+ Windows 10

HANDBOK FÖR INTERNETSÄKERHET

Tio åtgärder som alla företag bör vidta för att skydda sig mot nätattacker.

Var säkrare från start till avstängning.

Nätmiljön förändras och utökas hela tiden. Små och mellanstora företag måste hantera allt fler nätattacker som hotar deras information och deras kunders privata uppgifter. Den här handboken har utformats för att hjälpa sådana små och mellanstora företag med begränsade IT-resurser att stärka nätsäkerheten, till låg eller ingen kostnad.

INNEHÅLLSFÖRTECKNING

Befintliga hot

Nätsäkerhetstrender i små och mellanstora företag

Dessa är de fem vanligaste trenderna när det gäller internetsäkerhet för små och mellanstora företag, i enlighet med Ponemon Institute[1]:

1. **Fler företag attackeras.**
Under de senaste 12 månaderna har internetattacker på små och mellanstora företag ökat med 11 % från 55 till 61 %. De vanligaste attackerna mot mindre företag är nätfiske/social ingenjörskonst (48 %) och webbaserade attacker (43 %). Samtidigt blir nätattackerna mer målinriktade, allvarliga och sofistikerade.

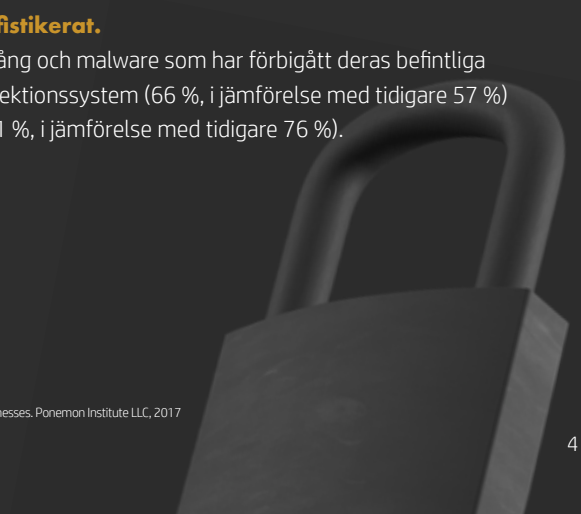
2. **Attackerna blir dyrare.**
Den genomsnittliga kostnaden för driftavbrotten ökade med 26 % från 955 429 USD till 1 207 965 USD. Den genomsnittliga kostnaden på grund av skador på eller stöld av IT-tillgångar eller infrastruktur ökade från 879 582 USD till 1 027 053 USD.

3. **Den mänskliga faktorn är den främsta orsaken.**
Av alla små och mellanstora företag där ett dataintrång skedde anger 54 % att vårdslöshet från medarbetarnas sida var en grundläggande orsak – en ökning på 48 % i jämförelse med förra året. I likhet med förra året kunde dock 1 av 3 företag i den här undersökningen inte avgöra vad som orsakat det.

4. **Starka lösenord och multifaktorsautentisering används fortfarande inte i tillräckligt hög grad.**
Lösenord fortsätter att vara en viktig del av internetsäkerheten. Trots detta säger 59 % av de svarande att de inte har någon insyn i de anställdas lösenordsrutiner, som t.ex. användning av unika eller starka lösenord eller att dela lösenord med andra – vilket är oförändrat i jämförelse med förra året.

> 59 % säger att de inte har någon insyn i de anställdas lösenordsrutiner

5. **Malware blir allt mer sofistikerat.**
Fler företag blir offer för intrång och malware som har förbigått deras befintliga skydd, som t.ex. intrångsdetektionssystem (66 %, i jämförelse med tidigare 57 %) och virusskyddslösningar (81 %, i jämförelse med tidigare 76 %).



1 – Rapport: 2017 State of Cybersecurity in Small & Medium-Sized Businesses. Ponemon Institute LLC, 2017

De fem vanligaste attackerna mot små och mellanstora företag.

1

Nätfiske/social manipulation

Attacker med social manipulation innebär att man använder mänsklig interaktion för att komma över information om ett företag eller dess datorsystem. Till exempel kan angriparen utge sig för att vara en ny medarbetare, en tekniker eller en forskare. Genom att ställa frågor kan han eller hon lyckas samla tillräckligt med information för att kunna infiltrera företagets nätverk.[2]

Nätfiske är en form av social manipulation. I en nätfiskeattack låtsas angriparen tillhöra ett pålitligt företag och använder e-post eller illasinnade webbplatser för att be om personlig information.[2]

2

Webbaserade attacker

I webbaserade attacker får angriparen åtkomst till en legitim webbplats och lägger upp malware. Den legitima webbplatsen agerar som en parasitvärd och infekterar icke ont anande besökare. En av de lömskaste typerna av webbaserade attacker är en ”drive-by-download”, där illasinnat innehåll laddas ner till användarens dator när användaren besöker webbplatsen. För detta krävs ingen användarinteraktion.[3]

3

Malware

Malware är en bred term som hänvisar till all programvara som har utformats avsiktligt för att orsaka skada på en enhet eller ett nätverk[4] Detta inkluderar virus, spionprogram, ransomware och liknande typ av programvara. Utöver webbaserade attacker kan de även ta sig in på offrets dator via ett USB-minne eller en kompromitterad nätverksanslutning.[5]

4

Kompromitterade/stulna enheter

En kompromitterad eller stulen enhet kan innehålla både värdefull information och lokalt lagrade uppgifter som möjliggör ytterligare intrång i företagets information eller nätverk. Svaga lösenord och datakryptering kan ytterligare förvärra effekterna av den här typen av attacker.

5

Denial of service-attacker

Funktionsförlust uppnås genom att man överbelastar ett nätverk med trafik tills det inte längre kan svara eller helt enkelt kraschar, vilket förhindrar åtkomst från legitima användare. En distribuerad denial of service-attack (DDoS) inträffar när flera datorer samarbetar för att attackera ett mål och därmed ökar kraften i attacken. DDoS försvårar också möjligheten att hitta den verkliga källan till attacken.[6]

2 – https://www.us-cert.gov/ncas/tips/ST04-014

3 – https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/web-based-attacks-09-en.pdf

4 – https://technet.microsoft.com/en-us/library/dd632948.aspx

5 – https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CaseStudy-002.pdf

6 – https://www.us-cert.gov/ncas/tips/ST04-015

Tio sätt att skydda sig

Avsnitt 1:

Aktivera multifaktorautenti-sering

Användarnamn och lösenord är viktiga mål för hackare och det finns goda skäl till detta – din identitet är din mest värdefulla tillgång. Starka och säkra lösenord gör mycket, men enbart lösenord är inte den allra säkraste autentiseringsmekanismen. I en värld där det finns allt fler kommersiella hackare kan tjuvar som inte själva är experter anlita andra för att utföra sådana uppgifter. Hackare kan bygga speciell maskinvara som har utformats för att cracka lösenord, hyra utrymme från molntjänstleverantörer eller skapa ett botnät för att göra bearbetningen.

- 90 % av alla data som stjäls genom nätfiske är användaruppgifter [7]
- 80–90 % av alla lösenord kan hackas på mindre än 24 timmar[8]

För multifaktorautentisering krävs att du använder två eller flera oberoende inloggningsuppgifter för att identifiera dig, vilket ökar säkerhetsnivån avsevärt. Inloggningsuppgifter kan vara någonting som användaren **känner till** (lösenord eller PIN-koder), någonting användaren **har** (Bluetooth®-telefoner eller smartkort) eller någonting användaren **är** (igenkänning av ansikte eller fingeravtryck). Om en av faktorerna komprometteras eller intrång görs, måste angriparen även ta sig förbi nästa hinder.

HP MFA och Intel® Authenticate möjliggör båda flera autentiseringsfaktorer som krävs för varje inloggningsförsök.

7 – Verizon, 2016 Data Breach Investigations Report, 2016
8 – Källa: Brian Contos, CISO at Verodin, Inc. Citerat med tillstånd. https://www.csoonline.com/article/3236716/authentication/how-hackers-crack-passwords and-why-you-cant-stop-them.html

Konfigurera multifaktorautentisering med HP.

Moderna HP Pro- eller Elite-enheter har stöd för konfiguration av MFA genom HP:s Client Security Manager.[9]

1. Öppna Client Security Manager (du behöver administratörsbehörighet för att göra detta). Om du öppnar den i HP:s Manageability Integration Kit (MIL) kan du införa dina MFA-policyn för alla datorer på företaget.[10]
2. Från instrumentpanelen klickar du på Standardinställningar.
3. Välj de två eller tre faktorer som du vill konfigurera en inloggningspolicy för och följ anvisningarna som följer för att registrera inloggningsuppgifterna – som t.ex. att läsa in ett fingeravtryck från datorns fingeravtryckläsare eller ange en PIN-kod.

Diversifiera med Windows Hello.

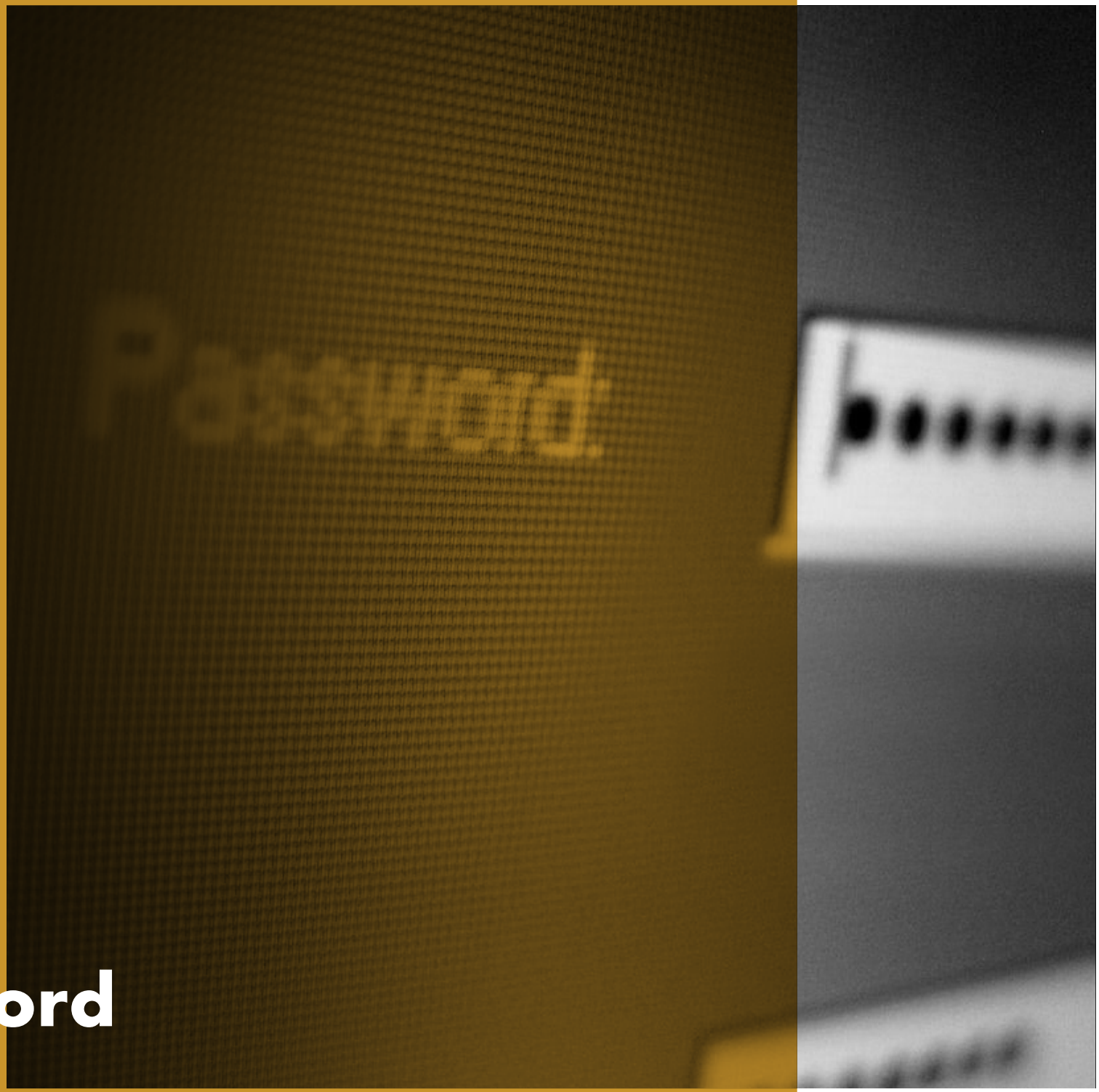
Många moderna Windows 10 Pro-enheter med en inbyggd webbkamera är kompatibla med Windows Hello, detta inkluderar hela utbudet av bärbara och konvertibla datorer från HP. Windows Hello erbjuder ansiktsigenkänning som ett alternativ till lösenord som en av dina MFA-inloggningsuppgifter.

1. Öppna Inställningar > Konton > Inloggningsalternativ
2. Under ”PIN” väljer du ”Lägg till” om du inte redan har ställt in detta.
3. Under ”Windows Hello” väljer du ”Konfigurera” och följer anvisningarna på skärmen för att läsa in ditt ansikte.

9 – För HP Client Security Manager Gen4 krävs Windows 8:e generationens Intel®- eller AMD-processorer.
10 – HP Manageability Integration Kit kan hämtas från http://www.hp.com/go/clientmanagement.

Avsnitt 2:

Stärk dina lösenord



Lösenord används flitigt i vår vardag. Vi använder dem för praktiskt taget alla privata och professionella enheter, tjänster och konton. Eftersom de utgör den första – och alldeles för ofta den enda – försvarslinjen för att skydda vår identitet och data kan användning av dåliga lösenord få förödande effekter. Trots detta använder många varken starka eller unika lösenord.

- 59 % vet att säkra lösenord är viktiga, men endast 41 % väljer ett lösenord som är enkelt att komma ihåg
- 91 % förstår risken med att återanvända lösenord, men 55 % gör det ändå
- Millenniegenerationen använder oftast starkare lösenord än babyboomgenerationen (65 % mot 45 %)[11]

Om enheten eller tjänsten inte har stöd för MFA, är det näst bästa alternativet att se till att lösenordet som används får jobba så hårt som möjligt. De flesta använder inte starka lösenord eftersom de inte vet hur de ska skapa dem. De kanske tror att det måste vara en slumpmässig kombination av bokstäver, siffror och symboler. Men det finns starkare och enklare sätt att förbättra lösenordsskyddet dramatiskt.

11 – Källa: LastPass, "New Research: Psychology of Passwords, Neglect is Helping Hackers Win", Katie Petrillo, May 1, 2018

Minnesteknik framför numeriska lösenord.

Minnestekniska lösenordsfraser är säkrare än enskilda lösenord och lättare att komma ihåg än numeriska lösenord.
När de används istället för ett enskilt lösenord är minnestekniska lösenordsfraser praktiskt taget omöjliga att lösa för en hacker.

1 Börja med en mening som är lätt att komma ihåg.

Du kan till exempel använda ett talesätt som ”Alla goda ting är 3” som en enkel lösenordsfras. Denna fras kan uppfylla majoriteten av alla lösenordsstandarder: Den är 8–32 tecken lång och inkluderar stora och små bokstäver samt ett specialtecken (mellanslagen – eller understreck om mellanslag inte tillåts).

2 Maximera konstigheten.

Öka antalet siffror och specialtecken som används. Du kan till exempel ändra bokstäverna i det tidigare exemplet så att det står: "@ll@ Goda Ting är 3".

3 Anpassa, kopiera inte.

Genom att helt enkelt kombinera tillägg av ett enkelt suffix till slutet av varje lösenordsfras kan du återanvända masterlösenordet på ett enkelt sätt utan den säkerhetsrisk som dubblettlösenord innebär. Du kan till exempel lägga till ”FB” i slutet av lösenordet för ett Facebook-konto och ”IG” för Instagram.

Använd en lösenordshanterare.

Lösenordshanterare är en av de bästa säkerhetsrutinerna och rekommenderas av säkerhetsexperter. De genererar och lagrar långa, komplicerade lösenord för vart och ett av dina konton – så att du inte behöver komma ihåg dem själv. I allmänhet behöver du då bara komma ihåg ett lösenord, huvudlösenordet till ”valvet”. Det är enkelt att konfigurera en lösenordshanterare och processen går vanligtvis till på samma sätt:

1. Hämta och installera programvaran och ett tillägg till webbläsaren. Du kan också hämta en app för din mobila enhet.
2. Konfigurera ett konto med en e-postadress och huvudlösenordet.
3. Lägg in uppgifterna för dina olika konton.

De flesta lösenordshanterare kräver att du uppdaterar dina gamla lösenord manuellt: logga in på kontot, gå till kontoinställningarna och låt lösenordshanteraren generera ett nytt, säkrare lösenord. Att ersätta ditt gamla svaga lösenord kan ta tid, men det innebär en avsevärd förbättring av säkerheten så det är värt det.

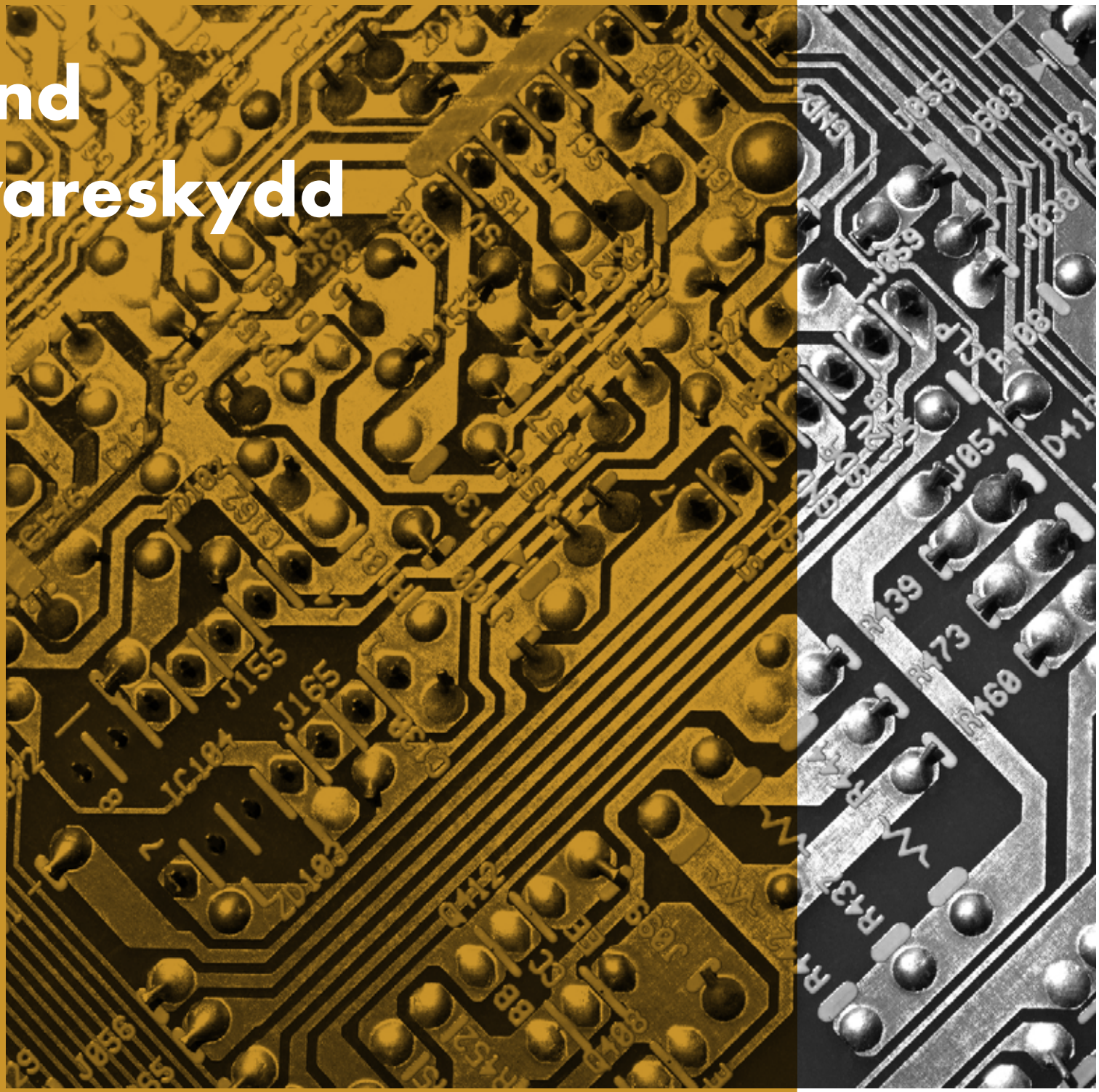
Välja en lösenordshanterare.

Det finns ett antal olika kostnadsfria lösenordshanterare på marknaden, bl.a. Bitwarden, Dashlane och Enpass. I allmänhet ska du välja en lösenordshanterare som:

- Är lätt att integrera i den webbläsare du använder mest
- Gör det möjligt att spara lösenordsfilen som en krypterad fil som inte kan läsas av användare som inte är verifierade. Mer specifikt så ska du använda en lösenordshanterare som använder AES-256-kryptering eller starkare.
- Tillåter tvåfaktorsautentisering för att ge åtkomst till lösenordsvalvet.
- Tilldelar en kontakt för nödsituationer som också har åtkomst till lösenordsvalvet.
- Lagrar ytterligare inloggningsinformation tillsammans med lösenordet (t.ex. säkerhetsfrågor, telefonnummer, kontouppgifter etc...)

Avsnitt 3:

Använd malwareskydd



Utan virusskydd kan datorn infekteras av malware inom några minuter efter att den har anslutits till internet.

Malware av olika former kan ligga på till synes pålitliga webbplatser eller nästlas in i bilagor till e-postmeddelanden, och ny malware skapas varje dag. Datorn bombarderas konstant av virus och därför måste verktygen som skyddar den vara starka, djupt rotade och uppdateras regelbundet. Ett bra malwareskydd har alla tre av dessa.

I ett nötskal är malwareskydd en uppsättning program som har utformats för att förebygga, söka efter, detektera och ta bort programvirus (och andra illasinnade program som t.ex. maskar, trojaner, annonsprogram och annat). Ett typiskt malwareskydd söker igenom systemet regelbundet och tar automatiskt bort malware som detekteras, samt varnar dig för farliga nedladdningar och programvaruuppdateringar.

Ha det eller skaffa det.

Det finns många malwareskydd på marknaden. Om du kör Windows 10 Pro på datorn så har du redan Windows Defender Antivirus installerat och aktiverat. Du kan även köpa malwareskydd från en tredje part. Se dock till att följa anvisningarna för att konfigurera automatiska uppdateringar så att du alltid har de mest aktuella virusskydden.

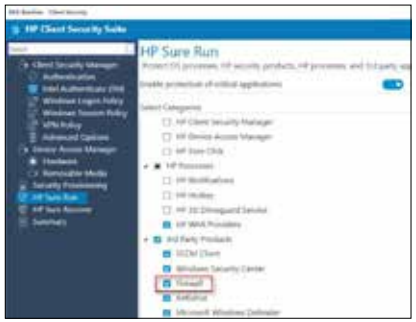
Alltid aktivt.

Det viktigaste är att malwareskyddet alltid ska vara aktivt för att vara effektivt. Eftersom det är vanligt att de som attackerar med malware i första hand riktar in sig på skyddsprogram som t.ex. malwareskydd, är det här inte så enkelt som det kanske kan låta. I Windows 10 Pro kan du verifiera om virusskyddsprogrammet är aktiverat för närvarande genom att gå till Windows Defender Security Center.

1. I Start-menyn startar du Windows Defender Security Center och går till hemskärmen.

2. Under inställningen för ”Skydd mot virus och hot” visas en grön bock om virusskyddet är aktivt. Om du använder ett virusskydd från tredje part ska du klicka på ”Leverantörer av säkerhetsprogramvara” för att visa ytterligare säkerhetsdetaljer i Windows kontrollpanel om status för virusprogrammen.

Håll det aktivt.



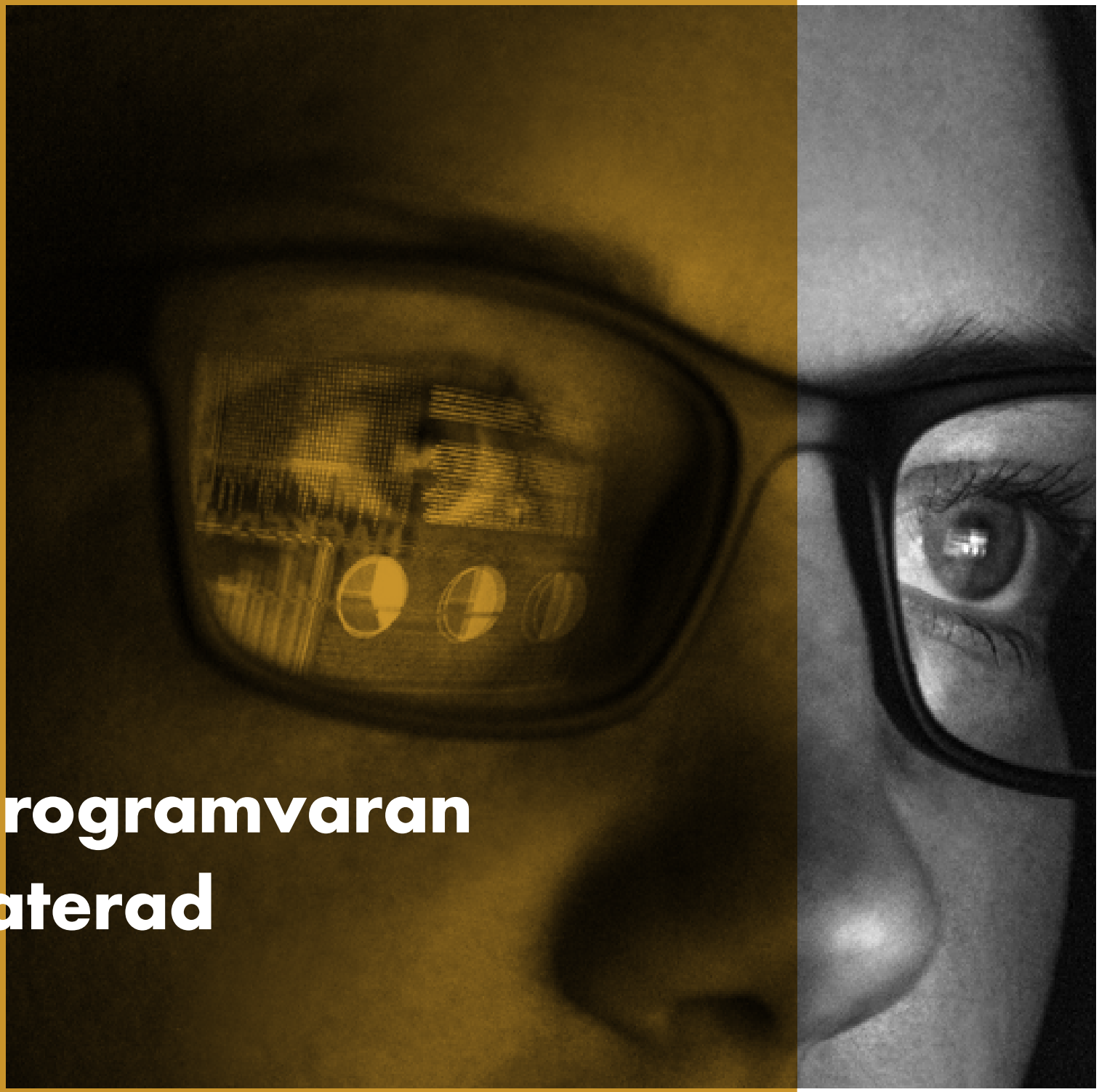
HP Elite-produkter inkluderar även HP Sure Run[12], ett extra säkerhetslager som ser till att alla dina kritiska processer på datorn, inklusive virusprogram, är aktiverade och fortsätter köras. Alla processer som Sure Run övervakar kommer att startas om automatisk om de aktiveras – vilket förebygger att inaktiverade eller kraschade virusskydd gör dig sårbar.

HP Sure Run måste aktiveras lokalt i HP Client Security Manager Gen4.

12 – HP Sure Start finns tillgängligt på HP Elite-produkter utrustade med 8:e generationens Intel®- eller AMD®-processorer.

Avsnitt 4:

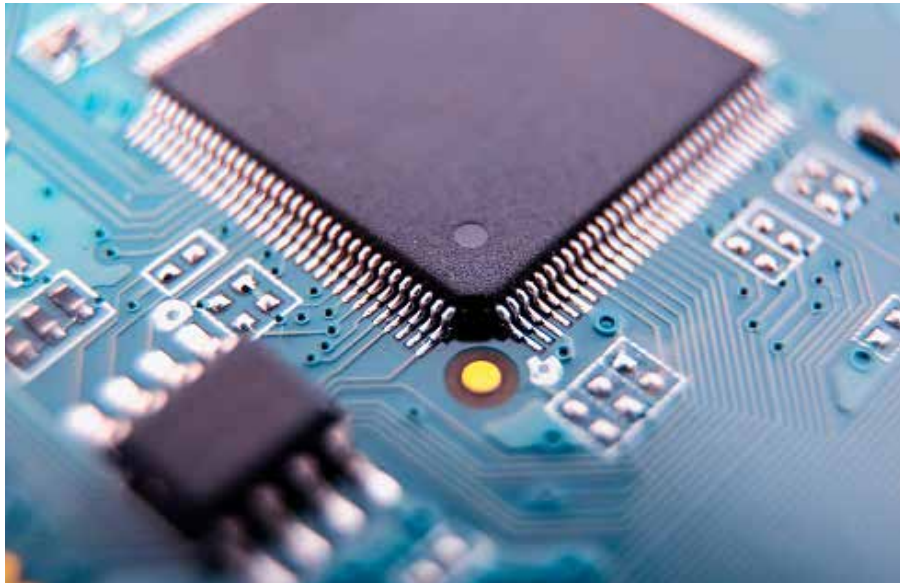
Håll programvaran uppdaterad



Malwareskydd är inte den enda typen av program som ställs inför ständigt utvecklande hot – det är viktigt att hålla all din programvara aktuell. Om programvaran inte är uppdaterad kanske den saknar viktiga säkerhetspatchar för nyupptäckta sårbarheter. Detta gäller både operativsystem (OS) som Windows® och alla program som körs på datorn, som t.ex. webbläsare, Office-program, redovisningsprogram, virusskyddprogram etc.

Användaren ska komma ihåg att äldre program eller avvecklade program kanske inte längre får säkerhetsuppdateringar. Nätbrottslingar hittar med tiden fler sårbarheter i programvara som publicerats och utnyttjar dessa. Om vi använder OS som ett exempel kanske du inte hittar någon ny programvara om du letar efter en uppdatering för Windows 7 Pro, utan att tänka på att Windows 7 Pro inte längre är den mest aktuella versionen av Windows. Att installera patchar för äldre program är inte samma sak som att uppdatera den senaste versionen – ju äldre din programvara är, desto sämre säkerhet.

> Ju äldre programvaran är desto, desto sämre säkerhet.



Kontrollera att programmet uppdateras.

När programvaruföretag hittar lösningar på sårbarheter så levererar de lösningarna i form av programvaruuppdateringar. De flesta program har en inbyggd uppdateringstjänst, som ser till att du meddelas om det finns en tillgänglig uppdatering eller patch. En del programleverantörer installerar till och med uppdateringarna automatiskt när de blir tillgängliga.
Windows 10 Pro, den nyaste versionen av Windows (och därmed den säkraste), har en automatisk programuppdateringsmekanism som håller operativsystemet uppdaterat – och alla andra Microsoft-program som t.ex. Microsoft Office också.

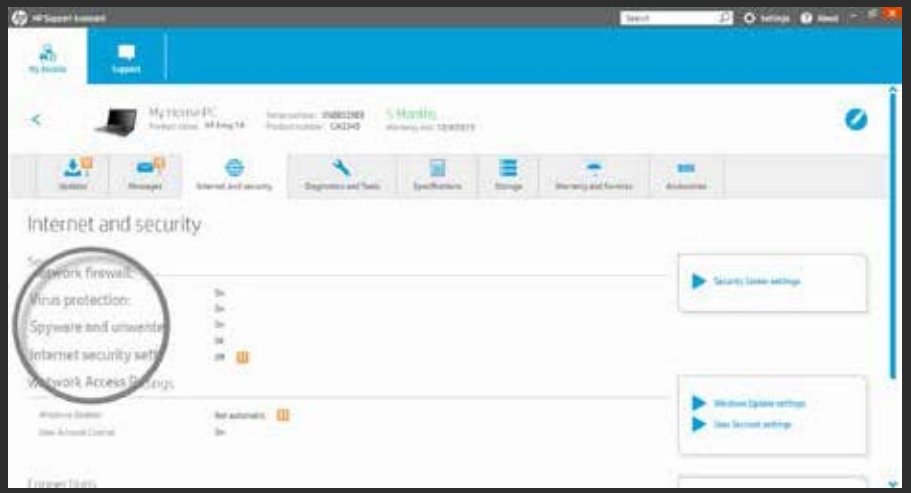
För att verifiera att automatiska uppdateringar är aktiverade:

1. Gå till inställningar och välj ”Uppdatering och säkerhet”
2. Under ”Windows-uppdateringar” väljer du ”Avancerade alternativ” och ser till att ”Automatisk” är markerat under ”Välj hur uppdateringar installeras”.
3. Se till att ”Automatisk” har valts under ”Välj hur uppdateringar installeras”.

Använd en uppdateringshanterare.

På grund av den stora mängd programvara som medföljer datorn kan det vara svårt att säkerställa att *allt* är uppdaterat. På grund av detta tillhandahåller många datorförsäljare förhandsinstallerade verktyg som automatiskt samlar ihop alla uppdateringar av programvara och fast programvara för systemet. På HP-system kallas detta verktyg HP Support Assistant.

För tredjepartsprogram utförs uppdateringar ofta av ett litet uppdateringsprogram som startas när du startar datorn. Dessa hjälpverktyg gör att det tar några sekunder längre att starta datorn, men det innebär också att du inte behöver söka efter uppdateringar på programleverantörens webbplatser. Om du har programvara som inte kontrollerar automatiskt efter uppdateringar eller om du är osäker, ska du kontrollera versionsnumret mot utvecklarens webbplats och uppdatera den för att matcha den om så behövs.



Avsnitt 5:

Se till att webbläsaren är säker

Webbläsare som t.ex. Internet Explorer eller Chrome™ är det främsta sättet att få åtkomst till internet – vilket gör dem till den främsta måltavlan för hackare. Dessa attacker inleds ofta genom att du oavsiktligt eller avsiktligt klickar på en länk som startar en illasinnad kod, som kallas malware.

Med hjälp av några enkla åtgärder kan du signifikant minska risken för en malware-attack via webbläsaren.

Använd en säker webbläsare.

Internet Explorer, Edge och Chrome™ innehåller alla starka säkerhetsfunktioner för Windows. Edge och Internet Explorer 11 använder till exempel Microsoft SmartScreen för att utföra en kontroll av anseende för varje webbplats och blockerar alla webbplatser som de misstänker vara en nätfiskewebbplats. Dessutom har Internet Explorer på HP:s kommersiella datorer den extra säkerhetsfunktionen HP Sure Click: när en flik öppnas så kör HP Sure Click den i en isolerad virtuell maskin. Detta innebär att eventuell illasinnad kod hålls kvar på fliken och förstörs när du stänger webbläsaren[13].

Var uppmärksam på varningar.

De flesta av de vanligaste moderna webbläsarna har en grundläggande spärr för att upptäcka illasinnade webbplatser och visar en varning om de anser att det finns rimliga skäl att tro att det föreligger ett hot. Vissa innehåller även autokorrigeringsfunktioner för webbadresser för att förebygga att du navigerar till en domän som har ett namn som representerar en vanlig felstavning (där illasinnade programvaror och webbplatser ofta ligger).

I Edge går du till Avancerade inställningar > Sekretess och aktiverar sedan inställningarna ”Använd en webbtjänst för att hjälpa till att lösa navigationsfel”

Håll den uppdaterad.

Aktivera automatiska webbläsaruppdateringar genom Inställningar. Som nämns ovan kan detta säkerställa att alla säkerhetsuppdateringar tillämpas för webbläsaren, vilket gör den mycket säkrare och ökar sannolikheten för att malware-attacker ska misslyckas.

I Edge tillämpas uppdateringar när Windows uppdateras. Om du vill kontrollera om du behöver uppdatera Edge ska du gå till

- Start
- Inställningar
- Uppdateringar och säkerhet
- Windows-uppdateringar
- Leta efter uppdateringar

Begränsa innehåll och tilläggsprogram.

Många av dessa tillägg till webbläsare (som t.ex. Flash eller JavaScript) behövs för komplexa webbplatser och webbprogram, men deras ökade åtkomst till systemet innebär också en sårbarhet.

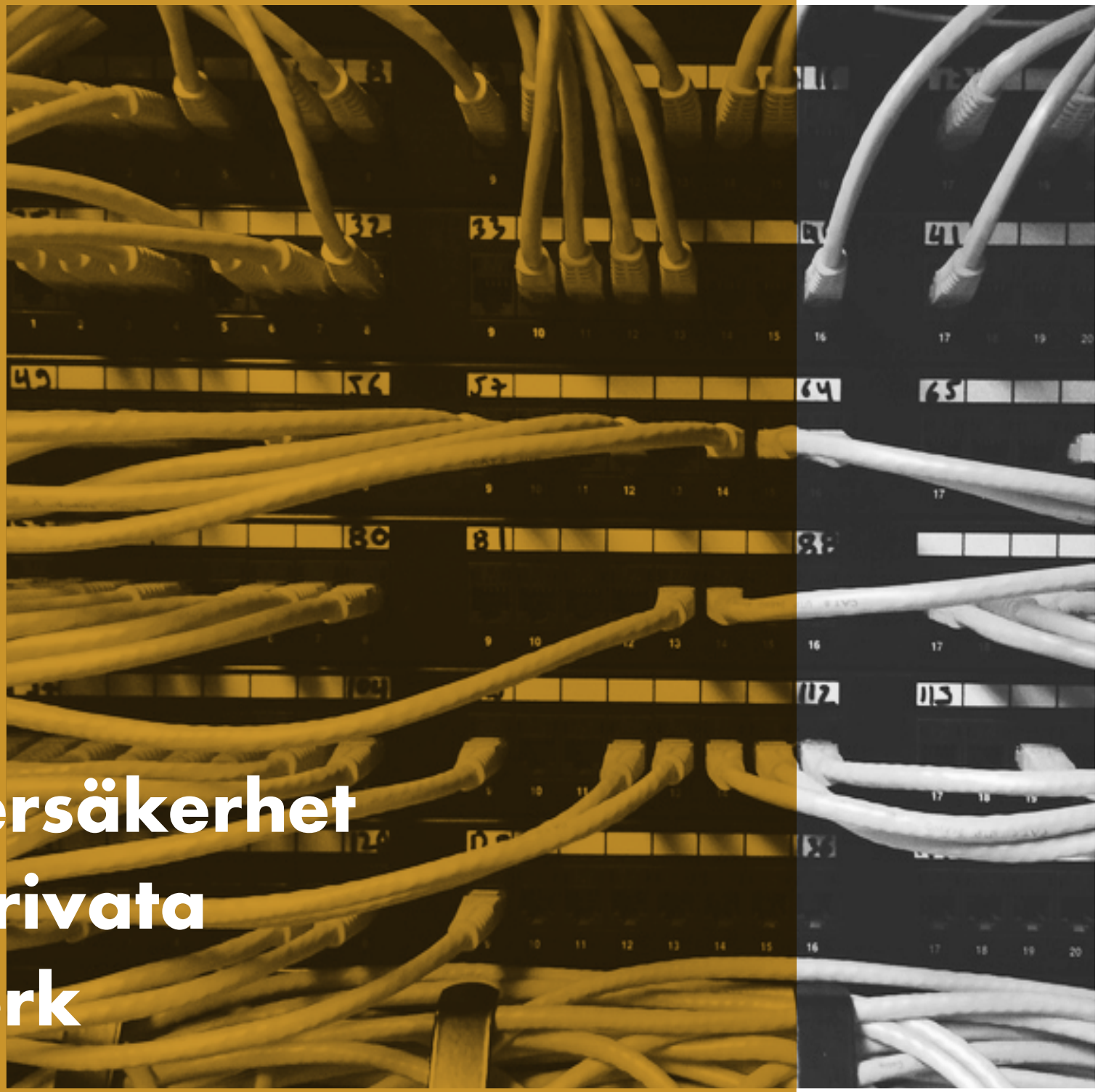
Om dessa inaktiveras som standard måste en webbplats begära tillstånd för att använda dem och därför kan endast de webbplatser du litar på använda sådana funktioner.

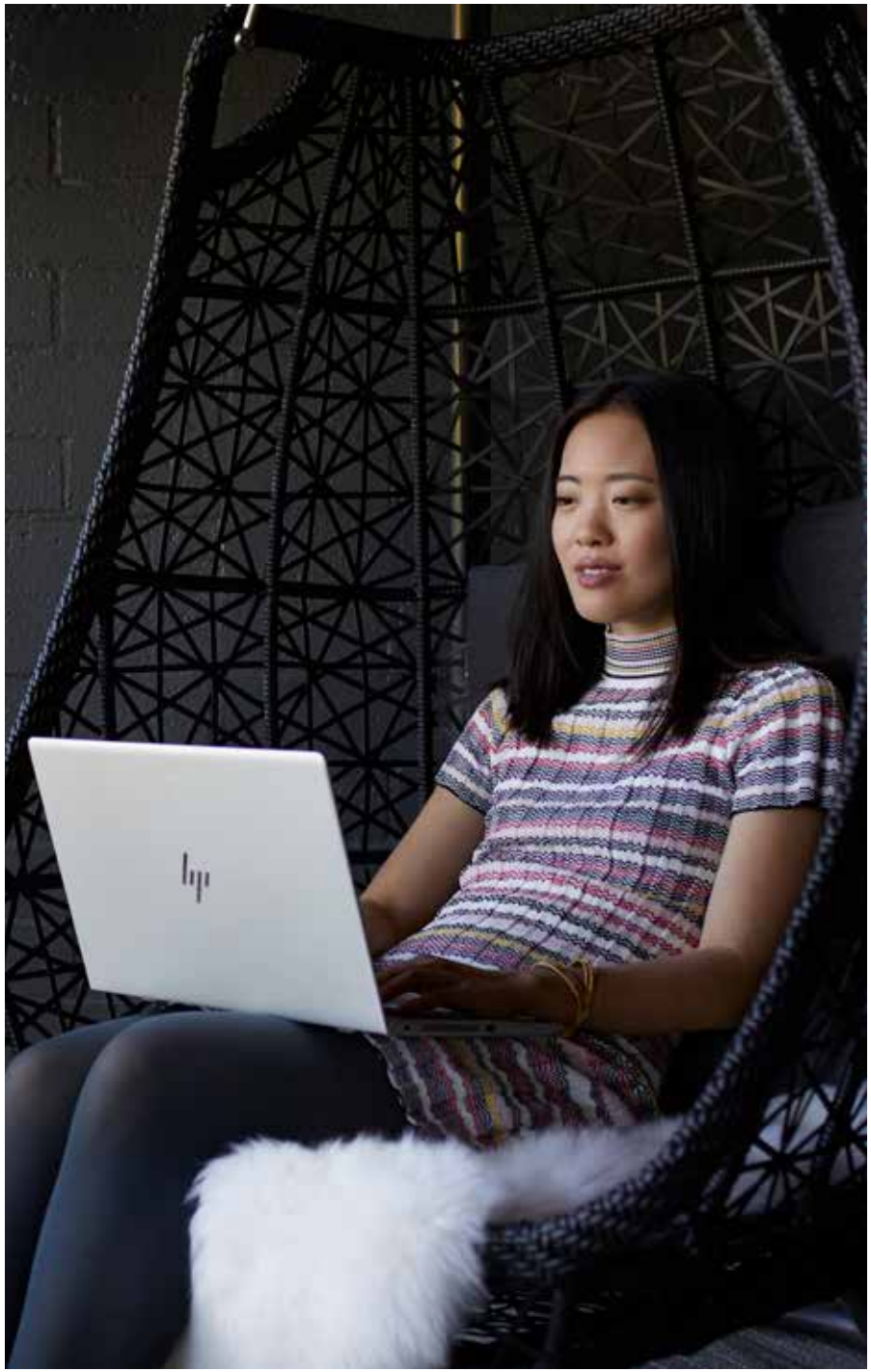
I IE går du till Verktyg (en verktygsikon) -> Internet-alternativ -> Säkerhet -> Internet -> Anpassad nivå... -> Script. Du kan inaktivera JavaScript genom att välja ”Inaktivera” eller så kan du se till att IE frågar innan en webbplats försöker använda den genom att välja ”Fråga”.

13 – HP Sure Click finns på de flesta av HP:s datorer och stödjer Microsoft® Internet Explorer och Chromium™. De bilagor som stöds är bland annat Microsoft Office (Word, Excel, PowerPoint) och PDF-filer i skrivskyddat läge, när Microsoft Office eller Adobe Acrobat är installerade.

Avsnitt 6:

Routersäkerhet och privata nätverk





Routern utgör den första skyddslinjen mot intrång i nätverket. Alla som ansluter till internet gör detta genom en router. Denna maskinvaruenhet, antingen kabelansluten eller trådlös (Wi-Fi®), möjliggör kommunikation mellan ditt lokala nätverk (din dator och eventuella andra anslutna enheter) och internet. Därför är det bästa sättet att hålla dator, skrivare och data säkra från illasinnade attacker att se till att routern har bästa möjliga säkerhet.

> Det angavs att en router var den enhetstyp som utnyttjades ofta i IoT-attacker.[14]

Eftersom routern transporterar ALLA data som flödar in och ut ur ditt hem eller företag, inklusive e-post och kreditkortsinformation, så har de länge utgjort en favoritmåltavla för hackare. I Symantecs rapport om näthot från år 2018 angavs att routrar var den typ av enhet som utnyttjades oftast vid IoT-attacker. Hackare kan använda malware eller designfel för att dölja sin identitet, stjäla bandbredd, göra dina enheter till botnät-zombier – eller göra något ännu värre. De kan också utnyttja osäkrade enheter.

14 – Källa: Symantec Corporation, 2018 Internet Security Threat Report, 2018

Säkra ditt nätverk.

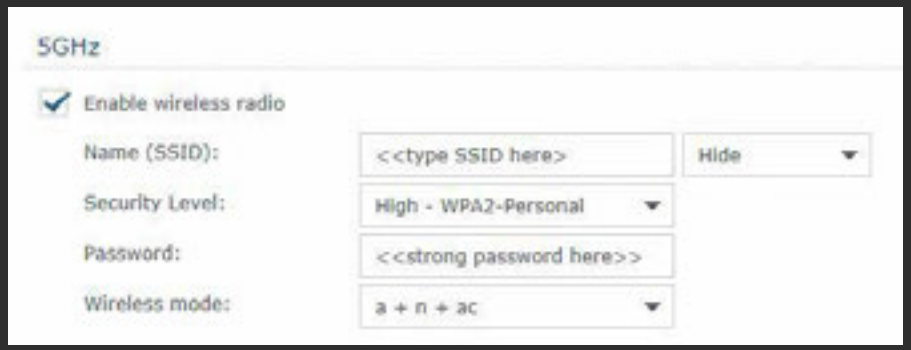
Tyvärr fortsätter dock många återförsäljare att erbjuda både oskyddade och säkra routerkonfigurationer. Om en router inte är skyddad (vilket innebär att det går att ansluta till denna utan ett administratörslösenord), kan vem som helst ansluta till routern och sedan ta sig in på det lokala nätverket. En hacker kan ändra dina lösenord, spionera på dig och till och med få åtkomst till filerna på en nätverksansluten hårddisk.

Se till att alltid säkra din router med ett annat lösenord än det standardinställda med utgångspunkt i tipsen i Avsnitt 2: Stärk dina lösenord. Nedan finns en skärmdump som visar hur de flesta routrarna gör det möjligt att ställa in lösenord för att säkra dem på nätverket.

Konfigurera kryptering.

Med trådlösa routrar är lösenord endast halva jobbet – att välja en lämplig krypteringsnivå är precis lika viktigt. De flesta trådlösa routrarna stödjer fyra trådlösa krypteringsstandarder: WEP (svagast), WPA (stark), WPA2 (starkare) och WPA3 (starkast). Använd den högsta krypteringsstandard som stöds av din router.

Nedan finns en skärmdump som visar hur du ställer in lämplig krypteringsnivå för routern. För att göra detta ska du logga in som administratör på routern och navigera till krypteringsinställningarna (varierar efter routerleverantör).



Se till att hålla den fasta programvaran uppdaterad.

Många routertillverkare gör nya programuppdateringar tillgängliga flera gånger om året för att åtgärda säkerhetsproblem. Precis som vi sa om datorprogram är det mycket mindre sannolikt att en router med de senaste uppdateringarna infekteras av malware. De flesta routerleverantörerna tillämpar uppdateringar av den fasta programvaran automatiskt utan att kunderna måste göra detta. Nya routermodeller kan också tillhandahålla en mobilapp som du kan hämta till en telefon precis som vilken annan app som helst och som du kan använda för att kontrollera efter uppdateringar. Om automatiska uppdateringar av den fasta programvaran inte tillhandahålls av routerleverantören, ska du gå till routertillverkarens webbplats, gå till support och identifiera rätt uppdatering baserat på routerns specifika modellnamn och ID (hittas vanligtvis på själva routern).

Använd virtuella privata nätverk (VPN).

Ta ännu ett steg för att säkra maskinvaran i företaget med hjälp av ett virtuellt privat nätverk (VPN) som är en server som du ansluter med för att omdirigera dina externa nätaktiviteter. En VPN kan skydda och säkra identiteter och information. Målet med en VPN är att tillhandahålla ett sätt att använda webben privat (men inte alltid anonymt). All trafik som går genom VPN-anslutningen är säker och kan i teorin inte ses av någon annan – vilket innebär att de är bra att använda både på lokala och offentliga nätverk. Mer om VPN och deras fördelar i Avsnitt 7.

Avsnitt 7:

Skydda dig på offentliga Wi-Fi®

Offentlig Wi-Fi® används flitigt i vår vardag. Flygplatser, lokala barer, shoppingcenter och till och med utomhusparker tillhandahåller ofta kostnadsfri uppkoppling via hotspot. De är otroligt praktiska – och farliga.

Användare som är anslutna till dessa hotspots delar samma nätverk – vilket innebär att det finns stor risk för att någon ska kunna utnyttja den oskyddade trafiken. En hackare kan till och med skapa en hotspot och försöka lura andra att ansluta till deras falska nätverk (med ett liknande namn). De kan då tjuvlyssna på okrypterade dataströmmar eller genomföra man-in-the-middle-attacker för att kringgå kryptering.

Det är viktigt att alltid utgå från att din kommunikation inte är säker utan kan ses offentligt när du använder ett öppet nätverk. Men om du inte har något annat alternativ så finns det andra sätt att minska riskerna.

Begränsa din aktivitet.

Skicka inte högkänsligt material som t.ex. dokument, e-postmeddelanden eller lösenord och använd inte någon typ av bank-/bokföringsprogram eller -portaler.

Se till att ha en plan B.

Om det är möjligt ska du använda halvöppna nätverk som åtminstone är lösenordskyddade. Dessa är oftast ett nätverk som hanteras av någon och leverantören har ett intresse i att hålla nätverket säkert (t.ex. i en lounge på en flygplats).

Använd bara krypterade webbplatser.

Se till att du är ansluten till en webbplats som stödjer krypterad trafik med hjälp av HTTPS-protokoll (https://), till skillnad från osäkrade webbplatser som använder HTTP-protokoll med vanlig text. Kontrollera webbplatsens webbadress – i en modern webbläsare finns oftast en ikon i webbadressfältet som anger när HTTPS används och certifikatet är giltigt (oftast en hänglåsikon eller en grön färg). Om du klickar på området visas en dialog med ytterligare detaljer på krypteringsnivån.

Dirigera allt genom en VPN.

Som vi har nämnt tidigare kan en VPN hjälpa till att skydda dina data när du inte kan lita på nätverksanslutningen – och ett offentligt Wi-Fi®-nätverk är ett perfekt exempel på detta. En VPN-tunnel krypterar dina data från ände till ände och ser till att det inte går att tolka din aktivitet om det är någon som lyssnar på den. Alla VPN:er skapas inte på samma sätt och du måste därför välja rätt tjänst för ditt prisintervall och enhetstyp. Kostnadsfria VPN:er har oftast begränsad bandbredd och enkla krypteringsprotokoll, vilket innebär att webbläsaren går långsammare och att aktiviteterna ändå kan exponeras. Det är dock bättre att använda en kostnadsfri VPN med gott renommé än att inte använda någon alls.

Avsnitt 8:

Stoppa visuella hackare

Visuell hacking innebär att känslig information visas på skärmen på offentliga ställen och att konkurrenter, identitetstjuvar eller skrupulösa individer kan se, spara och utnyttja den. Även tillfälliga nyfikna åskådare kan vara ett potentiellt hot. Risk föreligger för allt från lösenord till kontonummer till ekonomiska data och företagsinformation – och inga skyddsprogram i världen kan förhindra insyn från nyfikna i din omgivning.

Allteftersom den moderna arbetsplatsen i allt högre grad flyttar ut från de traditionella kontoren till distansarbete och offentliga utrymmen är risken för att bli ”visuellt hackad” mer verklig än någonsin. Faktum är att visuell hackning kan vara det mest underskattade lågteknologiska hotet som företag idag står inför. Det är enkelt, effektivt och förblir ofta oupptäckt förrän det är för sent.

I enlighet med en studie som publicerats av Ponemon Institute[1] anges följande:

- 91 % av alla visuella hackningsförsök lyckades
- 68 % av alla visuella hackningsförsök upptäcktes inte av offret
- 52 % av den känsliga informationen hämtades direkt från enhetsskärmen

Tänk på var du är.

När du arbetar på offentliga platser ska du alltid utgå från att någon kan titta över axeln och välja uppgifter i enlighet med detta.

Begränsa exponeringen.

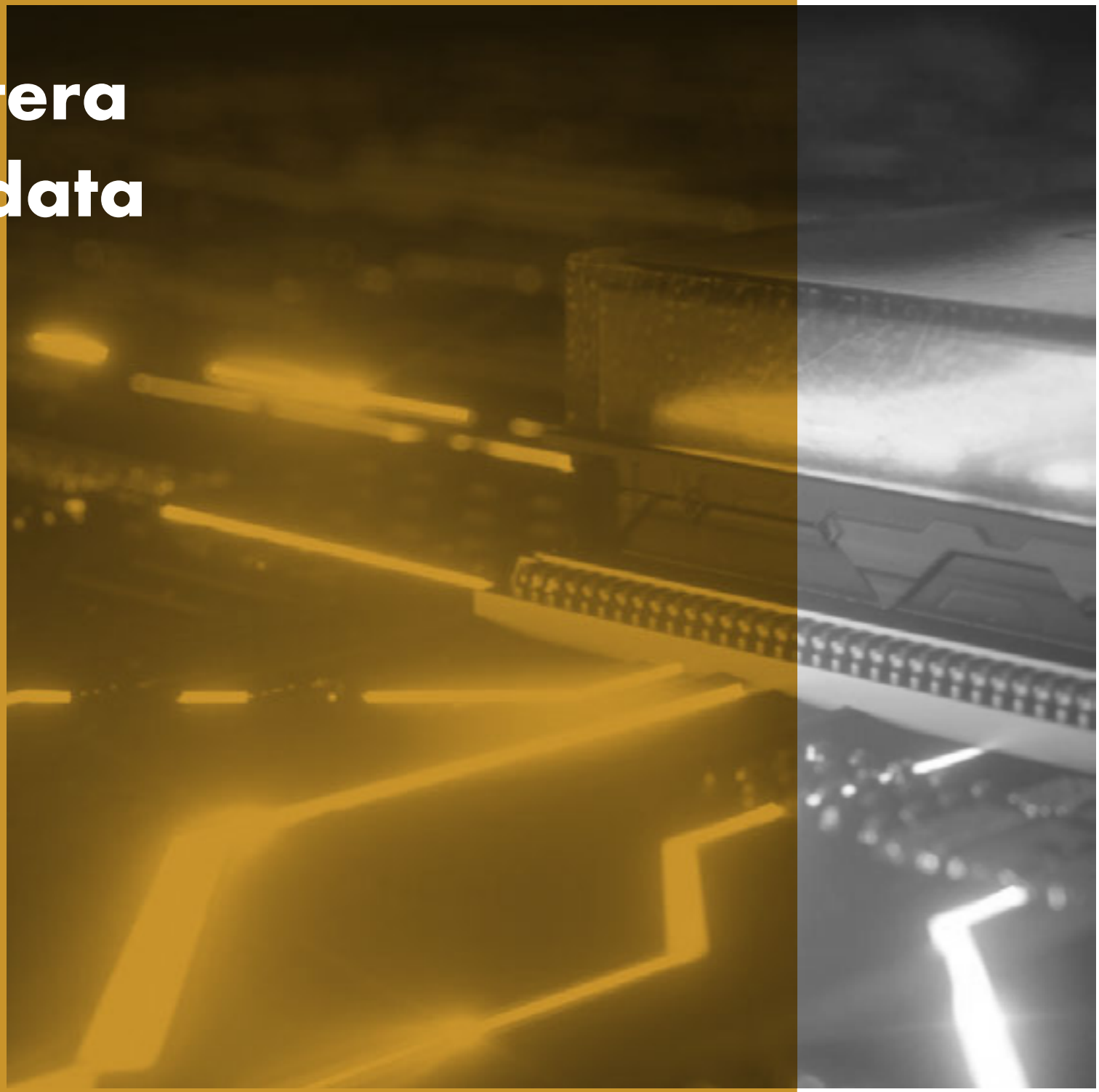
Sekretesskärmar har utformats för att minska insynsvinkeln på skärmen, så att en eventuell hackare inte kan se vad som visas utan att vara direkt bakom skärmen. Ett externt filter är ett enkelt sätt att lägga till denna typ av skydd. Du kan fästa det över skärmen och ta bort det när du behöver dela skärmen med fler personer.

En inbyggd sekretesskärm är ett annat alternativ som gör denna process ännu smidigare, eftersom du inte behöver fästa, förvara och sätta tillbaka ett externt skydd. Många av HP:s datorer har HP Sure View Gen2[15], en inbyggd sekretesskärm som har utformats för att förhindra visuell hackning, som tillval. Den fungerar genom att dynamiskt modifiera strukturen i LCD-pixlarna på molekylär nivå – vilket gör att den kan aktiveras eller inaktiveras med en knapptryckning och förbättra prestandan i både ljusa och mörka omgivningar.

15 – HP Sure Views inbyggda sekretesskärm är en tillvalsfunktion som måste konfigureras vid inköp och som har utformats för att används i liggande orientering.

Avsnitt 9:

Kryptera dina data



Om en dator förloras eller stjäls så är hårddisken det första som attackeras. Det enda som håller den på plats är några skruvar och när den har tagits ut ur datorn, kan informationen hämtas ut på en annan dator. Om du inte har skyddat data på lämpligt sätt kan det vara lika enkelt att läsa hårddisken som att öppna en bok.

Med hjälp av kryptering kan du se till att all information som eventuellt inhämtas är omöjlig att förstå. Kryptering är ett sätt att koda data så att de inte kan läsas av någon som inte har den hemliga krypteringsnyckeln. Om en dator med en krypterad hårddisk stjäls, går det inte att få åtkomst till informationen – detta är ett mycket bättre resultat än att företagsinformation eller personlig information hamnar i fel händer för alltid.

Aktivera programvarukryptering.

Windows 10 Pro stödjer lösenordskryptering av hårddisken där inloggningsuppgifterna utgör nyckeln. Då behöver en eventuell hackare ditt användarnamn och lösenord för att få åtkomst till dina data.

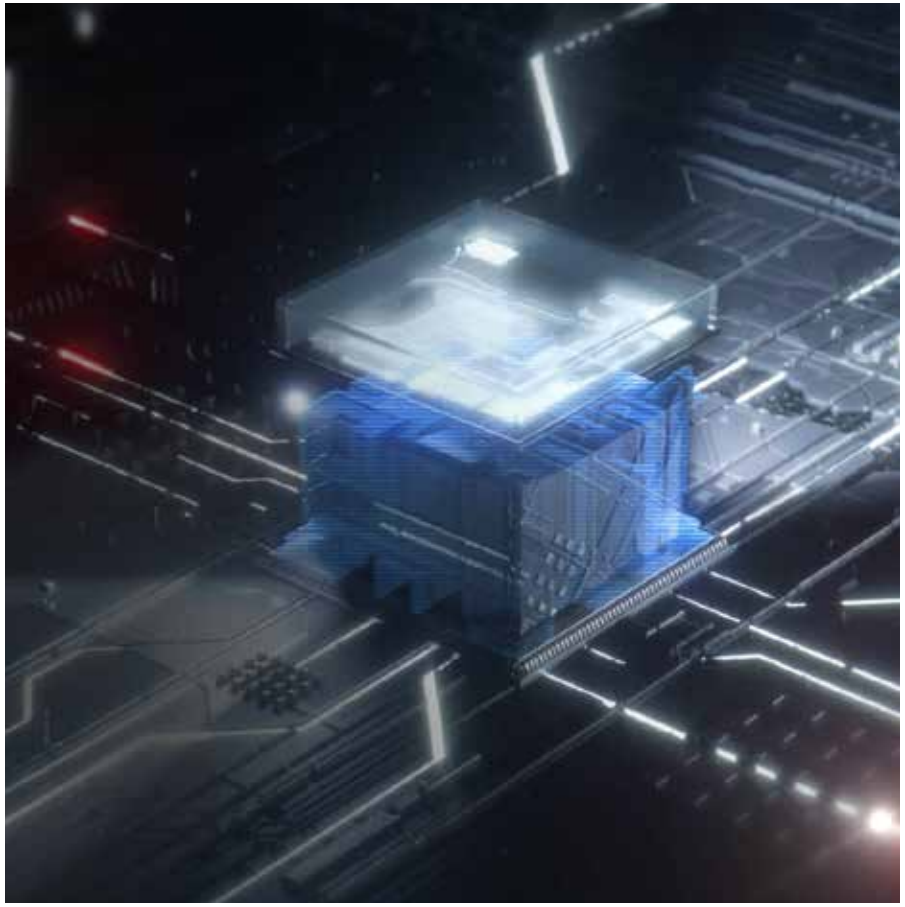
1. Se till att använda ett starkt lösenord för användarkontot:
   - Öppna Inställningar > Konton > Inloggningsalternativ > Lösenord

2. Om tillgängligt ska du aktivera Trusted Platform Manager (TPM), vilket aktiverar ett säkerhetschip på datorn för att kryptera ditt nya lösenord och data på enheten:
   - Inställningar > Uppdateringar och säkerhet > Windows-säkerhet > Enhetssäkerhet > Processor

3. Aktivera kryptering för att se till att data inte kan visas eller kopieras utan dina inloggningsuppgifter:
   - Inställningar > Uppdateringar och säkerhet > Hårddiskkryptering

Utnyttja maskinvarukryptering.

BitLocker är en funktion i Windows 10 Pro som tillhandahåller programvarukryptering som kan låsas upp med en hårdvarunyckel. Enheter som har ett TPM-chip som t.ex. bärbara HP-datorer kan kryptera utan extra hårdvara. TPM förhindrar åtkomst till krypterade data om den upptäcker att systemet har manipulerats när det var avstängt. Enheter utan TPM använder också BitLocker men för dessa krävs en borttagbar enhet, som t.ex. en USB-enhet som kan fungera som en nyckel.



Avsnitt 10:

Skydda datorn innan operativsystemstart

BIOS (Basic Input Output Software) är ett program som startar datorn och hjälper till att ladda operativsystemet. Om detta viktiga program infekteras kan spioner plantera in malware som fortsätter vara aktiva och inte upptäcks av virusskydd. Den fortsätter vara aktiv även om hårddisken raderas eller om operativsystemet ominstalleras.

Om en hackare får åtkomst till BIOS så äger de helt enkelt alla aspekter av datorn.

Detta ger angriparen ett sätt att få åtkomst till data eller göra systemet oanvändbart genom att modifiera den fasta programvaran så att du måste byta ut hela moderkortet om du vill reparera datorn. För HP Elite och Pro kan HP Sure Start automatiskt självläka BIOS från malware, rotkit eller korruption genom att lägga till ett extra skyddslager och skapa en pålitlig bas för datorskydd[16].

Lämna inte några uppdateringar ogjorda.

Som vi nämnde tidigare i avsnitt 4 ser uppdateringar till att nyfunna sårbarheter lagas – och BIOS är inget undantag. Eftersom de flesta BIOS-implementeringarna har samma källkod för en hel arbetsplats eller användargrupp, kan alla upptäckta sårbarheter finnas på många ställen i alla datorer från samma tillverkare. OEM-verktyg som t.ex. HP Support Assistant kontrollerar efter uppdateringar automatiskt, eller så kan du kontrollera tillverkarens webbplats för BIOS-uppdateringar.

Gräva sig in i BIOS.

Fabriksinställningarna för BIOS kan ses som en balansgång mellan säkerhet och användbarhet. För att skydda systemet mot de många möjliga sätt som illasinnad kod kan spridas på, kanske du vill ta bort några av funktionerna.

Hur vi får åtkomst till BIOS-inställningarna kan variera lite mellan olika tillverkare men det görs vanligtvis genom att trycka på en funktionsnyckel under start av datorn (F10 eller FN-10 på bärbara HP datorer).

16 – HP Sure Start Gen4 finns tillgängligt på HP Elite- och HP Pro 600-produkter utrustade med 8:e generationens processorer från Intel eller AMD.

Konfigurera ett lösenord för BIOS.

För att se till att BIOS-inställningarna inte ändras av obehöriga användare rekommenderas det att du konfigurerar ett BIOS-lösenord:

- Till exempel: Säkerhet > Administratörsverktyg > Skapa BIOS-administratörslösenord

Det är viktigt att komma ihåg BIOS-lösenordet eftersom det har utformats för att inte kunna kringgås eller återställas.

Ställ in ett lösenord för start av datorn.

För ännu bättre skydd kan du konfigurera ett lösenord för Start. När datorn startas, innan systemet kör någonting, måste du ange lösenordet för att den ska starta. Precis som för BIOS-lösenordet så kan inte det här lösenordet återställas på ett enkelt sätt och om du glömmer det blir datorn oanvändbar.

Begränsa oanvända funktioner.

I BIOS finns ett fåtal inställningar som du kan överväga att tillämpa för att uppnå maximal säkerhet. Även om de kan ta bort vissa funktioner eller minska åtkomst kan de skyddsfunktioner före OS som de möjliggör inte replikeras med annan programvara på ett enkelt sätt:

1. Ta bort externa och optiska enheter från startuppordningen (T.ex. Avancerat > Avancerade startalternativ). Särskilt start av USB-lagring, nätverksstart (PXE) och start av optisk enhet, eftersom dessa gör det möjligt för malware att laddas från externa källor. Om start av de här enheterna behövs kan funktionen sedan aktiveras efter behov.
2. Inaktivera stöd för äldre versioner (t.ex. Avancerad > Säker startkonfiguration) och aktivera Säker start.
3. Aktivera funktionen ”Spara/Återställa GPT på systemets hårddisk” (t.ex. Säkerhet > Hårddiskfunktioner).
4. Aktivera DriveLock och ställ in ett lösenord.

Slutsats

Det finns idag fler digitala hot som är inriktade på små och mellanstora företag än någonsin förut. Den goda nyheten är att mycket av hårdvaran och programvaran du äger innehåller oanvända säkerhetsfunktioner som du kan aktivera för att motverka dessa. Det finns också fler produkter och tjänster än någonsin med det allra senaste inom säkerhetstekniken som kan bidra till att skydda dig mot morgondagens okända faror. Från hårdvarubaserad säkerhet på moderna enheter till självuppdaterande programvara, en smart investering i anslutna säkra enheter ger avkastning långt in i framtiden. HP utformar säkerhetslösningar som utnyttjar styrkorna i Windows 10 Pro och stödjer inbyggda funktioner med diskreta hårdvaruförbättringar och support för programvara som ständigt uppdateras. De hot du ställs inför utvecklas dagligen – och rätt säkerhetsstrategi innebär en avsevärd förbättring av dina odds mot dem.

TACK.

För mer information ska du gå till: www.hp.com/go/windows10now

Var säkrare från start till avstängning.