Bitdefender®

PASSWORD MANAGER

ANVÄNDARMANUAL

Bitdefender Password Manager

Användarmanual

Publiceringsdatum 2022-11-21

Rättsligt meddelande

Bitdefender

Innehållsförteckning

OM DEN HÄR GUIDEN

Syfte och avsedd målgrupp

Den här guiden är avsedd för alla Bitdefender-användare på alla operativsystem som stöds (Windows, MacOS, Android, iOS) som har valt Bitdefender Password Manager som deras go-to lösenordshanteringsverktyg. Informationen som presenteras i den här boken är inte bara lämplig för datorvana, utan den fungerar som en tillgänglig och vänlig guide för alla.

Den här guiden hjälper dig att ta reda på hur du får ut det bästa av vår ultrasäkra och funktionsrika lösenordshanterare genom att diskutera alla dess funktioner och funktioner i detalj.

Vi önskar dig en trevlig och användbar föreläsning.

Hur man använder den här guiden

Den här guiden är organiserad kring flera viktiga ämnen:

Komma igång (sida 4)

Kom igång med Bitdefender Password Manager och installationsprocessen.

Funktioner och funktioner (sida 15)

Lär dig hur du använder Bitdefender Password Manager och alla dess funktioner.

Få hjälp (sida 26)

Var man ska leta och var man kan be om hjälp om något oväntat dyker upp.

Konventioner som används i denna guide

Typografiska konventioner

Flera textstilar används i den här guiden för att förbättra läsbarheten. Deras aspekt och betydelse presenteras i tabellen nedan.

Utseende	Beskrivning
`sample syntax`	Syntaxexempel skrivs ut med `monospaced` tecken.
https://www.bitdefender.com	URL-länken pekar på någon extern plats, på http- eller ftp-servrar.
documentation@bitdefender.com	E-postadresser infogas i texten för kontaktinformation.
Om den här guiden (sida 1)	Detta är en intern länk till någon plats i dokumentet.
`filename`	Filer och kataloger skrivs ut med `monospaced` font.
alternativ	Alla produktalternativ skrivs ut med hjälp av **djärv** tecken.
nyckelord	Viktiga sökord eller fraser markeras med hjälp av **djärv** tecken.

Förmaningar

Förmaningarna är anteckningar i texten, grafiskt markerade, som uppmärksammar dig på ytterligare information relaterad till det aktuella stycket.

Notera

Anteckningen är bara en kort observation. Även om du kan utelämna det, kan anteckningarna ge värdefull information, som specifik funktion eller en länk till något relaterat ämne.

Viktig

Detta kräver din uppmärksamhet och rekommenderas inte att hoppa över det. Vanligtvis ger den icke-kritisk men betydande information.

Varning

Detta är viktig information som du bör behandla med ökad försiktighet. Inget dåligt kommer att hända om du följer anvisningarna. Du bör läsa och förstå den, för den beskriver något extremt riskabelt.

Begäran om kommentarer

Vi inbjuder dig att hjälpa oss att förbättra boken. Vi har testat och verifierat all information efter bästa förmåga. Skriv för att berätta för oss om eventuella brister du hittar i den här boken eller hur du tror att den kan förbättras, för att hjälpa oss att förse dig med bästa möjliga dokumentation.

Meddela oss genom att skicka ett mejl till documentation@bitdefender.com. Skriv alla dina dokumentationsrelaterade e-postmeddelanden på engelska så att vi kan behandla dem effektivt.

1. VAD ÄR BITDEFENDER PASSWORD MANAGER

Bitdefender Password Manager är en multiplattformstjänst utformad för att hjälpa användare att lagra och organisera alla sina onlinelösenord. Den är byggd med de starkaste kända kryptografiska algoritmerna för högsta nivå av säkerhet och digital säkerhet. Det fungerar som en webbläsartillägg och mobilappslösning för identitets- och lösenordshantering, banktjänster och all annan typ av känslig information över enheter.

Bitdefender Password Manager kan automatiskt spara, autofyll, automatiskt generera och hantera dina lösenord för alla webbplatser och onlinetjänster med hjälp av ett enda huvudlösenord, vilket gör din övergripande digitala identitet mycket lättare att hantera.

1.1. Säkerhet och hur det fungerar

Bakom Bitdefender Password Manager Programvaran står för några av de senaste kryptografiska algoritmerna som garanterar den högsta datasäkerheten användare kan hoppas på, såsom AES-256-CCM, SH512, BCRYPT, HTTPS och WSS-protokoll för dataöverföring. All data inblandad är alltid krypterad och dekrypterad lokalt. Detta gör det så att endast kontoinnehavaren ensam kan ha tillgång till den information som finns lagrad på kontot, samt till huvudlösenordet som används för att komma åt och därefter använda uppgifterna i fråga.

1.2. Lösenordshanteraren testversion och betalversioner

Testversionen av Bitdefender Password Manager fungerar av alla konton som är identiska med den betalda versionen av produkten, men dess tillgänglighet kommer att upphöra efter 90 dagar efter aktiveringen.

> **Notera**
> Observera att den betalda versionen av produkten, även om den kan köpas som en helt fristående produkt, är obegränsad tillgång till Password Manager inkluderad i prenumerationerna 'Bitdefender Premium Security och Bitdefender Ultimate Security.

2. KOMMA IGÅNG

2.1. Systemkrav

Du kan använda den senaste versionen av Bitdefender Password Manager endast på enheter som kör följande operativsystem:

- **För PC-användare:**
  - Windows 7 med Service Pack 1
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows 11
- **För macOS-användare:**
  - macOS 10.14 (Mojave) och senare macOS-operativsystem

  Notera
  Observera att systemprestanda kan påverkas på enheter som har gamla generationens processorer.
- **För iOS-användare:**
  - iOS 11.0 eller senare iOS operativsystem
- **För Android-användare:**
  - Android 5.1 och senare Android-operativsystem

  Notera
  - Funktionen för upplåsning av fingeravtryck stöds på **Android 6.0** och senare.
  - Autofyll-funktionen stöds på **Android 8.0** och senare, kompatibel med iPhone, iPad och iPod touch.

2.1.1. Programvarukrav

För att kunna använda Bitdefender Password Manager och alla dess funktioner måste dina Windows- eller macOS-enheter uppfylla följande programvarukrav:

- **Microsoft Edge** (baserat på Chromium 80 och senare)
- **Mozilla Firefox** (version 65 eller senare)
- **Google Chrome** (version 72 eller senare)
- **Safari** (version 12 eller senare)

Notera
Programvarukraven gäller inte för Android och iOS.

Varning
Underlåtenhet att uppfylla systemkraven som presenteras ovan kommer att resultera i antingen oförmåga att installera Bitdefender Password Manager eller fel på produkten.

2.2. Installation

Det här kapitlet kommer att vägleda dig om hur du installerar Bitdefender Password Manager till både webbläsarna på din Windows-dator och macOS, såväl som på dina mobila Android- eller iOS-enheter.

Viktig
Innan installationen, se till att du har en giltig Password Manager-prenumeration i din Bitdefender Central konto så att det här webbläsartillägget kan hämta sin giltighet från ditt konto.

Aktiva prenumerationer listas i **mina prenumerationer** avsnitt inom Bitdefender Central.

2.2.1. Installerar på Windows- och macOS-enheter

Till skillnad från de flesta stationära applikationer och mjukvara som måste installeras och konfigureras på dessa enheter, kommer Bitdefender Password Manager som ett webbläsartillägg - även kallat ett tillägg - som snabbt kan läggas till och aktiveras i din föredragna webbläsare.

De webbläsare som för närvarande stöds för produkten är följande: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge**, och **Safari**.

1. Gå till https://central.bitdefender.com/ och logga in på ditt konto.
   Om du inte redan har ett konto, klicka på **SKAPA KONTO**, skriv sedan ditt fullständiga namn, en e-postadress och ett lösenord.
2. Välj **Mina enheter** på skärmens vänstra sidofält.
3. I den **Mina enheter** fortsätt genom att klicka på **+ Lägg till enhet**.
4. Denna åtgärd kommer att uppmana ett nytt fönster att dyka upp. Välja **Lösenordshanteraren** i urvalsskärmen.
5. Välja **Denna apparat**.
   Om du vill installera på en annan enhet väljer du Andra enheter. Du kan sedan e-posta en nedladdningslänk till respektive enhet eller direkt kopiera URL:en för installationen.
6. Välj sedan i vilken webbläsare du vill installera tillägget Password Manager.
7. Varje motsvarande knapp omdirigerar dig till webbläsarens Extensions Store. Därifrån följer du bara instruktionerna på skärmen som visas nedan:

   Microsoft Edge

   - Klicka på **Skaffa sig** knapp
   - Klick **Lägg till tillägg** i prompten som visas på skärmen

   Google Chrome

   - Klicka på **Lägg till i Chrome** knapp
   - Klicka på i bekräftelserutan **Lägg till tillägg**

   Mozilla Firefox

   - Klicka på **Lägg till i Firefox** knapp
   - Klicka på **Installera** knappen i det övre högra hörnet av skärmen

   Safari

   - Klicka på **Skaffa sig** knappen och klicka sedan **Installera**
   - Öppna Safari och välj **Inställningar** i den översta menyraden
   - I fönstret Inställningar klickar du på **Tillägg** flik
   - Markera kryssrutan bredvid Password Manager för att aktivera det

När du har följt dessa steg, ställ in ett starkt huvudlösenord och tryck sedan på **Spara huvudlösenord** knappen efter att du läst och godkänner **Villkor**.

Viktig

Observera att du kommer att kräva detta huvudlösenord för att låsa upp alla lösenord, kreditkortsinformation och anteckningar som sparats i Bitdefender Password Manager. Detta är i huvudsak nyckeln som gör att ägaren kan använda denna produkt.

Varning

När du skapar huvudlösenordet får du ett **24-siffrig återställningsnyckel**. Anteckna din återställningsnyckel på ett säkert ställe och tappa inte bort den. Den här nyckeln är det enda sättet att komma åt dina lösenord som sparats i Lösenordshanteraren i händelse av att du råkar **glöm huvudlösenordet** tidigare konfigurerat för ditt konto.

- Du kan trycka på **Stänga** när det är klart.

2.2.2. Installerar på Android-enheter

Den enklaste metoden för att installera Bitdefender Password Manager för Android-telefoner och surfplattor är att ladda ner applikationen direkt från Google Play.

Installation av Bitdefender Password Manager-appen kan också göras via din Bitdefender Central konto:

1. Logga in på ditt Bitdefender Central-konto på din Android-mobilenhet genom att gå till https://login.bitdefender.com/central/login.
2. Välj **Mina enheter** på skärmens vänstra sidofält.
3. I den **Mina enheter** fortsätt genom att klicka på **+ Lägg till enhet**.
4. Denna åtgärd kommer att uppmana ett nytt fönster att dyka upp. Välja **Lösenordshanteraren** i urvalsskärmen.
5. Välja **Denna apparat**.

Om du vill installera på en annan enhet, välj **Andra enheter**. Du kan sedan e-posta en nedladdningslänk till respektive enhet eller direkt kopiera URL:en för installationen.

6. Du kommer att omdirigeras till Google Play. Knacka **Installera** för att ladda ner Bitdefender Password Manager på Android.
7. När nedladdningen är klar öppnar du Lösenordshanteraren program.
8. Om du inte är inloggad automatiskt på ditt konto, logga in med ditt användarnamn och lösenord.
   När du har följt dessa steg, ställ in ett starkt huvudlösenord och tryck sedan på **Spara huvudlösenord** knappen efter att du läst och godkänner **Villkor**.

   Viktig
   Observera att du kommer att kräva detta huvudlösenord för att låsa upp alla lösenord, kreditkortsinformation och anteckningar som sparats i Bitdefender Password Manager. Detta är i huvudsak nyckeln som gör att ägaren kan använda denna produkt.

   Varning
   När du skapar huvudlösenordet får du ett **24-siffrig återställningsnyckel**. Anteckna din återställningsnyckel på ett säkert ställe och tappa inte bort den. Den här nyckeln är det enda sättet att komma åt dina lösenord som sparats i Lösenordshanteraren i händelse av att du råkar **glöm huvudlösenordet** tidigare konfigurerat för ditt konto.

   - Du kan trycka på **Stänga** när det är klart.
9. Skapa en **4-siffrig PIN-kod**, så om du byter till en annan app och sedan återgår till lösenordshanteraren behöver du inte ange huvudlösenordet som du ställt in tidigare. Om tillgängligt kan du även aktivera ansiktsigenkänning eller fingeravtrycksautentisering.
10. Knacka på **Aktivera Autofyll** för att konfigurera Android autofyll-inställningar.

    Notera
    Om du hoppar över det här steget kan du aktivera och anpassa Androids autofyllfunktioner vid ett senare tillfälle genom att följa instruktionerna på Intelligent autofyll (sida 16).

11. Du kommer att mötas av en lista med appar som kan fylla i lösenord automatiskt.
    Välj **Lösenordshanteraren** och sedan kommer enheten att uppmana dig att bekräfta att du litar på den här appen.
    Knacka **OK**.
12. Ange PIN-koden du konfigurerade i **steg 9** för att bekräfta denna åtgärd.

Installationen på din Android-enhet är nu klar.

2.2.3. Installerar på iOS-enheter

Den enklaste metoden för att installera Bitdefender Password Manager för iOS- och iPadOS-enheter är att ladda ner programmet från Apple App Store.

Installation av Bitdefender Password Manager-appen kan också göras via din Bitdefender Central konto:

1. Logga in på ditt Bitdefender Central-konto på din iPhone eller iPad genom att gå till https://login.bitdefender.com/central/login.
2. Välj **Mina enheter** på skärmens vänstra sidofält.
3. I den **Mina enheter** fortsätt genom att klicka på **+ Lägg till enhet**.
4. Denna åtgärd kommer att uppmana ett nytt fönster att dyka upp. Välja **Lösenordshanteraren** i urvalsskärmen.
5. Välja **Denna apparat**.
   Om du vill installera på en annan enhet, välj **Andra enheter**. Du kan sedan e-posta en nedladdningslänk till respektive enhet eller direkt kopiera URL:en för installationen.
6. Du kommer att omdirigeras till **App Store**. Tryck på molnikonen med en pil som pekar nedåt för att ladda ner Bitdefender Password Manager för iOS.
7. När applikationen är installerad, öppna den och markera den lilla rutan på skärmen. Välj **Fortsätta** efter att du läst och håller med **Prenumerationsavtal**.
8. Om du inte är inloggad automatiskt på ditt konto, logga in med ditt användarnamn och lösenord.

När du har följt dessa steg, ställ in ett starkt huvudlösenord och tryck sedan på **Spara huvudlösenord** knappen efter att du läst och godkänner **Villkor**.

Viktig

Observera att du kommer att kräva detta huvudlösenord för att låsa upp alla lösenord, kreditkortsinformation och anteckningar som sparats i Bitdefender Password Manager. Detta är i huvudsak nyckeln som gör att ägaren kan använda denna produkt.

Varning

När du skapar huvudlösenordet får du ett **24-siffrig återställningsnyckel**. Anteckna din återställningsnyckel på ett säkert ställe och tappa inte bort den. Den här nyckeln är det enda sättet att komma åt dina lösenord som sparats i Lösenordshanteraren i händelse av att du råkar **glöm huvudlösenordet** tidigare konfigurerat för ditt konto.

- Du kan trycka på **Stänga** när det är klart.

9. Skapa en **4-siffrig PIN-kod**, så om du byter till en annan app och sedan återgår till lösenordshanteraren behöver du inte ange huvudlösenordet som du ställt in tidigare. Om tillgängligt kan du även aktivera ansiktsigenkänning eller fingeravtrycksautentisering.

Installationen på din iOS / iPadOS-enhet är nu klar!

3. IMPORTERA OCH EXPORTERA DINA LÖSENORD

Bitdefender Password Manager är byggd på ett sådant sätt att det effektivt underlättar kommunikation och dataöverföring med externa källor, plattformar och mjukvaruverktyg. Detta är den centrala anledningen till att det mycket vanliga behovet av att importera eller exportera lösenord till eller ut ur Bitdefender Password Manager kan tillfredsställas med lätthet.

3.1. Kompatibilitet

Bitdefender Password Manager kan sömlöst överföra data från följande lista med applikationer:

- **1 Lösenord**
- **Bitwarden**
- **Bitdefender Password Manager**
- **Hejdå**
- **Chrome webbläsare**
- **Claro**
- **Dashlane**
- **Edge webbläsare**
- **ESET Password Manager v2**
- **ESET Password Manager v3**
- **StickyPassword**
- **Watchguard**
- **Firefox webbläsare**
- **Gestor de contraseñas – Claro**
- **Gestor de contraseñas – SIT**
- **Gestor de contraseñas – Telnor**
- **KeepPass 2.x**
- **LastPass**
- **Panda Dome lösenord**

- **PassWatch**
- **Saferpass**
- **SFR Cybersécurité**
- **SITTA**
- **F-Secure**
- **Telnor**

> **Notera**
> Om namnet på webbläsaren eller lösenordshanteraren som du försöker överföra datafiler från inte nämns i listan ovan kan du följa vår onlineguide om hur användare kan redigera en CSV-fil från lösenordshanterare som inte stöds så att du kan importera din information till **Bitdefender Password Manager**: https://www.bitdefender.com/consumer/support/answer/2472/

Denna överföring av data mellan Bitdefender Password Manager och annan programvara för kontohantering kan göras genom följande dataformat:

CSV, **JSON**, **XML**, **Text**, **1pif** och **FSK**.

3.2. Importerar till lösenordshanteraren

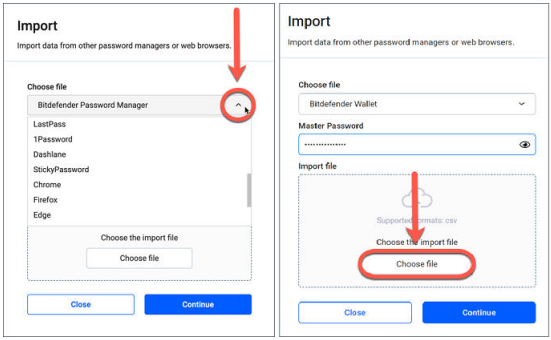
Bitdefender Password Manager låter dig enkelt importera lösenord från andra lösenordshanterare och webbläsare. Om du för närvarande funderar på att byta till Bitdefender Password Manager från en annan lösenordshanteringstjänst, har du med största sannolikhet lagrat en stor mängd referenser som användarnamn, lösenord och annan inloggningsinformation som krävs för alla dina konton.

Nu när du har valt Bitdefender Password Manager kommer du att leta efter att importera den sparade informationen till den.

Så här importerar du din lagrade information från andra appar och webbläsare till Bitdefender Password Manager, **oavsett operativsystem** där du har valt att installera denna produkt:

1. Klicka på ikonen Lösenordshanteraren i din webbläsare (på Windows eller macOS) eller starta applikationen Lösenordshanteraren (på Android eller iOS). Om du uppmanas anger du din Huvudlösenord.

2. Öppna lösenordshanteraren menyn för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
3. Scrolla ner till **Data** avsnittet och klicka på **Importera data** alternativ.
4. Använd rullgardinsmenyn för att välja namnet på lösenordshanterarens app eller webbläsare som du vill importera dina konton från. Mata in din Huvudlösenord i motsvarande fält och klicka sedan på **Välj FIL**.



5. Bläddra igenom dina mappar för att hitta platsen där du har sparat filen som innehåller dina användarnamn och lösenord, exporterat från din andra lösenordshanterare eller webbläsare och tryck sedan på **Fortsätta**.

När de har importerats kommer dina lösenord att vara tillgängliga på alla enheter där Bitdefender Password Manager-applikationen eller webbläsartillägget är installerat.

3.3. Exporterar från Password Manager

Bitdefender Password Manager låter dig enkelt exportera dina sparade lösenord (inklusive kontoinloggningsuppgifter, säkra anteckningar etc.) till en CSV-fil (kommaseparerade värden) eller en krypterad fil om du någonsin vill byta till en annan lösenordshanterartjänst, så att din avgång från Bitdefender Password Manager inte kommer att vara en svår process.

> **Viktig**
> En CSV-fil är **inte** krypterad och innehåller användarnamn och lösenord i vanlig textformat, vilket innebär att din privata information kan läsas av alla som har tillgång till din enhet. Vi rekommenderar därför att du följer instruktionerna nedan på en betrodd enhet.

Så här kan du exportera dina data från Bitdefender Password Manager:

1. Klicka på ikonen Lösenordshanteraren i din webbläsare (på Windows eller macOS) eller starta applikationen Lösenordshanteraren (på Android eller iOS). Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
3. Scrolla ner till **Data** avsnitt och klicka på **Exportera data** alternativ.
4. Nu bör du få följande två alternativ:
   - **CSV**
   - **Lösenordsskyddade filer**

   Välj önskat alternativ, ange sedan ditt huvudlösenord och klicka på **Exportera data** knapp.

   > **Notera**
   > Om du väljer alternativet för lösenordsskyddad fil kommer du att bli ombedd att kryptera data som innehåller kontolistan med ett lösenord, så på detta sätt skulle bara du kunna komma åt den om det behövs.

5. Din webbläsare/app kommer att fortsätta genom att spara en fil med namnet `Bitdefender Password Manager_exported_data_current-date` till ditt system i standardmappen för nedladdning. Den innehåller alla dina data lagrade i Bitdefender Password Manager.

Efter att ha exporterat din data kan du ladda upp den till den lösenordshanterare du väljer.

4. FUNKTIONER OCH FUNKTIONER

Det här kapitlet tar dig igenom alla funktioner och funktioner i Bitdefender Password Manager, förklarar deras användbarhet och hur du använder dem mest effektivt.

4.1. Lösenordshantering

4.1.1. Lösenordsgenerator

Den gyllene regeln när det gäller onlinesäkerhet är att alltid använda unika slumpmässiga lösenfraser för varje tjänst som kräver kontoskapande. Lösenordsåteranvändning på flera plattformar är den främsta orsaken bakom identitetsstöld och förluster i samband med fientlig kontoövertagande.

Den här funktionen hjälper användare att skapa säkra, komplexa och unika lösenord för varje nytt konto de skapar var som helst online. Detta eliminerar behovet för användare att komma på starka lösenord på egen hand eller vara noga med att inte återanvända samma lösenord för flera konton.

De **Lösenordsgenerator** kan nås via fliken överst i lösenordshanterarens gränssnitt.

Generatorn kan ställas in för att returnera lösenord **mellan 4 och 32 tecken**.

Du kan också ange vilka typer av tecken som ska eller inte ska finnas i det slumpmässigt genererade lösenordet genom att markera eller avmarkera motsvarande kryssrutor. **(gemener, versaler, siffror, special)**

Genom att trycka på knappen till höger om det visade lösenordet kommer generatorn att ändra det föreslagna lösenordet.

För att använda det visade lösenordet, tryck **Använd lösenord**, åtgärd som sparar teckensträngen till ditt urklipp.

> **Notera**
> Dina tidigare genererade lösenord kommer att lagras tillfälligt i lösenordshistoriken, som kan nås via **Lösenordshistorik** knapp.

4.1.2. Lösenordsfångning

Med den här funktionen i Lösenordshanteraren kommer du att bli ombedd att lagra alla dina nya lösenord direkt efter att du har skapat dem. Lösenordshanteraren kommer att uppmana användare att lagra sina nyskapade lösenord, så att de kan läggas till i den ultrasäkra miljön som tillhandahålls av Bitdefender direkt.

4.1.3. Intelligent autofyll

Bitdefender Password Manager kan ställas in på ett sådant sätt att den kan autofylla dina inloggningsuppgifter och viktigast av allt lösenord. Proprietära algoritmer kan upptäcka och förfylla inloggningsuppgifter på tidigare besökta webbplatser, vilket sparar användarnas tid varje gång de loggar in på en tjänst.

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.
   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
3. Klicka på **Enhetsinställningar**.
4. Här kommer du att märka en knapp som visar antingen **Inaktivera automatisk fyllning** eller **Aktivera automatisk fyllning**. Den här inställningen styr drifttillståndet för den intelligenta autofyllfunktionen.

4.1.4. Säkerhetsrapport

Säkerhetsrapporten är ett verktyg som genererar rapporter baserade på ett antal funktioner som är avsedda att stärka din digitala säkerhet. Det kommer att meddela dig om ett lösenord kräver din omedelbara uppmärksamhet genom att bestämma dess säkerhetsnivå. Det kommer att upptäcka lösenordsdubbletter och uppmana dig att ändra dem i enlighet med detta, vilket undviker farorna med att återvinna samma lösenord för flera konton.

Rapporten kommer att koncentrera sig på att ge dig information om din övergripande lösenordshygien: detta avser dubbletter av lösenord, svaga eller på annat sätt läckta lösenord eller e-postadresser.

Detta görs genom att jämföra listan med krypterade hash från Troys webbsida lokalt på din enhet för att kontrollera om den innehåller motsvarande hash för dina lösenord. Om en matchning hittas kommer du att meddelas för att uppmuntra dig att följaktligen ändra dina lösenord och andra inloggningsuppgifter.

För att komma åt **Säkerhetsrapport**, gå in i lösenordshanterarens gränssnitt och välj motsvarande knappen i den övre raden.

4.1.5. Synkronisera mellan andra plattformar

Genom att spara dina lösenord en gång i Bitdefender Password Manager kan du lagra och säkert komma åt dem på alla dina Windows-, Mac-, Android- eller iOS-enheter från Chrome, Safari, Firefox och Edge eller inuti mobilappar.

> **Notera**
> Bitdefender är också utrustad med en **offlineläge** för att komma åt dina lösenord, i händelse av att du inte råkar ha tillgång till internet. Detta gör dina lösenord tillgängliga när som helst och var som helst.

4.1.6. Ta bort en post

För att radera sparade lösenord tryck först på redigera-ikonen bredvid posten du vill ta bort, som finns i **konton** flik. Scrolla ner och välj sedan **Radera**. När du tillfrågas om du är säker på att du vill ta bort kontot väljer du **Avlägsna**.

4.2. Kontohantering

4.2.1. Autentisering

Autentiseringen i Bitdefender Password Manager görs genom **STIFT** ställs in i installationsprocessen av produkten. (Observera att **Auto lås** funktionen låser lösenordshanteraren eller loggar ut efter en period av inaktivitet på webbläsarnivå eller stängning av mobilappen)

Dessutom kan det också göras genom att använda biometri, om tillgängligt, som t.ex **Fingeravtryck** eller **Ansiktsupplåsning**.

Till **aktivera eller inaktivera** biometribaserad autentisering:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.

På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
Om du uppmanas anger du din Huvudlösenord.

2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
3. Klicka på **Enhetsinställningar**.
4. Här kommer du att märka en knapp som visar antingen **Inaktivera biometri** eller **Aktivera biometri**. Den här inställningen styr driftsstatusen för den biometribaserade autentiseringsfunktionen.

4.2.2. Återställ huvudlösenord

> **Viktig**
> De **Ändra huvudlösenord** funktionen är inte tillgänglig på mobila enheter. Det enda sättet du kan ändra eller återställa ditt huvudlösenord är via webbläsartillägget Bitdefender Password Manager på en Windows-dator eller en macOS-enhet.

Så här ändrar du din Huvudlösenord som en försiktighetsåtgärd och skapa en ny i Bitdefender Password Manager:

1. När du har installerat webbläsartillägget klickar du på **Lösenordshanteraren** ikonen i webbläsarens verktygsfält.
2. Ange ditt nuvarande huvudlösenord för att låsa upp valvet.

> **Viktig**
> Om du inte kommer ihåg det aktuella huvudlösenordet, klicka på **jag har glömt mitt lösenord** alternativet på samma skärm. Gå in i **24-siffrig återställningsnyckel** tillhandahålls under den initiala Bitdefender Password Manager-inställningen och skriv sedan ett nytt huvudlösenord. **Om du glömmer eller tar bort** både Huvudlösenord och den **återställningsnyckel**, som en sista utväg, **kontakta en Bitdefender-representant för att hjälpa dig att återställa ditt konto**. Återställa ditt konto kommer radera alla dina data och lösenord sparas i Bitdefender Password Manager.

3. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
4. Klicka på **Mitt konto** knappen i **konto** sektion.
5. Ett fönster med information om din Password Manager-prenumeration kommer att visas.

Klicka på **Ändra huvudlösenord** knapp.

6. Du omdirigeras till ett nytt fönster där du kan välja ett nytt huvudlösenord. Ange ditt nuvarande huvudlösenord och skriv sedan ett nytt huvudlösenord. Det nya huvudlösenordet måste innehålla minst 8 tecken, minst en liten bokstav, en stor bokstav och en siffra.
7. tryck på **Förändra** knappen när du är klar.
8. Vänta några ögonblick tills Bitdefender återställer det gamla huvudlösenordet.
   Lämna inte din webbläsare!
9. Därefter får du en ny **24-siffrig återställningsnyckel**. Anteckna återställningsnyckeln på en säker plats och **tappa den inte**. Den här nyckeln är det enda sättet att komma åt dina lösenord som sparats i Lösenordshanteraren om du glömmer huvudlösenordet.
   Tryck **Stänga** när du är klar.
10. Du kommer att loggas ut från Bitdefender Password Manager.
    För att låsa upp valvet, använd det nya huvudlösenordet du just angett.

4.3. Andra funktioner

4.3.1. Identitetshantering

Den här funktionen tillåter användare att lagra flera identiteter och låter Password Manager automatiskt fylla i detaljer i webbformulär innan de gör ett köp på ett snabbt, enkelt och säkert sätt.

Som allt annat i lösenordshanteraren är all känslig data som finns i dessa lagrade identiteter krypterad och endast tillgänglig för användarens enhet.

Så här lägger du till en identitet i lösenordshanteraren:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.
   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **Identiteter** menyalternativ.
3. Tryck på **Lägg till identitet** knappen längst ner.

4. Fyll i de uppgifter du vill lagra och tryck sedan på **Spara**.

4.3.2. Kreditkortshantering

Den här funktionen låter dig spara och fylla i kreditkortsuppgifter för enklare, snabbare och säkrare shopping.

Så här lägger du till ett kreditkort i lösenordshanteraren:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.
   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **Kreditkort** menyalternativ.
3. Tryck på **Lägg till identitet** knappen längst ner.
4. Fyll i de uppgifter du vill lagra och tryck sedan på **Spara**.

4.3.3. Säkra mig

Secure Me-funktionen låter dig logga ut på distans eller ta bort webbhistorik på din dator, surfplatta eller mobilenhet. Om du delar en enhet med andra rekommenderar vi starkt att du aktiverar den här funktionen.

Så här hittar du och aktiverar den här funktionen:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.
   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **Säkra mig** menyalternativ.
3. Tryck på **Säkra alla sessioner** knapp.
   Om du bara vill säkra en viss enhet, leta efter den i listan över enheter där lösenordshanteraren är installerad eller aktiverad i en specifik webbläsare.

4.3.4. Anteckningar

Secure Notes är en funktion som fungerar precis som en hemlig anteckningsbok där du kan lagra känslig data, sortera den och

använda färgkodning för att bättre visualisera den. Det håller inte bara informationen snygg, utan du håller den också säker och säker.

Så här hittar du och aktiverar den här funktionen:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.
   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **Anteckningar** menyalternativ.
3. Tryck på ⊕ **Lägg till anteckning** knapp.
   När du har skrivit ner den information du vill förvara trycker du på **Spara**.

5. VANLIGA FRÅGOR

Några vanliga frågor om Bitdefender Password Manager tenderar att återkomma. Vi har svaren! Här kan du lära dig mer om ditt Bitdefender-konto, import av lösenord, datasäkerhetsprotokoll och andra ämnen som är viktiga för våra kunder.

Allmänna frågor om Bitdefender Password Manager

Hur stoppar jag lösenordshanterarens popup-fönster i min Bitdefender-säkerhetslösning?

Lösenordshanterarens meddelande som visas av Bitdefender Total Security, Internet Security och Antivirus Plus i augusti 2022 kan avvisas genom att klicka på knappen "x". Fönstret "Hantera dina lösenord med Bitdefender Password Manager" kommer att dyka upp igen slumpmässigt ett par gånger innan det försvinner för alltid. Du kan välja bort detta reklammeddelande genom att växla**Rekommendationsmeddelanden**till avstängd position i Bitdefender-inställningarna.

Vad händer när Bitdefender Password Manager löper ut?

När din Password Manager-prenumeration löper ut och inte längre är aktiv har du högst 90 dagar på dig att exportera dina lösenord. Dina lösenord kommer att säkerhetskopieras i ytterligare 30 dagar. Under dessa 90 dagar kommer du bara att kunna exportera dina data. Du kan inte fortsätta använda lösenordshanteraren. Autofyll-funktionen slutar fungera, liksom möjligheten att generera lösenord.

I slutet av den 90-dagars respitperioden har du 30 extra dagar på dig att kontakta Bitdefender-supporten och begära att återställa dina lösenord till livedatabasen. Du kommer då att kunna exportera dina lösenord från Bitdefender Password Manager.

Dina data kommer endast att lagras i livedatabasen till slutet av dagen då de återställdes på begäran. Vid midnatt raderas databasen – och om du ännu inte har överskridit den extra 30-dagarsperioden kan lösenord återställas från backup. Rådatabasdata från säkerhetskopian kan tillhandahållas på begäran till användaren, men databasen är krypterad och informationen kan inte nås.

Vad är ett huvudlösenord och varför måste jag komma ihåg det?

Huvudlösenordet är nyckeln som låser upp dörren till alla lösenord som är lagrade i ditt Bitdefender Password Manager-konto. Huvudlösenordet måste vara minst 8 tecken långt. Så skapa ett starkt huvudlösenord, memorera det och dela det aldrig med någon. För att skapa ett starkt huvudlösenord rekommenderar vi att du använder en kombination av stora och små bokstäver, siffror och specialtecken (som #, $ eller @).

Hur kan jag hindra Bitdefender från att fråga efter mitt huvudlösenord varje gång jag öppnar webbläsaren?

Om du låser din enhet utan att stänga din webbläsare, låses inte Password Manager och du kan komma åt din data när du kommer tillbaka. Som en säkerhetsåtgärd, varje gång du öppnar webbläsaren måste du logga in med ditt Bitdefender Central-konto och sedan ange ditt huvudlösenord.

- För att stoppa den centrala inloggningsprompten, gå till ⚙ Inställningar och markera "Inaktivera inloggningsfliken vid start".
- För att stoppa uppmaningen av huvudlösenordet, markera rutan "Kom ihåg mig" på skärmen Lås upp ditt valv.

Varför sparar du inte mitt huvudlösenord, och vad händer om jag glömmer det?

Anledningen till att vi inte lagrar ditt huvudlösenord på våra servrar är så att bara du kan komma åt ditt konto. Det är det säkraste sättet. Om Bitdefender Password Manager inte känner igen ditt huvudlösenord, se till att du skriver det korrekt och att Caps Lock-tangenten inte är aktiv på tangentbordet.

Om du glömmer huvudlösenordet kan du alltid använda återställningsnyckeln för att låsa upp lösenordshanteraren. Under registreringsprocessen tillhandahåller Bitdefender Password Manager en **återställningsnyckel** som kan användas för att återfå åtkomst till kontot utan att förlora din data.

Om du glömmer eller tappar bort både huvudlösenordet och återställningsnyckeln, som en sista utväg, kontakta en Bitdefender-representant för att återställa ditt konto.

> **Viktig**
> Att återställa ditt konto kommer att radera alla dina data och lösenord som sparats i Bitdefender Password Manager.

Kan flera användare dela en Bitdefender Password Manager-prenumeration?

För närvarande är möjligheten att ha flera användare på samma Password Manager-prenumeration inte tillgänglig men vi arbetar på att aktivera den här funktionen inom en snar framtid.

Vad är offlineläge och hur fungerar det?

Offlineläge aktiveras automatiskt när Internetanslutningen sjunker när du använder Bitdefender Password Manager. Om du redan är inloggad och har angett ditt huvudlösenord, låter offlineläget dig komma åt dina lösenord när en internetanslutning är utom räckhåll.

Hur avinstallerar jag Bitdefender Password Manager?

För att avinstallera Bitdefender Password Manager:

- På Windows och macOS:
  Ta bort tillägget Password Manager från din webbläsare. Högerklicka på Bitdefender-ikonen och välj "Ta bort".
- På Android:
  Knacka och håll appen Password Manager och dra den till toppen av skärmen där det står "Avinstallera".
- På iOS och iPadOS:
  Tryck och håll appen Lösenordshanteraren tills alla appar på skärmen börjar vicka, tryck sedan på X:et uppe till vänster om Bitdefender-ikonen.

Sekretess- och säkerhetsfrågor om Bitdefender Password Manager

Kan Bitdefender-anställda se mina lösenord?

Absolut inte. Din integritet är vår högsta prioritet. Detta är huvudorsaken till att vi inte lagrar ditt huvudlösenord på våra dataservrar: så att ingen har tillgång till ditt konto, inte ens företagets anställda. Varje lösenord och konto är mycket krypterade med den starkaste datasäkerhetsalgoritmen, och koden vi ser ser helt enkelt ut som en slumpmässig sträng av siffror och bokstäver som blandas ihop.

Vad skulle hända om lösenordshanterarens servrar hackades?

Varje lösenord krypteras lokalt på din enhet innan det kommer någonstans i närheten av våra servrar, så om hackare skulle bryta sig in i vårt system skulle de bara få sidor med slumpmässiga bokstäver och siffror utan din

nyckel för att dekryptera dem. Det betyder att du och dina kontouppgifter alltid är säkra hos oss.

6. FÅ HJÄLP

6.1. Ber om hjälp

Bitdefender ger sina kunder en oöverträffad nivå av snabb och exakt support. Om du upplever några problem eller om du har några frågor om din Bitdefender-produkt, kan du använda flera onlineresurser för att hitta en lösning eller ett svar. Samtidigt kan du kontakta Bitdefender Customer Care-teamet. Våra supportrepresentanter kommer att svara på dina frågor i tid och ge dig den hjälp du behöver.

6.2. Onlineresurser

Flera onlineresurser finns tillgängliga för att hjälpa dig att lösa dina Bitdefender-relaterade problem och frågor.

- Bitdefender Support Center:
  https://www.bitdefender.se/consumer/support/
- Bitdefender Expert Community:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Du kan också använda din favoritsökmotor för att ta reda på mer information om datorsäkerhet, Bitdefender-produkterna och företaget.

6.2.1. Bitdefender Support Center

Bitdefender Support Center är ett onlineförråd med information om Bitdefender-produkterna. Den lagrar, i ett lättillgängligt format, rapporter om resultaten av den pågående tekniska supporten och buggfixningsaktiviteterna för Bitdefender-support- och utvecklingsteamen, tillsammans med mer allmänna artiklar om hotförebyggande, hantering av Bitdefender-lösningar med detaljerade förklaringar och många andra artiklar.

Bitdefender Support Center är öppet för allmänheten och fritt sökbart. Den omfattande informationen den innehåller är ytterligare ett sätt att förse Bitdefender-kunder med den tekniska kunskap och insikt de behöver. Alla giltiga förfrågningar om information eller buggrapporter

som kommer från Bitdefender-klienter hittar så småningom vägen till Bitdefender Support Center, som bugfixrapporter, fuskblad för lösningar eller informationsartiklar för att komplettera produkthjälpfiler.

Bitdefender Support Center är tillgängligt när som helst på följande adress: https://www.bitdefender.se/consumer/support/.

6.2.2. Bitdefender Expert Community

Expertgemenskapen är en miljö där Bitdefender-användare, entusiaster och fans kan engagera sig, utbyta idéer, stödja varandra och dela sina kunskaper och lösningar. Det är också en plats för idéer och ger värdefull feedback till våra utvecklingsteam. Community-medlemmarna är erfarna Bitdefender-användare som gärna hjälper andra kamrater på sin egen tid. Med deras enorma bidrag och genuina frivilliga insatser har vi skapat en kunskapsbas där användare kan hitta svar och vägledning, men med den mänskliga touchen.

Här hittar du meningsfulla konversationer med personer som använder Bitdefender på sina enheter. Gemenskapen erbjuder en sann kontakt med våra medlemmar och gör din röst hörd. Det är en plats där du uppmuntras att delta i vetskapen om att din åsikt och din input respekteras och omhuldas. Som en uppskattad leverantör strävar vi efter att erbjuda en oöverträffad nivå av snabb, exakt support och vi vill föra våra användare närmare oss. Vi har utformat vår community med detta syfte i åtanke.

Du hittar vår webbsida för expertgemenskapen här:

https://community.bitdefender.com/en/

6.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia har all information du behöver om de senaste cyberhoten. Det här är platsen där Bitdefender-experter delar med sig av tips och tricks om hur man kan hålla sig skyddad från hackare, dataintrång, identitetsstöld och sociala identitetsförsök.

Bitdefender Cyberpedias webbsida finns här:

https://www.bitdefender.com/cyberpedia/.

6.3. Kontaktinformation

Effektiv kommunikation är nyckeln till ett framgångsrikt företag. Sedan 2001 har BITDEFENDER etablerat ett obestridligt rykte genom att ständigt

sträva efter bättre kommunikation för att överträffa våra kunders och partners förväntningar. Om du har några frågor, tveka inte att kontakta oss direkt via vår Bitdefender Support Center (sida 26).

https://www.bitdefender.se/consumer/support/

6.3.1. Lokala distributörer

Bitdefender lokala distributörer är redo att svara på alla förfrågningar om deras verksamhetsområden, både i kommersiella och allmänna frågor.

Så här hittar du en Bitdefender-distributör i ditt land:

1. Gå till https://www.bitdefender.com/partners/partner-locator.html.
2. Välj ditt land och din stad med hjälp av motsvarande alternativ.

ORDLISTA

Aktiveringskod

Är en unik nyckel som kan köpas från detaljhandeln och användas för att aktivera en specifik produkt eller tjänst. En aktiveringskod möjliggör aktivering av ett giltigt abonnemang under en viss tidsperiod och antal enheter och kan även användas för att förlänga ett abonnemang med villkoret att genereras för samma produkt eller tjänst.

ActiveX

ActiveX är en modell för att skriva program så att andra program och operativsystemet kan anropa dem. ActiveX-teknik används med Microsoft Internet Explorer för att skapa interaktiva webbsidor som ser ut och beter sig som datorprogram, snarare än statiska sidor. Med ActiveX kan användare ställa eller svara på frågor, använda tryckknappar och interagera på andra sätt med webbsidan. ActiveX-kontroller skrivs ofta med Visual Basic. Active X är anmärkningsvärt för en fullständig brist på säkerhetskontroller; datorsäkerhetsexperter avråder från att använda det över internet.

Avancerat ihållande hot

Advanced persistent hot (APT) utnyttjar sårbarheter i system för att stjäla viktig information för att leverera den till källan. Stora grupper som organisationer, företag eller regeringar är föremål för detta hot. Målet med ett avancerat ihållande hot är att förbli oupptäckt under lång tid och kunna övervaka och samla in viktig information utan att skada de riktade maskinerna. Metoden som används för att injicera hotet i nätverket är genom en PDF-fil eller ett Office-dokument som ser ofarliga ut så att alla användare kan köra filerna.

Reklamprogram

Adware kombineras ofta med en värdapp som tillhandahålls utan kostnad så länge som användaren accepterar adware. Eftersom adware-appar vanligtvis installeras efter att användaren har godkänt ett licensavtal som anger syftet med appen, begås inget brott. Men popup-annonser kan bli irriterande och i vissa fall försämra systemets prestanda. Dessutom kan informationen som vissa av dessa appar samlar in orsaka integritetsproblem för användare som inte var fullt medvetna om villkoren i licensavtalet.

Arkiv

En disk, ett band eller en katalog som innehåller filer som har säkerhetskopierats.

En fil som innehåller en eller flera filer i ett komprimerat format.

Bakdörr

Ett hål i säkerheten i ett system som medvetet lämnats på plats av designers eller underhållare. Motivationen för sådana hål är inte alltid olycksbådande; vissa operativsystem, till exempel, kommer ur lådan med privilegierade konton avsedda att användas av fältservicetekniker eller säljarens underhållsprogrammerare.

Boot sektor

En sektor i början av varje disk som identifierar diskens arkitektur (sektorstorlek, klusterstorlek, och så vidare). För startdiskar innehåller bootsektorn även ett program som laddar operativsystemet.

Boot virus

Ett hot som infekterar startsektorn på en fast eller diskett. Ett försök att starta från en diskett som är infekterad med ett bootsektorvirus gör att hotet blir aktivt i minnet. Varje gång du startar ditt system från den tidpunkten kommer du att ha hotet aktivt i minnet.

Botnet

Termen "botnät" är sammansatt av orden "robot" och "nätverk". Botnät är internetanslutna enheter som är infekterade med hot och kan användas för att skicka skräppost, stjäla data, fjärrstyra sårbara enheter eller sprida spionprogram, ransomware och andra typer av hot. Deras mål är att infektera så många uppkopplade enheter som möjligt, såsom datorer, servrar, mobila eller IoT-enheter som tillhör stora företag eller industrier.

Webbläsare

Förkortning för webbläsare, en programvaruapp som används för att hitta och visa webbsidor. Populära webbläsare inkluderar Microsoft Internet Explorer, Mozilla Firefox och Google Chrome. Dessa är grafiska webbläsare, vilket innebär att de kan visa grafik såväl som text. Dessutom kan de flesta moderna webbläsare presentera multimediainformation, inklusive ljud och video, även om de kräver plugin-program för vissa format.

Brute Force Attack

Lösenordsgissningsattack används för att bryta sig in i ett datorsystem genom att ange möjliga lösenordskombinationer, oftast med det enklast att gissa lösenordet.

Kommandorad

I ett kommandoradsgränssnitt skriver användaren kommandon i utrymmet som tillhandahålls direkt på skärmen med hjälp av kommandospråk.

Småkakor

Inom internetbranschen beskrivs cookies som små filer som innehåller information om enskilda datorer som kan analyseras och användas av annonsörer för att spåra dina intressen och smaker online. I det här området utvecklas fortfarande cookieteknologi och avsikten är att rikta annonser direkt till det du har sagt att dina intressen är. Det är ett tveeggat svärd för många människor eftersom det å ena sidan är effektivt och relevant eftersom du bara ser annonser om det du är intresserad av. Å andra sidan handlar det faktiskt om att "spåra" och "följa" vart du går och vad du klickar på. Det är förståeligt nog att det finns en debatt om integritet och många känner sig kränkta av uppfattningen att de ses som ett "SKU-nummer" (ni vet, streckkoden på baksidan av paketen som skannas vid utcheckningslinjen) . Även om denna synpunkt kan vara extrem, är den i vissa fall korrekt.

Cybermobbning

När kamrater eller främlingar begår kränkande handlingar mot barn med avsikt för att fysiskt skada dem. För att skada känslomässigt skickar angriparna elaka meddelanden eller föga smickrande bilder, vilket gör att deras offer isolerar sig från andra eller känner sig frustrerade.

Ordbok Attack

Lösenordsgissningsattacker används för att bryta sig in i ett datorsystem genom att ange en kombination av vanliga ord för att generera potentiella lösenord. Samma metod används för att gissa dekrypteringsnycklar för krypterade meddelanden eller dokument. Ordboksattacker lyckas eftersom många människor är benägna att välja korta och enstaka ordlösenord som är lätta att gissa.

Diskenhet

Det är en maskin som läser data från och skriver data till en disk. En hårddisk läser och skriver hårddiskar. En diskettenhet får åtkomst till

disketter. Diskenheter kan antingen vara interna (inrymd i en dator) eller externa (inrymd i en separat låda som ansluts till datorn).

Ladda ner

Att kopiera data (vanligtvis en hel fil) från en huvudkälla till en kringutrustning. Termen används ofta för att beskriva processen att kopiera en fil från en onlinetjänst till sin egen dator. Nedladdning kan också syfta på att kopiera en fil från en nätverksfilserver till en dator i nätverket.

E-post

E-post. En tjänst som skickar meddelanden på datorer via lokala eller globala nätverk.

evenemang

En åtgärd eller händelse som upptäckts av ett program. Händelser kan vara användaråtgärder, som att klicka på en musknapp eller trycka på en tangent, eller systemhändelser, som att minnet blir slut.

Utnyttjar

Ett sätt att dra nytta av olika buggar eller sårbarheter som finns i en dator (mjukvara eller hårdvara). Således kan hackare få kontroll över datorer eller nätverk.

Falskt positivt

Uppstår när en skanner identifierar en fil som infekterad när den faktiskt inte är det.

Filnamnstillägg

Den del av ett filnamn, efter den sista punkten, som anger vilken typ av data som lagras i filen. Många operativsystem använder filnamnstillägg, t.ex. Unix, VMS och MS-DOS. De är vanligtvis från en till tre bokstäver (vissa tråkiga gamla operativsystem stöder inte mer än tre). Exempel inkluderar "c" för C-källkod, "ps" för PostScript, "txt" för godtycklig text.

Heuristisk

En regelbaserad metod för att identifiera nya hot. Denna metod för skanning är inte beroende av specifik databas med hotinformation. Fördelen med den heuristiska skanningen är att den inte luras av en ny variant av ett befintligt hot. Det kan dock ibland rapportera misstänkt kod i vanliga program, vilket genererar den så kallade "falska positiva".

Honungsburk

Ett lockdatorsystem som lockar hackare att studera hur de agerar och identifiera de kätterska metoder de använder för att samla in systeminformation. Företag och företag är mer intresserade av att implementera och använda honeypots för att förbättra sin övergripande säkerhet.

IP

Internet Protocol - Ett routbart protokoll i TCP/IP-protokollsviten som ansvarar för IP-adressering, routing och fragmentering och återmontering av IP-paket.

Java applet

Ett Java-program som är designat för att endast köras på en webbsida. För att använda en applet på en webbsida skulle du ange namnet på appleten och storleken (längd och bredd, i pixlar) som appleten kan använda. När webbsidan nås laddar webbläsaren ner appleten från en server och kör den på användarens dator (klienten). Applets skiljer sig från appar genom att de styrs av ett strikt säkerhetsprotokoll.

Till exempel, även om appletar körs på klienten, kan de inte läsa eller skriva data på klientens dator. Dessutom är appletar ytterligare begränsade så att de bara kan läsa och skriva data från samma domän som de betjänas från.

Keylogger

En keylogger är en app som loggar allt du skriver. Keyloggers är inte skadliga till sin natur. De kan användas för legitima ändamål, som att övervaka anställda eller barnaktivitet. De används dock i allt högre grad av cyberbrottslingar i skadliga syften (till exempel för att samla in privata uppgifter, såsom inloggningsuppgifter och personnummer).

Makrovirus

En typ av datorhot som är kodat som ett makro inbäddat i ett dokument. Många appar, som Microsoft Word och Excel, stöder kraftfulla makrospråk. Dessa appar låter dig bädda in ett makro i ett dokument och få makrot att köras varje gång dokumentet öppnas.

E-postklient

En e-postklient är en app som gör att du kan skicka och ta emot e-post.

Minne

Interna lagringsutrymmen i datorn. Termen minne identifierar datalagring som kommer i form av chips, och ordet lagring används för minne som finns på band eller diskar. Varje dator kommer med en viss mängd fysiskt minne, vanligtvis kallat huvudminne eller RAM.

Icke-heuristisk

Denna metod för skanning bygger på specifik databas med hotinformation. Fördelen med den icke-heuristiska skanningen är att den inte luras av vad som kan tyckas vara ett hot och inte genererar falsklarm.

Rovdjur online

Individer som försöker locka minderåriga eller tonåringar till konversationer med avsikt att involvera dem i illegala sexuella aktiviteter. Sociala nätverk är den idealiska platsen där utsatta barn lätt kan jagas och förföras till att begå sexuella aktiviteter, online eller ansikte mot ansikte.

Packade program

En fil i ett komprimeringsformat. Många operativsystem och appar innehåller kommandon som gör att du kan packa en fil så att den tar mindre minne. Anta till exempel att du har en textfil som innehåller tio på varandra följande mellanslagstecken. Normalt skulle detta kräva tio byte lagring.

Ett program som packar filer skulle dock ersätta mellanslagstecken med ett speciellt mellanslagsserietecken följt av antalet mellanslag som ersätts. I detta fall skulle de tio utrymmena endast kräva två byte. Detta är bara en packningsteknik - det finns många fler.

Väg

Den exakta vägbeskrivningen till en fil på en dator. Dessa riktningar beskrivs vanligtvis med hjälp av det hierarkiska arkiveringssystemet uppifrån och ner.

Rutten mellan två valfria punkter, till exempel kommunikationskanalen mellan två datorer.

Nätfiske

Handlingen att skicka ett e-postmeddelande till en användare som falskeligen påstår sig vara ett etablerat legitimt företag i ett försök att lura användaren till att överlämna privat information som kommer att användas för identitetsstöld. E-postmeddelandet uppmanar användaren att besöka

en webbplats där de ombeds att uppdatera personlig information, såsom lösenord och kreditkort, personnummer och bankkontonummer, som den legitima organisationen redan har. Webbplatsen är dock falsk och inrättad endast för att stjäla användarens information.

Foton

Photon är en innovativ, icke-påträngande Bitdefender-teknik, designad för att minimera prestandapåverkan från din säkerhetslösning. Genom att övervaka din dators aktivitet i bakgrunden skapar den användningsmönster som hjälper till att optimera uppstarts- och skanningsprocesser.

Polymorft virus

Ett hot som ändrar form för varje fil som den infekterar. Eftersom de inte har något konsekvent binärt mönster är sådana hot svåra att identifiera.

Hamn

Ett gränssnitt på en dator som du kan ansluta en enhet till. Persondatorer har olika typer av portar. Internt finns det flera portar för att ansluta diskenheter, bildskärmar och tangentbord. Externt har persondatorer portar för anslutning av modem, skrivare, möss och annan kringutrustning.

I TCP/IP- och UDP-nätverk, en slutpunkt till en logisk anslutning. Portnumret identifierar vilken typ av port det är. Till exempel används port 80 för HTTP-trafik.

Ransomware

Ransomware är ett skadligt program som försöker tjäna pengar på användare genom att låsa deras sårbara system. CryptoLocker, CryptoWall och TeslaWall, är bara några varianter som jagar användarnas personliga system.

Infektionen kan spridas genom att komma åt skräppostmeddelanden, ladda ner e-postbilagor eller installera appar, utan att låta användaren veta vad som händer på hans system. Dagliga användare och företag riktas mot ransomware-hackare.

Rapportfil

En fil som listar åtgärder som har inträffat. Bitdefender har en rapportfil som visar sökvägen som skannats, mapparna, antalet skannade arkiv och filer, hur många infekterade och misstänkta filer som hittades.

Rootkit

Ett rootkit är en uppsättning mjukvaruverktyg som ger åtkomst till ett system på administratörsnivå. Termen användes först för UNIX-operativsystemen och den hänvisade till omkompilerade verktyg som gav inkräktare administrativa rättigheter, så att de kunde dölja sin närvaro så att de inte syns av systemadministratörerna.

Den huvudsakliga rollen för rootkits är att dölja processer, filer, inloggningar och loggar. De kan också fånga upp data från terminaler, nätverksanslutningar eller kringutrustning, om de innehåller lämplig programvara.

Rootkits är inte skadliga till sin natur. Till exempel döljer system och till och med vissa appar viktiga filer med rootkits. Men de används mest för att dölja hot eller för att dölja närvaron av en inkräktare i systemet. I kombination med hot utgör rootkits ett stort hot mot integriteten och säkerheten i ett system. De kan övervaka trafik, skapa bakdörrar i systemet, ändra filer och loggar och undvika upptäckt.

Manus

En annan term för makro- eller batchfil, ett skript är en lista med kommandon som kan köras utan användarinteraktion.

Spam

Elektronisk skräppost eller skräpnyhetsgrupper. Allmänt känd som all oönskad e-post.

Spionprogram

All programvara som i hemlighet samlar in användarinformation via användarens internetanslutning utan hans eller hennes vetskap, vanligtvis i reklamsyfte. Spionprogram är vanligtvis paketerade som en dold komponent av gratisprogram eller shareware-program som kan laddas ner från internet; Det bör dock noteras att majoriteten av shareware och freeware-appar inte kommer med spionprogram. När det väl har installerats övervakar spionprogrammet användaraktivitet på internet och överför informationen i bakgrunden till någon annan. Spionprogram kan också samla information om e-postadresser och till och med lösenord och kreditkortsnummer.

Spionprograms likhet med ett trojansk hästhot är det faktum att användare omedvetet installerar produkten när de installerar något annat. Ett vanligt sätt att bli offer för spionprogram är att ladda ner vissa peer-to-peer filbytesprodukter som är tillgängliga idag.

Bortsett från frågorna om etik och integritet stjäl spionprogram från användaren genom att använda datorns minnesresurser och även genom att äta bandbredd då det skickar information tillbaka till spionprogrammets hembas via användarens internetanslutning. Eftersom spionprogram använder minne och systemresurser kan apparna som körs i bakgrunden leda till systemkrascher eller allmän systeminstabilitet.

Startobjekt

Alla filer som placeras i den här mappen öppnas när datorn startar. Till exempel kan en startskärm, en ljudfil som ska spelas upp när datorn startar, en påminnelseskalender eller appar vara startobjekt. Normalt placeras ett alias för en fil i den här mappen istället för själva filen.

Prenumeration

Köpeavtal som ger användaren rätt att använda en viss produkt eller tjänst på ett visst antal enheter och under en viss tid. Ett utgånget abonnemang kan förnyas automatiskt med den information som användaren lämnade vid första köpet.

Systemfältet

Systemfältet, som introducerades med Windows 95, finns i aktivitetsfältet i Windows (vanligtvis längst ner bredvid klockan) och innehåller miniatyrikoner för enkel åtkomst till systemfunktioner som fax, skrivare, modem, volym med mera. Dubbelklicka eller högerklicka på en ikon för att visa och komma åt detaljerna och kontrollerna.

TCP/IP

Transmission Control Protocol/Internet Protocol - En uppsättning nätverksprotokoll som ofta används på internet som tillhandahåller kommunikation över sammankopplade nätverk av datorer med olika hårdvaruarkitekturer och olika operativsystem. TCP/IP innehåller standarder för hur datorer kommunicerar och konventioner för att ansluta nätverk och dirigera trafik.

Hot

Ett program eller kod som läses in på din dator utan din vetskap och som körs mot din vilja. De flesta hot kan också replikera sig själva. Alla datorhot är konstgjorda. Ett enkelt hot som kan kopiera sig själv om och om igen är relativt lätt att producera. Även ett så enkelt hot är farligt eftersom det snabbt kommer att använda allt tillgängligt minne och få systemet att

stanna. En ännu farligare typ av hot är en som kan överföra sig själv över nätverk och kringgå säkerhetssystem.

Uppdatering av hotinformation

Det binära mönstret för ett hot, som används av säkerhetslösningen för att upptäcka och eliminera hotet.

Trojan

Ett destruktivt program som maskerar sig som en godartad app. Till skillnad från skadliga program och maskar replikerar trojaner inte sig själva men de kan vara lika destruktiva. En av de mest lömska typerna av trojanska hästhot är ett program som påstår sig befria din dator från hot men istället introducerar hot på din dator.

Termen kommer från en berättelse i Homeros Iliaden, där grekerna ger en gigantisk trähäst till sina fiender, trojanerna, skenbart som ett fredsoffer. Men efter att trojanerna släpat hästen innanför sina stadsmurar, smyger grekiska soldater ut ur hästens ihåliga mage och öppnar stadsportarna, så att deras landsmän kan strömma in och fånga Troja.

Uppdatering

En ny version av en mjuk- eller hårdvaruprodukt utformad för att ersätta en äldre version av samma produkt. Dessutom kontrollerar installationsrutinerna för uppdateringar ofta att en äldre version redan är installerad på din dator; Om inte kan du inte installera uppdateringen.

Bitdefender har sin egen uppdateringsfunktion som låter dig söka manuellt efter uppdateringar, eller låta den uppdatera produkten automatiskt.

Virtual Private Network (VPN)

Är en teknik som möjliggör en tillfällig och krypterad direktanslutning till ett visst nätverk över ett mindre säkert nätverk. På så sätt är det säkert och krypterat att skicka och ta emot data, svårt att fångas av snokare. Ett bevis på säkerhet är autentiseringen, som endast kan göras med ett användarnamn och lösenord.

Mask

Ett program som sprider sig över ett nätverk och reproducerar sig själv allt eftersom. Den kan inte koppla sig till andra program.