory, dokud uživatel z vlastní vůle nerestartuje počítač. 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 2018.

DOPORUČENÉ POSTUPY

8. INSTALACE

8.1. Jak nainstaluji produkt Bitdefender na druhý počítač?

Pokud vámi zakoupené předplatné zahrnuje více než jeden počítač, můžete využít Bitdefender účet a aktivovat druhý počítač.

Pro instalaci Bitdefender na druhý počítač:

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

   Budete přesměrováni na webovou stránku účtu Bitdefender. Přihlaste se pomocí svých přihlašovacích údajů.

2. Klikněte na **ODESLAT ODKAZ KE STAŽENI** v okně, které se objeví.

3. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Zapamatujte si, 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.

4. Spusťte produkt Bitdefender, který jste stáhli.

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 Antivirus Plus** a vyberte možnost **Odinstalovat**.
3. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
4. Pro dokončení procesu bude třeba restartovat počítač.

- 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 Antivirus Plus** a vyberte možnost **Odinstalovat**.
  4. V okně, které se zobrazí, klikněte na **PŘEINSTALOVAT**.
  5. Pro dokončení procesu bude třeba restartovat počítač.
- 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 Antivirus Plus** a vyberte možnost **Odinstalovat**.
  4. Opětovným kliknutím na tlačítko **Odinstalovat** potvrďte váš výběr.
  5. Klikněte na **PŘEINSTALOVAT**.
  6. Pro dokončení procesu bude třeba restartovat počítač.

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?

Produkt Bitdefender lze nainstalovat z instalačního disku nebo pomocí webového instalačního programu, který můžete stáhnout do počítače z platformy Bitdefender Central.

Poznámka
Než sadu spustíte, doporučujeme odebrat případné antivirové řešení nainstalované ve vašem počítači. Pokud na jednom počítači používáte více než jedno řešení zabezpečení, systém se může stát 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 uložte instalační soubor.
   - **Chránit další zařízení**

     Vyberte tuto možnost a poté klikněte na **ODESLAT ODKAZ KE STAŽENÍ**. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Zapamatujte si, 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?

Pokud chcete používat Bitdefender v jiném jazyce, musíte přeinstalovat produkt se správným jazykem.

Chcete-li použít Bitdefender v jiném jazyce:

1. Pomocí následujícího postupu odeberte produkt 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 Antivirus Plus** a vyberte možnost **Odinstalovat**.

c. V okně, které se zobrazí, klikněte na **ODSTRANIT**.

d. 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. Vyhledejte položku **Bitdefender Antivirus Plus** a vyberte možnost **Odinstalovat**.

d. V okně, které se zobrazí, klikněte na **ODSTRANIT**.

e. 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. Vyhledejte položku **Bitdefender Antivirus Plus** 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.

2. Změnit jazyk Bitdefender Central:

a. Přihlaš se na Bitdefender Central.

b. Klikněte na ikonu v pravém horním rohu obrazovky.

c. Klikněte na **Můj účet** v rolovacím menu.

d. Vyberte kartu **Profil**.

e. Vyberte jazyk z rozevíracího seznamu **Jazyk** a poté klikněte na **ULOŽIT**.

3. Stažení instalačního souboru:

a. Vyberte menu **Moje Zařízení** a klikněte na **INSTALOVAT OCHRANU**.

b. Prosím vyberte jednu z následujících variant

- **Chránit toto zařízení**

Vyberte tuto možnost a uložte instalační soubor.

- **Chránit další zařízení**

  Vyberte tuto možnost a poté klikněte na **ODESLAT ODKAZ KE STAŽENÍ**. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Zapamatujte si, 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.

4. Spusťte produkt Bitdefender, který jste stáhli.

Poznámka
Tento přeinstalační proces trvale vymaže Vaše osobní nastavení.

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 Antivirus Plus** 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 Antivirus Plus** 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 **Nainstalované aplikace**.
3. Vyhledejte položku **Bitdefender Antivirus Plus** 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 uložte instalační soubor.
        - **Chránit další zařízení**

          Vyberte tuto možnost a poté klikněte na **ODESLAT ODKAZ KE STAŽENÍ**. Zadejte emailovou adresu do příslušného pole a klikněte na tlačítko **ODESLAT EMAIL**. Zapamatujte si, 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 2018, 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 na restartování počítače.

   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. PŘEDPLATNÁ

9.1. Jak aktivuji předplatné produktu Bitdefender pomocí licenčního klíče?

Pokud máte platný licenční klíč a chcete ho použít k aktivaci předplatného pro produkt Bitdefender Antivirus Plus, jsou možné dva případy:

- Upgradovali jste z předchozí verze produktu Bitdefender na novou:
  1. Jakmile je upgrade na Bitdefender Antivirus Plus dokončen, budete vyzváni k přihlášení k vašemu účtu Bitdefender.
  2. Klikněte na **Přihlásit se**, a pak napište svojí emailovou adresu a heslo Vašeho Bitdefender účtu.
  3. Pro pokračování klikněte na **Přihlásit se**.
  4. Na obrazovce vašeho účtu se objeví oznámení, které vás informuje, že bylo vytvořeno předplatné. Vytvořené předplatné bude platné po zbývající dobu platnosti vašeho licenčního klíče a pro stejný počet uživatelů.

     Na zařízeních, která používají předchozí verze produktu Bitdefender a jsou zaregistrovaná pomocí licenčního klíče, který jste převedli na předplatné, je třeba aktivovat produkt pomocí téhož účtu Bitdefender.
- Produkt Bitdefender nebyl na systému předtím nainstalován:
  1. Jakmile je proces instalace dokončen, budete vyzváni k přihlášení k vašemu účtu Bitdefender.
  2. Klikněte na **Přihlásit se**, a pak napište svojí emailovou adresu a heslo Vašeho Bitdefender účtu.
  3. Pro pokračování klikněte na **PŘIHLÁSIT** a poté na **DOKONČIT** k získání přístupu do rozhraní Bitdefender Antivirus Plus.
  4. Klikněte na **Můj účet** v navigačním menu v rozhraní Bitdefender.
  5. Klikněte na **Aktivovat nyní**.

     Objeví se nové okno.
  6. Klikněte na **Získat upgrade zdarma nyní!**.

7. Vepište váš licenční klíč do správného pole a klikněte na **UPGRADOVAT MŮJ PRODUKT**, K účtu bude přidruženo předplatné se stejnou dostupností a počtem uživatelů jako váš licenční klíč.

10. BITDEFENDER CENTRAL

10.1. Jak se mohu přihlásit k účtu Bitdefender Central pomocí jiného online účtu?

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

Chcete-li úspěšně použít jiný účet:

1. Klikněte na **Můj účet** v navigačním menu v rozhraní Bitdefender.
2. Klikněte na **Přepnout Účet** ve vrchním pravém rohu obrazovky, pro změnu účtu připojeného k počítači.
3. Zadejte emailovou adresu a heslo účtu do příslušných polí 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 *„Požádání o pomoc“* (str. 160).

10.2. 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. Vyberte kartu **Nastavení**.
5. Vypnout možnost **Zapnout/Vypnout pomocné zprávy**.

10.3. 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. Klikněte **Zapomenuté heslo**.
  4. Zadejte emailovou adresu použitou k vytvoření vašeho účtu Bitdefender ,a poté klikněte na tlačítko **ZAPOMENUTÉ HESLO**.
  5. Zkontrolujte váš email a klikněte na příslušné tlačítko.

     Otevře se okno RESETOVAT HESLO Bitdefender.
  6. Do příslušného pole zadejte svou emailovou adresu a nové heslo. Heslo musí mít délku alespoň 8 znaků a obsahovat číslice.
  7. Klikněte na tlačítko **RESETOVAT HESLO**.
- Z webového prohlížeče:
  1. Přejděte na adresu: https://central.bitdefender.com.
  2. Klikněte **Zapomenuté heslo**.
  3. Zadejte svou e-mailovou adresu a klikněte na tlačítko **ZAPOMENUTÉ HESLO**.
  4. 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.

10.4. 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 **Můj účet** v rolovacím menu.
4. Vyberte kartu **Řízení relací**.
5. V oblasti **Aktivní relace** zvolte možnost **ODHLÁSIT SE** vedle zařízení, na kterém chcete ukončit přihlašovací relaci.

11. SKENOVÁNÍ POMOCÍ PRODUKTU BITDEFENDER

11.1. 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.
- Skenujete sdílenou síťovou složku před zkopírováním souborů do vašeho počítače.

11.2. Jak mám provést sken systému?

Chcete-li provést úplnou kontrolu systému:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na **Sken Systému**.
3. 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. 81).

11.3. Jak mám naplánovat sken?

Produkt Bitdefender můžete nastavit tak, aby spouštěl skenování důležitých oblastí systému, když nejste u počítače.

Chcete-li naplánovat kontrolu:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na **Spravovat skeny**.
3. Vyberte druh skenu, který chcete naplánovat - Kompletní sken systému nebo Rychlý sken - a poté klikněte na položku **MOŽNOSTI SKENOVÁNÍ**.

   Alternativně můžete vytvořit nový druh skenu vyhovující vašim potřebám kliknutím na položku **NOVÝ VLASTNÍ SKEN**.
4. Zapněte možnost **Naplánování**.

   Vyberte jednu z odpovídajících možností a nastavte plán:

   - Při spouštění systému
   - Jednou
   - Opakovaně

V okně **Skenované objekty** můžete zvolit umístění, která mají být skenována. Tato možnost je dostupná pouze, když se rozhodnete provést nový vlastní sken.

11.4. Jak mám vytvořit vlastní sken?

Pokud chcete skenovat konkrétní umístění na vašem počítači nebo konfigurovat možnosti skenování, nakonfigurujte a spusťte vlastní sken.

Vlastní sken nakonfigurujte následujícím způsobem:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na **Spravovat skeny**.
3. Klikněte na položku **NOVÝ VLASTNÍ SKEN**. v okně **Obecné** zadejte název skenu a vyberte skenovaná umístění.
4. Pokud chcete konfigurovat podrobné možnosti skenování, vyberte kartu **Pokročilé**.

Nastavením úrovně skenu můžete snadno konfigurovat možnosti skenování. Přetažením posuvníku nastavte požadovanou úroveň skenování.

Můžete rovněž zvolit vypnutí počítače po dokončení skenu, pokud nebyly nalezeny žádné hrozby. Pamatujte, že půjde o výchozí chování při každém spuštění tohoto skenu.

5. Kliknutím na tlačítko **OK** uložte změny a zavřete okno.
6. Pokud chcete pro sken nastavit plán, použijte příslušný přepínač.
7. Klikněte na položku **SPUSTIT SKEN** a s použitím průvodce skenem dokončete sken. Na konci skenu budete vyzváni k výběru činností, které budou provedeny s případnými nalezenými soubory.
8. Pokud chcete, můžete rychle znovu spustit předchozí vlastní sken kliknutím na příslušnou položku v dostupném seznamu.

11.5. 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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
3. Klikněte na kartu **Výjimky**.
4. V nabídce klikněte na **Seznam souborů a složek vyloučených ze skenování** a poté na **Přidat**.
5. Klikněte na **Prohlížet**, zvolte složku, kterou chcete vyloučit ze skenování, a poté vyberte typ skenování, ze kterého chcete složku vyloučit.

6. Klikněte na **PŘIDAT** pro uložení změn a zavření okna.

11.6. 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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
   c. V okně **Štít** 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. 66).
3. Obnovení souboru z oblasti Karanténa:
   a. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
   b. V okně **ANTIVIRUS** klikněte na položku **Karantény**.
   c. Vyberte soubor a poté klikněte na tlačítko **Obnovit**.
4. Přidejte soubor do seznamu výjimek. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak mohu vyloučit složku ze skenování?“* (str. 56).
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 *„Požádání o pomoc“* (str. 160).

11.7. 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**.

12. KONTROLA SOUKROMÍ

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 **Otevřít Safepay**.
3. 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.

Likvidátor souborů produktu Bitdefender vám pomůže rychle vymazat soubory ze složek ve vašem počítači pomocí kontextové nabídky systému Windows prostřednictvím následujícího postupu:

1. Pravým tlačítkem klikněte na soubor nebo složku, které chcete trvale odstranit, vyberte položku Bitdefender a zvolte možnost **Likvidátor souborů**.
2. Klikněte na **SMAZAT NAVŽDY** a poté 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 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.

   Klikněte na **OBNOVIT SOUBORŮ** pro pokračování.
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 místo na vašem počítači.
5. Zobrazí se potvrzovací okno.

   Klikněte na **DOKONČIT** pro dokončení procesu obnovení.

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 *„Požádání o pomoc“* (str. 160).

13.2. Jak odeberu produkt Bitdefender?

Pokud chcete odstranit váš Bitdefender Antivirus Plus:

- 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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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?

Proces odstranění Bitdefender VPN je podobný těm, které provádíte při odstraňování jiných programů z vašeho počítače:

- 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 automaticky vypnout počítač po dokončení skenu?

Produkt Bitdefender nabízí více skenů, které můžete použít, abyste zajistili, že váš systém nebude infikovaný hrozbami. V závislosti na hardwarové a softwarové konfiguraci může skenování celého počítače trvat dlouho.

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

Představte si následující situaci: dokončili jste práci na počítači a chcete jít spát. Rádi byste nechali produktem Bitdefender zkontrolovat systém na přítomnost hrozeb.

Pokud chcete nastavit produkt Bitdefender tak, aby na konci skenu vypnul systém, použijte následující postup:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na **Spravovat skeny**.
3. V okně **Správce skenovacích úloh** klikněte na položku **NOVÝ VLASTNÍ SKEN**, zadejte název skenu a vyberte skenovaná umístění.

4. Pokud chcete konfigurovat podrobné možnosti skenování, vyberte kartu **Pokročilé**.
5. Zvolte vypnutí počítače po dokončení skenu, pokud nebyly nalezeny žádné hrozby.
6. Kliknutím na tlačítko **OK** uložte změny a zavřete okno.
7. Kliknutím na tlačítko **SPUSTIT SKEN** spusťte sken systému.

Pokud nejsou nalezeny žádné hrozby, počítač se vypne.

Pokud zbývají nějaké nevyřešené hrozby, budete vyzváni k výběru činností, které s nimi budou provedeny. Další informace viz *„Průvodce antivirovým skenem“* (str. 81).

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

Pokud se váš počítač připojuje k Internetu pomocí proxy serveru, musíte nakonfigurovat nastavení proxy v produktu Bitdefender. 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.

13.6. 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 oblasti Systém získáte informace o druhu systému.
- V systému **Windows 10**:

1. Do vyhledávacího pole na hlavním panelu zadejte „Systém“ a klikněte na příslušnou ikonu.
2. V oblasti Systém vyhledejte informace o druhu systému počítače.

13.7. 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**.

13.8. 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 jednom počítači používáte více než jedno řešení zabezpečení, systém se může stát nestabilním. Instalační program produktu Bitdefender Antivirus Plus 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 **Nainstalované 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.

13.9. 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 počítač.
  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

Produkt Bitdefender chrání váš počítač před všemi druhy hrozeb (malwarem, trojskými koni, spywarem, 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
  Abyste zabránili infikování počítače, nechte **skenování při přístupu** zapnuté.

- 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.

Produkt Bitdefender automaticky skenuje všechna vyjímatelná média, která jsou připojena k počítači, aby se ujistil, že je přístup k nim bezpečný. Další informace viz *„Automatický sken vyjímatelných médií“* (str. 85).

Pokročilí uživatelé mohou nakonfigurovat výjimky ze skenování, pokud nechtějí skenovat konkrétní soubory nebo typy souborů. Další informace viz *„Konfigurace výjimek skenování“* (str. 87).

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. 89).

Pokud byl váš počítač infikován hrozbami, čtěte část *„Odstranění hrozeb z vašeho systému“* (str. 149). Abyste počítač zbavili hrozeb, které nelze odstranit zevnitř operačního systému Windows, nabízí vám produkt Bitdefender*„Bitdefender Záchranný režim (Záchranné prostředí ve Windows 10)“* (str. 149). Jedná se o důvěryhodné prostředí, speciálně navržené pro odstraňování hrozeb, které umožňuje spustit počítač nezávisle na systému

Windows. Pokud počítač běží v Rescue Modu (Záchranné prostředí ve Windows 10), Windows hrozby jsou neaktivní, takže je snadné je odstranit.

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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
3. V okně **Štít** 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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
3. V okně **Štít** klikněte na nabídku **Zobrazit pokročilá nastavení**.

Zobrazí se okno tabulky.

4. Posouvejte se tabulkou dolů pro možnost konfigurace skenování tak, jak potřebujete.

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).
- **Skenovat síťové složky.** Abyste mohli ze svého počítače bezpečně přistupovat ke vzdálené síti, doporučujeme ponechat zapnutou možnost Skenování síťových složek.
- **Skenovat uvnitř archivů.** 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.

  Rozhodnete-li se využít této možnosti, zapněte ji a poté přetáhněte posuvník po stupnici pro nastavení maximální možné velikosti (v MB) archivů, které mají být skenovány při přístupu.
- **Skenovat emaily.** Bitdefender automaticky skenuje příchozí a odchozí emaily, aby zabránil stažení hrozeb na Váš počítač.

  Přestože to nedoporučujeme, můžete vypnout antivirové skenování emailů pro zvýšení výkonu systému. Pokud příslušné možnosti skenování vypnete, emaily a přijaté soubory nebudou skenovány, což umožní uložení infikovaných souborů do Vašeho počítače. Nejde o zásadní hrozbu, protože

ochrana v reálném čase hrozbu zablokuje, když dojde k přístupu k infikovaným souborům (jejich otevření, přesunutí, zkopírování nebo spuštění).

- **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.
- **Hledat keyloggery.** 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.
- **Skenování při startu systému.** 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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
3. V okně **Štít** klikněte na nabídku **Zobrazit pokročilá nastavení**.

   Zobrazí se okno tabulky.
4. Posouvejte okno dolů, až uvidíte volbu **Reakce na hrozby**.
5. 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. 89).

  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 soubory 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. 89).

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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
3. V okně **Štít** klikněte na nabídku **Zobrazit pokročilá nastavení**.

   Zobrazí se okno tabulky.
4. Skrolujte dolů, až uvidíte volbu **Obnovit nastavení**. Vyberte tuto možnost pro obnovení antivirových nastavení do výchozího stavu.

14.2. Manuální skenování

Hlavním účelem produktu Bitdefender je zajistit, aby se ve vašem počítači nenacházely žádné hrozby. To provádí zadržováním nových virů mimo vás počítač a skenováním vašich emailových zpráv a nových souborů stažených nebo zkopírovaných do vašeho systému.

Existuje riziko, že v systému je usazený virus už předtím, než vůbec nainstalujete produkt Bitdefender. Proto je velmi vhodné po instalaci produktu Bitdefender oskenovat, zda se v počítači nenacházejí rezidentní viry. Rovněž doporučujeme, abyste skenování vašeho počítače prováděli často.

Manuální skenování je založeno na skenovacích úlohách. Skenovací úlohy specifikují možnosti skenování a skenované objekty. Počítač můžete skenovat, kdykoli chcete, provedením výchozích nebo vlastních (uživatelem definovaných) skenů. Pokud chcete skenovat konkrétní umístění na vašem počítači nebo konfigurovat možnosti skenování, nakonfigurujte a spusťte vlastní sken.

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 okně **ANTIVIRUS** klikněte na položku **Rychlý sken**.
3. 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

Kompletní sken otestuje celý počítač na přítomnost malwaru ohrožujícího jeho bezpečnost, jako malware, spyware, adware, rootkity a další.

Poznámka

Protože **kompletní sken** provádí důkladné skenování celého systému, může chvíli trvat. Proto doporučujeme tento sken provádět, když počítač nepoužíváte.

Před spuštěním kompletního skenu doporučujeme provést následující:

- Ujistěte se, že je Bitdefender aktuální současně se svou informační databází o hrozbách. Skenování počítače pomocí neaktuální databáze s informacemi o hrozbách může způsobit, že Bitdefender nerozpozná nové hrozby nalezené od poslední aktualizace. Další informace viz *„Aktualizace produktu Bitdefender“* (str. 36).
- Ukončete všechny spuštěné programy.

Pokud chcete skenovat konkrétní umístění na vašem počítači nebo konfigurovat možnosti skenování, nakonfigurujte a spusťte vlastní sken. Další informace viz *„Konfigurace vlastního skenu“* (str. 78).

Chcete-li spustit Systémový sken:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na **Sken Systému**.
3. Poprvé, když spustíte sken systému, je vám představena tato funkce. Klikněte na **OK, chápu** pro pokračování.
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.

14.2.4. Konfigurace vlastního skenu

Chcete-li konfigurovat detaily vlastního skenu a poté ho spustit:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na **Spravovat skeny**.
3. Klikněte na položku **NOVÝ VLASTNÍ SKEN**. v okně **Obecné** zadejte název skenu a vyberte skenovaná umístění.
4. Pokud chcete konfigurovat podrobné možnosti skenování, vyberte kartu **Pokročilé**. Objeví se nové okno. Postupujte následovně:

   a. Nastavením úrovně skenu můžete snadno konfigurovat možnosti skenování. Přetažením posuvníku nastavte požadovanou úroveň skenování. Pomocí popisu na pravé straně stupnice určete úroveň skenu, která lépe splňuje vaše potřeby.

   Pokročilí uživatelé mohou využít výhody nastavení skenování, kterou produkt Bitdefender nabízí. Chcete-li nakonfigurovat podrobné možnosti skenu, klikněte na tlačítko **Vlastní**. Informace o nich najdete na konci této části.

   b. Můžete také nakonfigurovat následující obecné možnosti:

   - **Spustit sken s nízkou prioritou .** Sníží prioritu skenovacího procesu. Ostatní programy budou moci pracovat rychleji, prodlouží se však doba skenovacího procesu.
   - **Minimalizovat průvodce skenem do oznamovací oblasti .** Minimalizuje okno skenu do oznamovací oblasti. Okno otevřete dvojím kliknutím na ikonu Bitdefender.
   - Specifikujte akci, která se provede, když nebudou nalezeny žádné hrozby.

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

5. Pokud chcete nastavit pro vaši skenovací úlohu časový plán, použijte **Plánovat** v okně **Základní**. Vyberte jednu z odpovídajících možností a nastavte plán:
   - Při spouštění systému
   - Jednou
   - Opakovaně
6. Klikněte na položku **SPUSTIT SKEN** a s použitím Průvodce antivirovým skenem dokončete sken. V závislosti na skenovaných oblastech může sken chvíli trvat. Na konci skenu budete vyzváni k výběru činností, které budou provedeny s případnými nalezenými soubory.
7. Pokud chcete, můžete rychle znovu spustit předchozí vlastní sken kliknutím na příslušnou položku v dostupném seznamu.

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 soubory.** Produkt Bitdefender můžete nastavit tak, aby skenoval všechny typy souborů, nebo pouze aplikace (programové soubory). Skenování všech souborů poskytuje nejlepší ochranu, zatímco skenování aplikací lze použít k provedení rychlejšího skenu.

  Aplikace (neboli programové soubory) jsou daleko zranitelnější ohrožujícími útoky než ostatní druhy souborů. Tato kategorie zahrnuje následující přípony souborů: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs;

vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Možnosti skenování archivů.** 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.

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

- **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 zvolte pro skenování souborů cookie, které do vašeho počítače ukládají prohlížeče.
- **Skenovat pouze nové a změněné soubory.** Skenováním pouze nových a změněných souborů výrazně zlepšíte celkovou reakci systému s minimálními ústupky v oblasti zabezpečení.
- **Ignorovat komerční keyloggery.** Tuto možnost zvolte, pokud jste na počítač nainstalovali a používáte komerční keylogger. Komerční keyloggery představují legitimní počítačový software, jehož nejzákladnější funkcí je zaznamenávat vše, co píšete na klávesnici.
- **Hledat rootkity.** Tuto možnost zvolte pro skenování rootkitů a objektů skrytých pomocí tohoto softwaru.

- **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).

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 skenování tohoto objektu.** 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. 89).

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. Protokol je vystaven ve formátu .xml a je možné jej lokálně uložit kliknutím na tlačítko **Uložit protokol** a následným zvolením místa uložení.

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. 149).

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 zaznamená připojení vyjímatelného paměťového zařízení k Vašemu počítači a, je-li možnost Autoscan povolena, na pozadí jej skenuje. To je doporučeno pro zabránění hrozbám infikovat váš počítač.

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. 149).

14.3.2. Správa skenů vyjímatelných médií

Chcete-li automaticky skenovat vyměnitelná média:

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

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na položku **Nastavení**.
3. Vyberte kartu **Jednotky a zařízení**.

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.

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 systémové a kontextové skenování. Skenování systému je sken na vyžádání, který umožňuje analýzu celého systému proti škodlivým hrozbám, které by mohly ohrozit bezpečí Vašich dat. 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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
3. Vyberte kartu **Výjimky**.
4. V nabídce klikněte na **Seznam souborů a složek vyloučených ze skenování**. V zobrazeném okně můžete spravovat soubory a složky vyloučené ze skenování.
5. Přidejte výjimky podle těchto kroků:
   a. Klikněte na tlačítko **Přidat**.

b. Klikněte na tlačítko **PROCHÁZET**, vyberte soubor nebo složku, které chcete vyloučit ze skenování, a poté klikněte na tlačítko **PŘIDAT**. Alternativně můžete zadat (nebo zkopírovat a vložit) cestu k souboru či složce do editačního pole.

c. Ve výchozím stavu budou vybraný soubor nebo složka vyloučeny jak ze skenování při přístupu, tak z manuálního skenování. Pokud chcete změnit, kdy se výjimka použije, vyberte jednu z ostatních možností.

d. Klikněte na tlačítko **Přidat**.

14.5.2. Vyloučení přípon souborů ze skenování

Když vyloučíte příponu souboru ze skenování, produkt Bitdefender již nebude skenovat soubory s příslušnou příponou, bez ohledu na jejich umístění v počítači. Vyloučení se vztahuje i na soubory na vyjímatelných médiích, jako disky CD, DVD, paměťová zařízení USB nebo síťové jednotky.

Důležité
Vyloučení přípon souborů ze skenování používejte opatrně, protože takové výjimky mohou váš počítač učinit zranitelnějším.

Chcete-li vyloučit přípony souborů ze skenování:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na položku **Nastavení**.
3. Vyberte kartu **Výjimky**.
4. Klikněte na nabídku **Seznam souborů a složek vyloučených ze skenování**. V zobrazeném okně můžete spravovat přípony souborů vyloučené ze skenování.
5. Přidejte výjimky podle těchto kroků:

   a. Klikněte na tlačítko **Přidat**.

   b. Zadejte přípony, které chcete vyloučit ze skenování, a oddělte je středníky (;). Zde je příklad:

   txt;avi;jpg

   c. Ve výchozím stavu jsou všechny soubory se specifikovanými příponami vyloučeny ze skenování při přístupu i manuálního skenování. Pokud chcete změnit, kdy se výjimka použije, vyberte jednu z ostatních možností.

d. Klikněte na **PŘIDAT**.

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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
3. Vyberte kartu **Výjimky**.
4. Pro spravování výjimek ze skenování použijte možnosti v nabídce **Seznam souborů a složek vyloučených ze skenování**.
5. Chcete-li odebrat nebo upravovat výjimky skenování, klikněte na jeden z dostupných odkazů. Pokračujte následovně:
   - Pro odebrání položky ze seznamu ji vyberte a klikněte na tlačítko **Odstranit** .
   - Pokud chcete nějakou položku v tabulce upravit, dvakrát na ni klikněte (nebo ji vyberte a klikněte na tlačítko **Upravit**). Zobrazí se nové okno, ve kterém můžete změnit příponu nebo cestu, které budou vyloučeny, a dle potřeby zadat druh skenování, ze kterého mají být vyloučeny. 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 okně **ANTIVIRUS** klikněte na položku **Karantény**.

   Zde můžete zobrazit název souborů v karanténě, jejich původní umístění a název zjištěných hrozeb.
3. 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:

   Znovu oskenujte karanténu po aktualizaci informací o hrozbách
   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.
4. 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 neustále sleduje aplikace běžící na počítači a hledá akce s podezřelým chováním. 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 okně **POKROČILÁ OCHRANA PŘED HROZBAMI** zapněte nebo vypněte přepínač.

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

Vždy když je hrozba nebo potenciálně škodlivý proces detekován, Bitdefender jej zablokuje, aby předešel infekci vašeho počítače 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 okně **POKROČILÁ OCHRANA PŘED HROZBAMI** klikněte na **Ochrana před hrozbami**.
3. Při prvním přístupu k aplikaci Ransomware Protection jste uvedeni do funkce. Klikněte na **OK, chápu** pro pokračování.

   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 okně **POKROČILÁ OCHRANA PŘED HROZBAMI** klikněte na **Nastavení**.
3. V okně **Výjimky**, klikněte na **Přidat aplikace do výjimek**.
4. Najděte a vyberte aplikaci, kterou chcete vynechat, a poté klikněte na **OK**.

   Pro odebrání položky ze seznamu klikněte na možnost **Odstranit**, které se nachází vedle položky.

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 okně **Ochrana webu** klikněte na přepínače pro zapnutí nebo vypnutí:

- 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 proti podvodům.

- Ochrana před phishingem.

V okně **Prevence síťových hrozeb**, máte možnost **Prevence síťových hrozeb**. Abyste udrželi váš počítač v bezpečí před útoky komplexního malwaru (jako je ransomware) skrze zneužití zranitelností, ponechte tuto možnost zapnutou.

Můžete vytvořit seznam webových stránek, které nebudou skenovány antivirovými, antiphishingovými a antifraudovými jádry produktu Bitdefender. Seznam by měl obsahovat pouze webové stránky, kterým plně důvěřujete. Přidejte například webové stránky, na kterých nakupujete online.

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

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **PREVENCE ONLINE HROZEB** klikněte na **Výjimky**.
3. Do příslušného pole zadejte jméno stránky, kterou chcete přidat na whitelist, a poté klikněte na **PŘIDAT**.

   Pokud chcete webovou stránku ze seznamu odebrat, vyberte ji ze seznamu a klikněte na příslušný odkaz **Odstranit**.

   Klikněte na **ULOŽIT** k uložení změn a zavření okna.

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 odkaz **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 je stránka bezpečná, klikněte na **Odeslat** pro přidání stránky na whitelist. Doporučujeme přidávat pouze stránky, kterým plně důvěřujete.

17. ZRANITELNOSTI

Důležitou součástí ochrany vašeho počítače před podezřelými osobami a aplikacemi je aktualizovat operační systém a pravidelně používané aplikace na nejnovější verzi. Kromě toho, aby se zabránilo neoprávněnému fyzickému přístupu k počítači, musí být nakonfigurováno silné heslo (hesla, které nelze snadno uhodnout) pro každý uživatelský účet systému Windows a pro připojení do sítě Wi-Fi.

Produkt Bitdefender automaticky kontroluje zranitelnosti systému a upozorňuje vás na ně. Skenuje následující:

- Neaktuální aplikace ve vašem počítači.
- chybějící aktualizace systému Windows.
- slabá hesla uživatelských účtů systému Windows.
- nezabezpečené bezdrátové sítě a routery.

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.

17.1. Skenování zranitelností systému

Chcete-li opravit zranitelnosti pomocí funkce Sken zranitelností:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V modulu **ZRANITELNOST** vyberte **Sken zranitelností**.
3. Počkejte, než produkt Bitdefender zkontroluje zranitelnosti systému. Chcete-li průběh skenu zastavit, klikněte na tlačítko **Přeskočit** v horní části okna.

   - **Důležité aktualizace systému Windows**

Kliknutím na položku **Podrobnosti** zobrazíte seznam důležitých aktualizací systému Windows, které v současnosti nejsou ve vašem počítači nainstalovány.

Chcete-li spustit instalaci vybraných aktualizací, klikněte na položku **Instalovat aktualizace**. Instalace aktualizací může chvíli trvat a některé z nich mohou pro dokončení instalace vyžadovat restart systému. V případě potřeby restartujte systém, jakmile to bude možné.

- **Aktualizace aplikací**

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

  Kliknutím na položku **Podrobnosti** zobrazíte informace o aplikaci, kterou je třeba aktualizovat.

- **Slabá hesla k účtům systému Windows**

  Můžete se podívat na seznam uživatelských účtů systému Windows nakonfigurovaných na vašem počítači a úroveň ochrany, kterou poskytují jejich hesla.

  Pokud chcete pro systém nastavit nové heslo, klikněte na položku **Změnit heslo při přihlašování**.

  Klikněte na položku **Podrobnosti** a změňte slabá hesla. Můžete zvolit, zda má být uživatel vyzván ke změně hesla při příštím přihlášení, nebo zda chcete heslo ihned změnit sami. Silné heslo vytvoříte použitím kombinace malých a velkých písmen, číslic a speciálních symbolů (např. #, $ nebo @).

- **Sítě Wi-Fi**

  Klikněte na **Zobrazit Detaily** aby jste zjistili více o bezdrátové síti ke které jste připojen. Pokud je doporučeno nastavit silnější heslo pro vaši domácí síť, klikněte na odpovídající link.

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

V pravém horním rohu okna můžete filtrovat výsledky dle potřeby.

17.2. 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 okně **ZRANITELNOST** klikněte na **Nastavení**.

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

3. Vyberte zranitelnosti systému, které chcete pravidelně kontrolovat, pomocí příslušných přepínačů.

Aktualizace Windows

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.

Zabezpečení Wi-Fi

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.

17.3. 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
- Veřejné Wi-Fi sítě

17.3.1. 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 okně **ZRANITELNOST** klikněte na **Nastavení**.
3. V okně **Nastavení** vypněte volbu **Zabezpečení Wi-Fi**.

17.3.2. Konfigurace domácí Wi-Fi sítě

Chcete-li konfigurovat vaši domácí síť:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ZRANITELNOSTI** klikněte na **Zabezpečení Wi-Fi**.

3. Na kartě **DOMÁCÍ Wi-Fi** klikněte na tlačítko **VYBRAT DOMÁCÍ WI-FI**.

   Seznam s bezdrátovými sítěmi ke kterým jste byli dosud připojeni.

4. Vyberte domácí sít, 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**.

17.3.3. 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 Antivirus Plus je nastaven k automatickému dokončená nastavená následujících programů:

- Pokročilá ochrana před hrozbami je zapnuta
- 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.

17.3.4. 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 okně **ZRANITELNOSTI** klikněte na **Zabezpečení Wi-Fi**.
3. Podle toho, jaké informace potřebujete, vyberte jednu ze dvou karet - **DOMÁCÍ Wi-Fi** nebo **VEŘEJNÉ Wi-Fi**.
4. 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.

Udržujte možnost **Oznámení** povolenou k příjímání oznámení pokaždé když se váš systém připojí k síti.

18. BEZPEČNÉ SOUBORY

Ransomware je škodlivý software, který útočí na zranitelné systémy tím, že je uzamkne a požaduje peníze, aby uživateli vrátil kontrolu nad jeho systémem. Tento škodlivý software se chová obratně - zobrazuje podvodné zprávy, aby uživatele vyděsil a přinutil ho provést požadovanou platbu.

Infekce se může šířit nevyžádanými emaily, stahováním příloh nebo návštěvou infikovaných webových stránek a instalací škodlivých aplikací bez informování uživatele o dění v systému

Ransomware se může chovat jedním z následujících způsobů a bránit uživateli v přístupu k systému:

- Zašifruje citlivé a osobní soubory bez možnosti dešifrování, dokud oběť nezaplatí výkupné.
- Uzamkne obrazovku počítače a zobrazí zprávu se žádostí o peníze. V tomto případě není zašifrován žádný soubor, pouze je uživatel nucen k provedení platby.
- Blokuje aplikace před spuštěním.

S Bitdefender Bezpečnými soubory máte možnost zůstat chráněni proti ransomwarovým útokům na osobní soubory jako jsou dokumenty, fotky nebo filmy.

Poznámka

Pokročilá ochrana před hrozbami a Bezpečné soubory představují dvě vrstvy ochrany proti ransomwaru. Pokročilá ochrana před hrozbami je funkce, která zastaví ransomwarové útoky na jejich cestě ke kritickým oblastem Vašeho systému, zatímco Bezpečné soubory zajišťují, že žádný ze souborů na Vašem počítači nebude zašifrován.

18.1. Zapnutí/vypnutí Bezpečných souborů

Pro zapnutí/vypnutí modulu Bezpečné soubory:

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

Vždy, když se nějaká aplikace pokusí o přístup k chráněnému souboru, zobrazí se vyskakovací okno produktu Bitdefender. Přístup můžete povolit nebo odmítnout.

Poznámka
Safe Files nejsou standardně spuštěné.

18.2. Chraňte osobní soubory před ransomwarovými útoky

Pokud chcete vložit osobní soubory do úkrytu:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **BEZPEČNÉ SOUBORY** klikněte na **Chráněné složky**.
3. Při prvním přístupu k chráněným složkám jste uvedeni do funkce. Klikněte na **CHRÁNIT VÍCE SLOŽEK** pro pokračování.
4. Zvolte složku, kterou chcete zabezpečit, a klikněte na **OK**.

   Pro přidání dalších složek klikněte na odkaz **Chránit další složky**. Nebo také můžete složku přetáhnout do tohoto okna.

Ve výchozím stavu složky Obrázky, Videa, Dokumenty a Hudba jsou chráněny před útoky hrozeb. Osobní data uložená v online službám pro ukládání souborů, jako Box, Dropbox, Google Drive a OneDrive, jsou rovněž do chráněného prostředí začleněny, pokud jsou v systému nainstalované příslušné aplikace.

Pro vyhnutí se zpomalení systému doporučujeme přidat maximální počet 30 složek, nebo uložit více souborů do jedné složky.

Poznámka
Vlastní složky mohou být chráněny pouze pro aktuální uživatele. Systémové a aplikační soubory nelze přidat do výjimek.

18.3. Konfigurace přístupu k aplikacím

Ty aplikace, které se pokouší změnit nebo smazat chráněné soubory mohou být označeny jako potenciálně nebezpečné a budou přidány na list Blokovaných aplikací. Pokud je taková aplikace blokovaná a přitom jste si jisti, že je její chování normální, můžete ji povolit provedením následujících kroků:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **BEZPEČNÉ SOUBORY** klikněte na **Přístup k aplikacím**.

3. Zde je seznam aplikací, které se pokusily změnit soubory v chráněných složkách. Klikněte na spínač vedle aplikace, o které jste si jisti, že je bezpečná.

V tom samém okně můžete také vypnout ochranu proti ransomwaru u zvolených aplikací tím, že kliknete na příslušný přepínač.

Pro přidání nových aplikací do seznamu klikněte na odkaz **Přidat novou aplikaci do seznamu**.

18.4. Ochrana při bootu

Je známé, že mnoho škodlivých aplikací je nastaveno na spouštění při startu systému, a mohou tak způsobit závažné poškození počítače. Ochrana při spouštění produktu Bitdefender skenuje všechny kritické systémové oblasti před načtením všech souborů, s nulovým dopadem na systém.

K vypnutí Ochrany při bootu:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **BEZPEČNÉ SOUBORY** klikněte na **Nastavení**.
3. Vypněte **Ochranu při bootu**.

Poznámka

Aplikace přidané mezi výjimky budou také skenovány a bude s nimi náležitě naloženo.

19. ODSTRANĚNÍ RAMSOMWARE

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.

19.1. 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.

19.2. 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. Zapněte nebo vypněte **Automatická obnova**.

19.3. Zobrazování souborů, které byly automaticky obnoveny

Když je možnost **Automatické obnova** zapnutá, Bitdefender bude automaticky obnovovat soubory, které byly zašifrovány ransomwarem. Toto je způsob jak si můžete užívat bezstarostný pobyt u počítače s vědomím, že vaše soubory jsou v bezpečí.

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.

19.4. 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.

   Klikněte na **OBNOVIT SOUBORŮ** pro pokračování.
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 místo na vašem počítači.
5. Zobrazí se potvrzovací okno.

   Klikněte na **DOKONČIT** pro dokončení procesu obnovení.

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;

19.5. 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 **Výjimky**.
3. Pro přidání aplikací do seznamu, klikněte na **Přidat novou aplikaci do seznamu**.

20. OCHRANA VAŠICH OSOBNÍCH DAT SPRÁVCEM HESEL

Počítače používáme k online nákupům a placení účtů, pro připojení k sociálním sítím nebo přihlašování k aplikacím rychlého 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

20.1. 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 **Vytvořit novou portmonku**.
3. Klikněte na **Vytvořit nový**.
4. Zadejte požadované informace do příslušných polí.
   - Jméno portmonky - zadejte unikátní název pro portmonkovou databázi.
   - Hlavní heslo - zadejte heslo pro vaši portmonku.
   - Zopakujte heslo - znovu zadejte nastavené heslo.
   - Nápověda - zadejte nápovědu pro připomenutí hesla.
5. Klikněte na tlačítko **Pokračovat**.
6. V tomto kroku můžete provést uložení vašich informací do cloudu. Pokud zvolíte možnost Ano, bankovní informace zůstanou uloženy lokálně ve vašem zařízení. Vyberte požadovanou možnost a poté klikněte na tlačítko **POKRAČOVAT**.
7. Otevřete webový prohlížeč, ze kterého chcete importovat přihlašovací údaje.
8. Klikněte na **DOKONČIT**.

20.2. 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 **Vytvořit novou portmonku**.
3. Klikněte na **Z CÍLE**.
4. Ve vašem zařízení zvolte umístění, kam chcete uložit portmonkovou databázi, a zvolte pro něj název.
5. Klikněte na **Otevřít**.

6. Pojmenujte svou Portmonku a zadejte heslo, které jste poprvé použili při její tvorbě.
7. Klikněte na **IMPORTOVAT**.
8. Zvolte programy, ze kterých chcete, aby Portmonka importovala přihlašovací údaje, a poté klikněte na tlačítko **DOKONČIT**.

20.3. Export portmonkové databáze

Chcete-li exportovat databázi portmonky:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **SPRÁVCE HESEL** vyberte **Moje portmonky**.
3. Klikněte na ikonu ⋮ na požadované portmonce a poté zvolte **Exportovat**.
4. Vyhledejte umístění své portmonkové databáze a vyberte ji (.db soubor).
5. Klikněte na tlačítko **Save**.

Poznámka

Aby byla funkce **Exportovat** dostupná, Portmonka musí být otevřená.
Pokud je portmonka, kterou chcete exportovat, uzamčená, klikněte na **AKTIVOVAT PORTMONKU** a poté zadejte heslo, které jste poprvé použili při její tvorbě.

20.4. 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 **Moje portmonky**.
3. Klikněte na ikonu ⋮ na požadované portmonce a poté zvolte **Nastavení**.
4. 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.

20.5. 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 **Moje portmonky**.
3. Zvolte požadovanou portmonkovou databázi, a poté klikněte na **AKTIVOVAT PORTMONKU**.
4. 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.
- Pokud chcete upravit položku z tabulky, vyberte ji a klikněte na tlačítko **Editovat**.
- Pro smazání položky ji vyberte a klikněte na tlačítko **Odstranit**.

20.6. 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.

20.7. 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. Vyberte kartu **Nastavení zabezpečení**.

K dispozici jsou 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.
- **Neptat se mě na moje hlavní heslo** - nebudete vyzváni k zadání hlavního hesla při přístupu k počítači, prohlížeči nebo aplikaci.
- **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 kartu **Rozšíření**.

   Vyberte aplikaci, která má používat Správce hesel, a vylepšete tak svůj uživatelský komfort:

   - 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. Vyberte 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.

21. 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.

21.1. 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.
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.

21.2. 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**.

21.3. 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. 118).

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.

Když jste připojeni, na spodní straně rozhraní se zobrazuje uplynulý čas a IP adresa, která byla automaticky přiřazena k vašemu zařízení.

Pro přístup k dalším možnostem přejděte do **Menu** kliknutím na ikonu v horní levé 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**.
- **Nastavení** - můžete upravovat chování produktu dle svých potřeb:
  - nechat si zaslat upozornění, když se VPN automaticky připojí nebo odpojí
  - automaticky spustit aplikaci VPN při startu systému Windows
  - automaticky spustit aplikaci VPN, když se vaše zařízení připojí k nezabezpečeným bezdrátovým sítím

- **Přejít na Premium** - pokud užíváte bezplatnou verzi, zde můžete upgradovat na prémiový plán.
- **Podpora** - budete přesměrováni na naše Centrum podpory, kde si můžete přečíst užitečný článek o tom, jak používat Bitdefender VPN.
- **Informace o aplikaci** - vidíte informace o aktuálně nainstalované verzi.

21.4. 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 prémiovou verzi Bitdefender Premium VPN můžete přejít kdykoli kliknutím na tlačítko **ZÍSKAT NEOMEZENÝ PŘENOS**, které naleznete v rozhraní produktu.

Předplatné pro Bitdefender Premium VPN je nezávislé na předplatném produktu Bitdefender Antivirus Plus, 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 Antivirus Plus 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.

22. 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. 109).

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.
- Je vybaven vestavěnou ochranou hotspotu, která se použije, když je váš počítač připojený 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.

22.1. Použití prohlížeče Bitdefender Safepay™

Ve výchozím stavu produkt Bitdefender detekuje, když přejdete na stránku online bankovnictví nebo e-shop v kterémkoli prohlížeči ve vašem počítači, a vyzve vás k jejímu otevření v prohlížeči Bitdefender Safepay™.

Pro přístup do hlavního rozhran 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 **Otevřít 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.

Poznámka

Pokud není nainstalován modul plug-in Adobe Flash Player nebo je zastaralý, zobrazí se zpráva produktu Bitdefender. Pokračujte kliknutím na příslušné tlačítko.

Po dokončení procesu instalace je třeba ručně znovu otevřít prohlížeč Bitdefender Safepay™ a pokračovat v práci.

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.
- kliknutím na můžete vytisknout důležité informace.

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.

22.2. Konfigurace nastavení

Klikněte na a po výběru položku **Nastavení** proveďte konfiguraci prohlížeče Bitdefender Safepay™:

Seznam domén

Zvolte, jak se prohlížeč Bitdefender Safepay™ bude chovat, když navštívíte webové stránky na určitých doménách ve vašem obvyklém prohlížeči, jejich přidáním do seznamu domén a výběrm chování pro každou z nich:

- Automaticky otevřít v Bitdefender Safepay™.
- Produkt Bitdefender se vás pokaždé zeptá na akci.
- Nikdy nepoužívat prohlížeč Bitdefender Safepay™ při návštěvě stránky ze seznamu domén v obvyklém prohlížeči.

Blokování vyskakovacích oken

Kliknutím na příslušný přepínač můžete nastavit blokování vyskakovacích oken.

Můžete rovněž vytvořit seznam webových stránek, na kterých budou vyskakovací okna povolená. 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.

Spravovat pluginy
Můžete si vybrat, zda chcete povolit nebo zakázat konkrétní moduly v Bitdefender Safepay™.

Spravovat certifikáty
Můžete importovat certifikáty ze systému do úložiště certifikátů.

Vyberte **Import certifikátů** a následujte pokyny v průvodci k používání certifikátů v Bitdefender Safepay™.

Na polích s heslem automaticky zobrazit virtuální klávesnici
Virtuální klávesnice se automaticky zobrazí když je vybráno pole pro heslo.

Použít odpovídající přepínač pro zapnutí nebo vypnutí funkce.

Požádat o potvrzení před tiskem
Povolte tuto funkci, pokud si přejete dát svůj souhlas před zahájením tisku.

22.3. 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. Kliknutím na ikonu vedle panelu adresy 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.

22.4. 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. Vypnutí **Safepay upozornění**.

22.5. 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. Zapněte **Používat VPN se Safepay**.

23. OCHRANA DAT

23.1. 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.

Můžete rychle likvidovat soubory nebo složky v počítači pomocí kontextové nabídky systému Windows provedením následujícího postupu:

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 NAVŽDY** a poté potvrďte, že chcete v procesu pokračovat.

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

Nebo také můžete likvidovat soubory z rozhraní produktu Bitdefender následovně:

1. Klikněte na **Soukromí** v navigačním menu v rozhraní Bitdefender.
2. V okně **OCHRANA DAT** vyberte položku **Likvidátor dat**.
3. Postupujte podle průvodce likvidací souborů:
   a. Klikněte na tlačítko **PŘIDAT SLOŽKY** pro přidání složek, které si přejete trvale odstranit.

      Nebo také můžete přetáhnout soubory nebo složky přímo do tohoto okna.

   b. Klikněte na **SMAZAT NAVŽDY** a poté potvrďte, že chcete v procesu pokračovat.

      Počkejte, dokud produkt Bitdefender nedokončí likvidaci souborů.

   c. **Přehled výsledků**

Zobrazí se výsledky. Kliknutím na tlačítko **DOKONČIT** ukončíte průvodce.

24. USB IMUNIZÁTOR

Funkce automatického spouštění zabudovaná do operačních systémů Windows představuje velmi užitečný nástroj, který umožňuje počítačům automaticky spustit soubor z připojeného média. Například se může automaticky spustit instalace softwaru po vložení disku CD do optické jednotky.

Funkce však bohužel může být zneužita i hrozbami k automatickému spuštění a infiltraci vašeho počítače z přepisovatelných médií, jako USB flashdisky a paměťové karty připojené prostřednictvím čteček. 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. Když je zařízení USB imunizováno, hrozby ho již nemohou nakonfigurovat tak, aby se po připojení k počítači se systémem Windows spustila určitá aplikace.

Pro imunizaci USB zařízení:

1. Připojte flashdisk k počítači.
2. V počítači přejděte k vyjímatelnému paměťovému 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 počítači spouštět hrozby z neimunizovaných zařízení USB, vypněte funkci automatického spouštění média. Další informace viz *„Používání automatického sledování zranitelností“* (str. 97).

OPTIMALIZACE SYSTÉMU

25. 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 Antivirus Plus je nastaven k automatickému dokončení nastavení následujících programů:

- Pokročilá ochrana před hrozbami je zapnuta
- V Prevenci online hrozeb jsou zapnuta následující nastavení:
  - Šifrované skenování webu
  - Ochrana proti podvodům
  - Ochrana proti phishingu

25.1. 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 **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
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 **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
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.

25.2. 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 **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
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 **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
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.

25.3. 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 **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
3. Klikněte na tlačítko **KONFIGURACE** z karty Herního Profilu.
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 **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
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.

25.4. 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 **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
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**.

25.5. 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 **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
3. Klikněte na tlačítko **KONFIGURACE** z karty Profilu Módu 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.
- Bezpečnostní semafor je vypnutý.

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.

25.6. 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 **Nastavení** v navigačním menu v rozhraní Bitdefender.
2. Vyberte kartu **Profily**.
3. Posouvejte se dolů, dokud neuvidíte položku Optimalizování v reálném čase, a poté klikněte na příslušný vypínač a zapněte/vypněte ji.

ŘEŠENÍ PROBLÉMŮ

26. 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. 136)
- *„Sken se nespustí“* (str. 137)
- *„Nemůžete používat aplikaci“* (str. 140)
- *„Co dělat, když produkt Bitdefender blokuje bezpečnou webovou stránku nebo online aplikaci“* (str. 141)
- *„Co dělat pokud Bitdefender detekuje bezpečnou aplikaci jako ransomware“* (str. 141)
- *„Jak aktualizovat produkt Bitdefender na pomalém připojení k Internetu“* (str. 142)
- *„Služby produktu Bitdefender neodpovídají“* (str. 142)
- *„Funkce automatického vyplňování v mé portmonce nefunguje“* (str. 143)
- *„Odebrání produktu Bitdefender se nezdařilo“* (str. 144)
- *„Po instalaci produktu Bitdefender se můj systém nespustí“* (str. 145)

Pokud zde svůj problém nemůžete najít nebo ho navrhovaná řešení neodstraní, můžete kontaktovat zástupce technické podpory společnosti Bitdefender dle postupu uvedeného v kapitole *„Požádání o pomoc“* (str. 160).

26.1. 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. 66).

- **Nejsou splněny minimální požadavky na systém pro běh produktu Bitdefender.**

  Pokud váš počítač nesplňuje minimální požadavky na systém, zpomalí se, obzvláště pak v případě provozu několika aplikací současně. Další informace viz *„Minimální požadavky na systém“* (str. 3).

- **Máte nainstalované aplikace, které nepoužíváte**.

  Každý počítač má 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 si vybírají svou daň z výkonu vašeho počítače. 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 okně **ANTIVIRUS** klikněte na **Sken Systému**.
  3. Postupujte podle pokynů průvodce.

26.2. 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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. 66).
  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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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 *„Požádání o pomoc“* (str. 160).

26.3. 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 okně **POKROČILÁ OCHRANA PŘED HROZBAMI** klikněte na **Nastavení**.
3. V okně **Výjimky**, klikněte na **Přidat aplikace do výjimek**.
4. Najděte a vyberte aplikaci, kterou chcete vynechat, a poté klikněte na **OK**.

Pokud tyto informace nebyly užitečné, můžete se obrátit na podporu produktu Bitdefender dle popisu v části *„Požádání o pomoc“* (str. 160).

26.4. Co dělat, když produkt Bitdefender blokuje bezpečnou webovou stránku nebo online aplikaci

Produkt Bitdefender poskytuje bezpečné procházení webu díky filtrování veškerého webového provozu a blokování škodlivého obsahu. Je však možné, že produkt Bitdefender bude bezpečnou webovou stránku nebo online aplikaci za nebezpečnou, což způsobí, že je skenování HTTP provozu produktu Bitdefender chybně zablokuje.

Pokud je stejná stránka nebo aplikace blokována opakovaně, můžete ji přidat k výjimkám, aby nebyly jádry produktu 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 **Výjimky**.
3. Uveďte adresu blokované webové stránky nebo online aplikace do příslušného pole a klikněte na tlačítko **PŘIDAT**.
4. Klikněte na **ULOŽIT** k uložení změn a zavření okna.

Na tento seznam by měly být přidány pouze weby 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 *„Požádání o pomoc“* (str. 160).

26.5. Co dělat pokud Bitdefender detekuje bezpečnou aplikaci jako ransomware

Ransomware je škodlivý program, který se snaží získávat peníze od uživatelů tím, že uzamkne jejich zranitelné systémy. Pro udržení vašeho systému v bezpečí před nešťastnými situacemi, Bitdefender vám dává možnost odškodnit osobní soubory.

Pokud se pokusí aplikace změnit nebo smazat jeden z vašich chráněných souborů, bude považována za nebezpečnou a Bitdefender zablokuje její funkcionalitu.

Pokud je tato aplikace přidána do seznamu nedůvěryhodných aplikací a jste si jisti, že je bezpečné používat, postupujte takto:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **BEZPEČNÉ SOUBORY** klikněte na **Přístup k aplikacím**.
3. Zde je seznam aplikací, které se pokusily změnit soubory v chráněných složkách. Klikněte na tlačítko **Povolit** vedle aplikace, o které jste přesvědčeni, že je bezpečná.

26.6. 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.

26.7. 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.

- jiná řešení zabezpečení běžící na vašem počítači současně s produktem Bitdefender.

Chcete-li tuto chybu odstranit, vyzkoušejte následující řešení:

1. Chvíli počkejte, jestli se něco nezmění. Chyba může být dočasná.
2. Restartujte počítač a chvíli počkejte, než se produkt Bitdefender načte. Otevřete produkt Bitdefender a zjistěte, jestli chyba přetrvává. Restartování počítače problém obvykle 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. 66).

Pokud problém přetrvává, požádejte o pomoc zástupce podpory dle popisu v části *„Požádání o pomoc“* (str. 160).

26.8. 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 nabídku Nástroje.

3. Klikněte na Doplňky.
4. Klikněte na Rozšíření.
5. Ukažte na **Bitdefender Portmonku** a klikněte **Povolit**.

- V prohlížeči **Google Chrome:**
  1. Otevřete prohlížeč Google Chrome.
  2. Přejděte k ikoně Nabídka.
  3. Klikněte na Další nástroje.
  4. Klikněte na Rozšíření.
  5. Ukažte na **Bitdefender Portmonku** a klikněte **Povolit**.

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 *„Požádání o pomoc“* (str. 160).

26.9. 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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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.

26.10. 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. 68).
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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. 68).
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. 68).
2. Použijte funkci Obnovení systému v systému Windows a obnovte počítač do dřívějšího stavu před instalací produktu Bitdefender.
3. Restartujte systém v normálním režimu a požádejte o pomoc zástupce podpory dle popisu v části *„Požádání o pomoc“* (str. 160).

27. 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.

- *„Bitdefender Záchranný režim (Záchranné prostředí ve Windows 10)“* (str. 149)
- *„Co dělat, když produkt Bitdefender ve vašem počítači najde viry?“* (str. 153)
- *„Jak vyčistím virus v archivu?“* (str. 154)
- *„Jak vyčistím hrozbu v emailovém archivu?“* (str. 155)
- *„Co mám provést, pokud mám podezření na nebezpečný soubor?“* (str. 156)
- *„Co znamenají heslem chráněné soubory v protokolu skenu?“* (str. 157)
- *„Co znamenají přeskočené položky v protokolu skenu?“* (str. 157)
- *„Co znamenají překomprimované soubory v protokolu skenu?“* (str. 158)
- *„Proč produkt Bitdefender automaticky odstranil infikovaný soubor?“* (str. 158)

Pokud zde svůj problém nemůžete najít nebo ho navrhovaná řešení neodstraní, můžete kontaktovat zástupce technické podpory společnosti Bitdefender dle postupu uvedeného v kapitole *„Požádání o pomoc“* (str. 160).

27.1. Bitdefender Záchranný režim (Záchranné prostředí ve Windows 10)

Záchraný režim je funkce produktu Bitdefender, která vám umožňuje skenovat a dezinfikovat všechny existující oddíly pevných disků uvnitř i mimo Váš operační systém.

Jakmile je Bitdefender Antivirus Plus nainstalován na **Windows 7, Windows 8 and Windows 8.1** a soubor Bitdefender Obraz záchranného režimu stažen, můžete využívat Záchranného módu i když nebudete moci nastartovat systém Windows.

Ve Windows 10 je Bitdefender Záchranné prostředí integrováno s Windows RE, což znamená, že na tento operační systém není nutné stahovat žádný Obraz záchranného režimu, a že tohoto modulu není možné využít ani v

případě problémů se startem. Pro vyčištění systému předtím, než budou načteny služby systému Windows, doporučujeme použít Bitdefender Záchranný disk CD.

Bitdefender Záchranný disk je nástroj zdarma, který skenuje a čistí Váš počítač kdykoli budete mít podezření, že je jeho výkon ovlivněn nějakou hrozbou. Užitečné články s detaily o tom, jak ho vytvořit a používat, jsou k dispozici v Bitdefender Centru podpory na https://www.bitdef.cz/podpora/.

Stahuji Bitdefender Obraz záchranného režimu

Pro možnost využití Záchranného režimu na **Windows 7, Windows 8 and Windows 8.1** je nutné nejprve stáhnout jeho obrazový soubor podle následujících pokynů:

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na položku **Záchranný režim**.
3. Klikněte na **Ano** v potvrzovacím okně, které vás vyzývá k restartování vašeho počítače.

   Počkejte, než se Bitdefender Obraz záchranného režimu stáhne ze serverů produktu Bitdefender. Jakmile je stahování dokončeno, počítač se restartuje.

   Zobrazí se nabídka s výzvou k výběru operačního systému, který se má spustit. V tomto kroku můžete zvolit zapnutí systému v záchranném, nebo normálním režimu.

Poznámka

Díky integraci s Prostředím obnovy systému Windows ve **Windows 10** není na tento operační systém potřeba stahovat žádný Obraz záchranného režimu.

Nastartování vašeho systému v Záchranném režimu ve Windows 7, Windows 8 a Windows 8.1

Záchranný režim můžete spustit jedním ze dvou způsobů:

Z rozhraní produktu Bitdefender

1. Klikněte na **Zabezpečení** v navigačním menu v rozhraní Bitdefender.
2. V okně **ANTIVIRUS** klikněte na položku **Záchranný režim**.

3. Klikněte na **Ano** v potvrzovacím okně, které vás vyzývá k restartování vašeho počítače.
4. Po restartu se zobrazí nabídka s výzvou k výběru operačního systému. Vyberte položku **Záchranný režim Bitdefender** a nastartujte do prostředí produktu Bitdefender, ve kterém můžete vyčistit oddíl systému Windows.
5. Pokud k tomu budete vyzváni, stiskněte klávesu **Enter** a zvolte rozlišení obrazovky nejbližší tomu, které obvykle používáte. Poté znovu stiskněte klávesu **Enter**.

   Záchranný režim Bitdefender se za několik okamžiků načte.

Nastartování počítače přímo do záchranného režimu

Pokud se systém Windows již nedokáže spustit, můžete počítač nastartovat přímo do záchranného režimu Bitdefender pomocí následujícího postupu:

- V systému **Windows 7**:
  1. Držte stisknuté tlačítko **F8**, dokud se neobjeví obrazovka **Pokročilé možnosti nastartování systému**.
  2. Použijte směrové šipky pro zvolení Bitdefender Záchranného režimu a poté stiskněte **Enter**.

     Záchranný režim Bitdefender se za několik okamžiků načte.
- V systémech **Windows 8 a Windows 8.1**:
  1. Držte stisknuté tlačítko **Shift**, dokud se neobjeví obrazovka **Pokročilé možnosti spuštění**.
  2. Vyberte položku **Použít jiný operační systém** a poté Bitdefender Záchranný režim.

     Záchranný režim Bitdefender se za několik okamžiků načte.

Poznámka

Spuštění tohoto počítače v Záchranném režimu je možné pouze, pokud byl záznam záchranného režimu již předtím stažen, jak již bylo uvedeno v „Stahuji Bitdefender Obraz záchranného režimu“ (str. 150).

Startuji Váš systém v Záchranném prostředí ve Windows 10

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 okně **ANTIVIRUS** klikněte na položku **Záchranné prostředí**.
3. V okně, které se zobrazí, klikněte na **Restartovat**.

   Záchranné prostředí Bitdefender se za několik okamžiků načte.

Skenuji Váš systém v Záchranném režimu (Záchranné prostředí ve Windows 10)

Pro skenování systému v Záchranném režimu (Záchranném prostředí):

- V systémech **Windows 7, Windows 8 a Windows 8.1**:

  1. Vstupte do záchranného režimu dle popisu v části „Nastartování vašeho systému v Záchranném režimu ve Windows 7, Windows 8 a Windows 8.1“ (str. 150).
  2. Zobrazí se logo produktu Bitdefender a spustí se kopírování antivirových jader.
  3. Poté se objeví uvítací okno. Klikněte na tlačítko **Pokračovat**.
  4. Aktualizace informační databáze o hrozbách bude zahájena.
  5. Po dokončení aktualizace se objeví okno manuálního antivirového skenu produktu Bitdefender.
  6. Klikněte na tlačítko **Skenovat**, v zobrazeném okně vyberte cíl skenování a kliknutím na tlačítko **Otevřít** spusťte sken.

     Doporučujeme oskenovat celý oddíl systému Windows.

     Poznámka
     Při práci v záchranném režimu jsou oddíly pojmenované ve stylu systému Linux. Diskové oddíly budou uvedeny jako sda1, což pravděpodobně odpovídá oddílu (C:) systému Windows, sda2 odpovídá oddílu (D:) atd.

7. Počkejte na dokončení skenu. Při nalezení jakékoli hrozby následujte pokyny pro její odstranění.
8. Chcete-li záchranný režim ukončit, klikněte pravým tlačítkem na prázdné místo na ploše, v zobrazené nabídce vyberte položku **Ukončit** a zvolte, zda chcete počítač restartovat, nebo vypnout.

- V systému **Windows 10**:

1. Vstupte do Záchranného prostředí dle popisu v „Startuji Váš systém v Záchranném prostředí ve Windows 10“ (str. 152).
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. Pro ukončení Záchranného prostředí klikněte na tlačítko **ZAVŘÍT** v okně s výsledky skenování.

27.2. Co dělat, když produkt Bitdefender ve vašem počítači najde viry?

Přítomnost hrozby ve vašem počítači můžete zjistit jedním z následujících způsobů:

- Provedli jste sken počítače a produkt Bitdefender v něm našel infikované položky.
- Výstraha na ohrožení vás upozorní, že produkt Bitdefender zablokoval na vašem počítači 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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
   c. V okně **Štít** 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. 66).
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. 68).
2. Zobrazení skrytých objektů v systému Windows. Pokud chcete zjistit jak to udělat, obraťte se na *„Jak zobrazím skryté objekty v systému Windows?“* (str. 66).
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 *„Požádání o pomoc“* (str. 160).

27.3. 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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
   c. V okně **Štít** 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 *„Požádání o pomoc“* (str. 160).

27.4. 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 okně **ANTIVIRUS** klikněte na položku **Nastavení**.
   c. V okně **Štít** 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 *„Požádání o pomoc“* (str. 160).

27.5. 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 *„Požádání o pomoc“* (str. 160).

27.6. 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 jejich obsah byl extrahován, skenování produktu Bitdefender v reálném čase by je automaticky otestovalo, aby váš počítač zůstal chráněný. 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.

27.7. 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.

27.8. 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.

27.9. 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.

KONTAKTUJTE NÁS

28. POŽÁDÁNÍ 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. 136) 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 Antivirus Plus“ (str. 160)
- „Kontaktujte nás prostřednictvím našeho centra podpory online“ (str. 161)

Kontaktujte nás přímo z Bitdefender Antivirus Plus

Pokud máte funkční připojení k Internetu, můžete požádat podporu produktu Bitdefender o pomoc přímo z rozhraní produktu.

Postupujte následovně:

1. Klikněte na **Podpora** v navigačním menu v rozhraní Bitdefender.
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 řešení váš problém nevyřeší, přejděte na

   https://www.bitdef.cz/kontakt/a kontaktujte zástupce podpory.

29. 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.

29.1. 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/.

29.2. 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 funkci, 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.

29.3. Portál HOTforSecurity

HOTforSecurity je bohatý zdroj informací o počítačovém zabezpečení. Zde se můžete dozvědět o různých hrozbách, kterým je počítač vystaven při připojení k internetu (malware, phishing, spam, cyber-zločince).

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.

30. KONTAKTNÍ INFORMACE

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.

30.1. 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
Web: https://www.bitdef.cz/

30.2. 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.

30.3. 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
Telefon: (+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
Telefon: +34 902 19 07 65
Prodej: comercial@bitdefender.es
Technická podpora: https://www.bitdefender.es/support/consumer.html
Web: https://www.bitdefender.es

Rumunsko

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 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
Web: 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
Web: 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 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.

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.

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).

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.

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.

Spouštěcí sektor:

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.

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.

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.