+ Windows 10

CYBER-SECURITY SERVICE-MANUAL

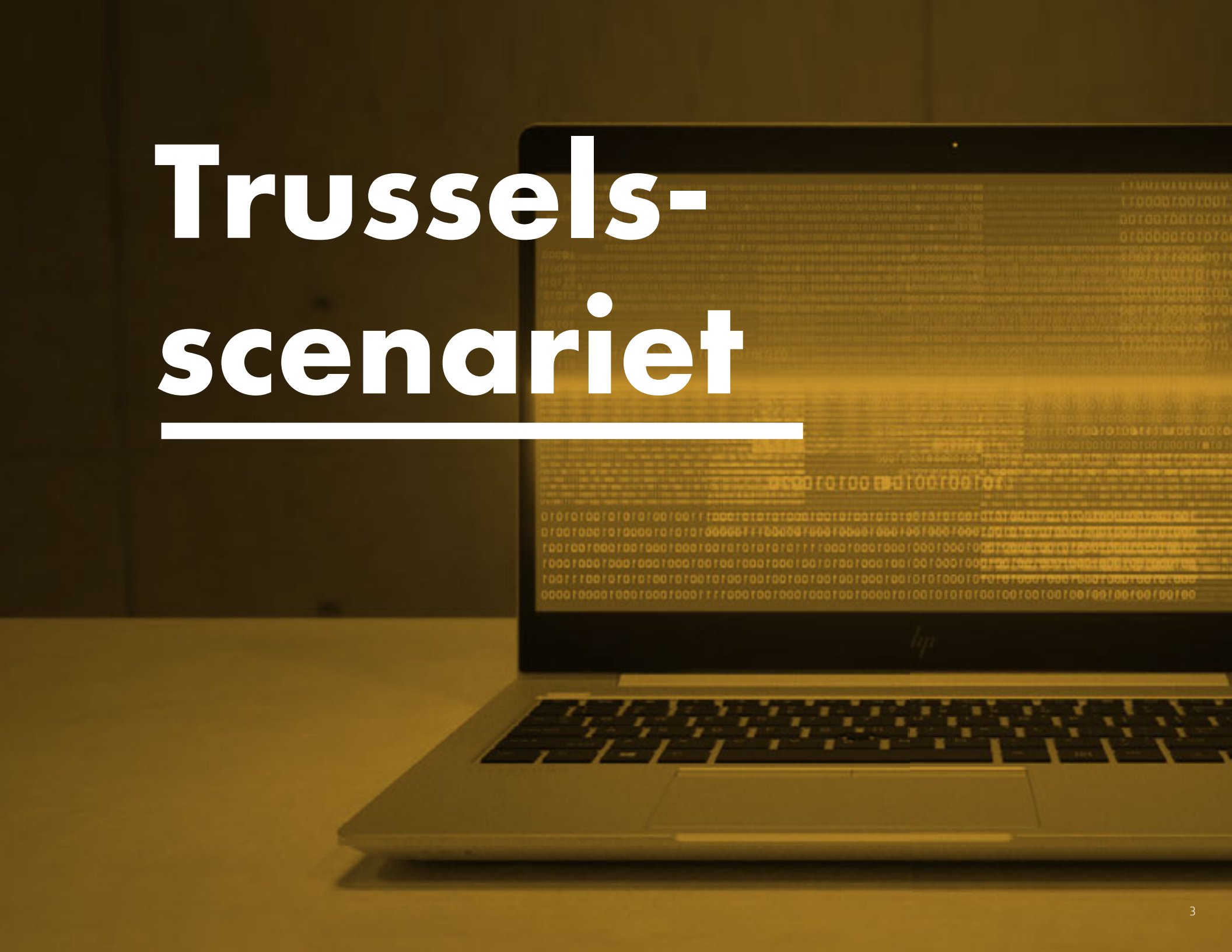
Ti trin enhver virksomhed burde tage for at beskytte sig mod cyberangreb.

Vær mere sikker, fra du tænder, og indtil du slukker.

Cybersecurity-landskabet er i konstant forandring og udvikling. Små og mellemstore virksomheder må i stigende grad konfrontere cyberangreb, som truer deres information og deres kunders private data. Denne vejledning er beregnet til at hjælpe de små og mellemstore virksomheder med begrænsede it-ressourcer til at styrke deres cybersecurity med små eller ingen omkostninger.

INDHOLDSFORTEGNELSE

Trussels-scenariet



Cybersecurity-tendenser i små og mellemstore virksomheder

Disse er fem af de mest udbredte tendenser, når det gælder cybersecurity for små og mellemstore virksomheder, i henhold til Ponemon Institute[1]:

1. **Flere virksomheder bliver udsat for angreb.**
I de sidste 12 måneder er cyberangreb på små og mellemstore virksomheder steget med 6 procentpoint fra 55 % til 61 %. De mest udbredte angreb mod små og mellemstore virksomheder er phishing/social engineering (48 %) og webbaseret (43 %). Samtidigt stiger cyberangreb mere målrettet, alvorligt og sofistikeret.

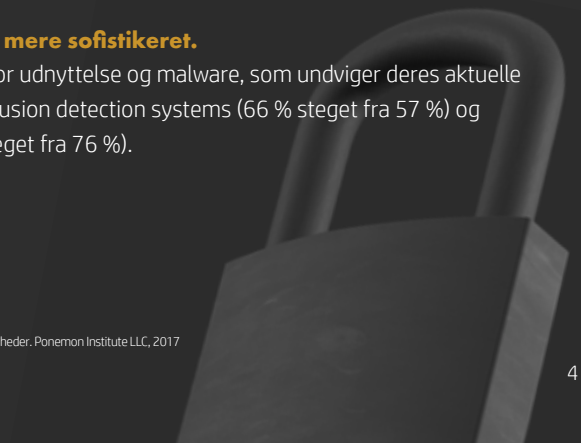
2. **Angrebene medfører stigende omkostninger.**
Gennemsnitsomkostningen pga. afbrydelse af den normale drift steg med 26 % fra 955.429 USD til 1.207.965 USD. Gennemsnitsomkostningen pga. skader eller tyveri af it-aktiver og infrastruktur steg fra 879.582 USD til 1.027.053 USD.

3. **Menneskelige fejl er den hyppigste årsag.**
Ud af små og mellemstore virksomheder, som oplevede et databrud, fortalte 54 %, at skødesløse medarbejdere var den væsentligste årsag, hvilket er en stigning på 48 % sammenlignet med året før. Men ligesom sidste år kunne 1 ud af 3 virksomheder i denne undersøgelse ikke afgøre, hvad der var hovedårsagen.

4. **Stærke adgangskoder og multifaktor-autorisation forbliver underudnyttet.**
Adgangskoder fortsætter med at være en uundværlig del af cybersecurity. 59 % af svarpersonerne fortalte imidlertid, at de ikke har noget indblik i medarbejdernes adgangskodepraksis, som eksempelvis brugen af unikke eller stærke adgangskoder eller deling af adgangskoder med andre, hvilket er uændret sammenlignet med sidste år.

> 59 % siger, at de ikke har indblik i medarbejdernes adgangskodepraksis

5. **Malware bliver mere og mere sofistikeret.**
Flere virksomheder er ofre for udnyttelse og malware, som undviger deres aktuelle beskyttelser, indbefattet intrusion detection systems (66 % steget fra 57 %) og antivirus-løsninger (81 % steget fra 76 %).



1—Rapport: 2017 cybersecurity-tilstand i små og mellemstore virksomheder. Ponemon Institute LLC, 2017

De fem mest almindelige angreb mod små og mellemstore virksomheder.

1

Phishing/social engineering

Social engineering-angreb anvender menneskelig interaktion til at indhente oplysninger om en organisation eller dens computersystemer. For eksempel kan hackeren optræde som en ny medarbejder, en tekniker eller en forsker. Ved at stille spørgsmål kan vedkommende være i stand til at sammenstykke tilstrækkelig mange informationer til at infiltrere en virksomheds netværk.[2]

Phishing er en form for social engineering. Under et phishing-angreb bruger den kriminelle en pålidelig organisations id og anvender e-mail eller skadelige websites til at indsamle personoplysninger.[2]

2

Webbaserede angreb

I webbaserede angreb får den kriminelle adgang til et legitimt website og posterer malware. Det legitime site optræder som en parasit-vært, der inficerer intetanende besøgende. En af de mest lumske typer af webbaseret angreb er en "drive-by-download", hvor det skadelige indhold automatisk bliver overført til brugerens computer, når vedkommende browser på sitet. Der kræves ingen handling af brugeren.[3]

3

Malware

Malware er et udtryk, der henviser til al software, der er beregnet til at forårsage skade på en enhed eller et netværk.[4] Dette indbefatter vira, spyware, ransomware og alle de andre "-ware". Udover webbaserede angreb kan den trænge ind på en computer via et USB-drev eller en usikker netværksforbindelse.[5]

4

Kompromitterede eller stjålne enheder

En stjålen eller kompromitteret enhed kan indeholde både værdifulde oplysninger og lokalt opbevarede brugeroplysninger, der giver adgang til en organisations informationer og netværk. Svage adgangskoder og datakryptering kan yderligere forværre denne type angreb.

5

Afvisning af serviceangreb

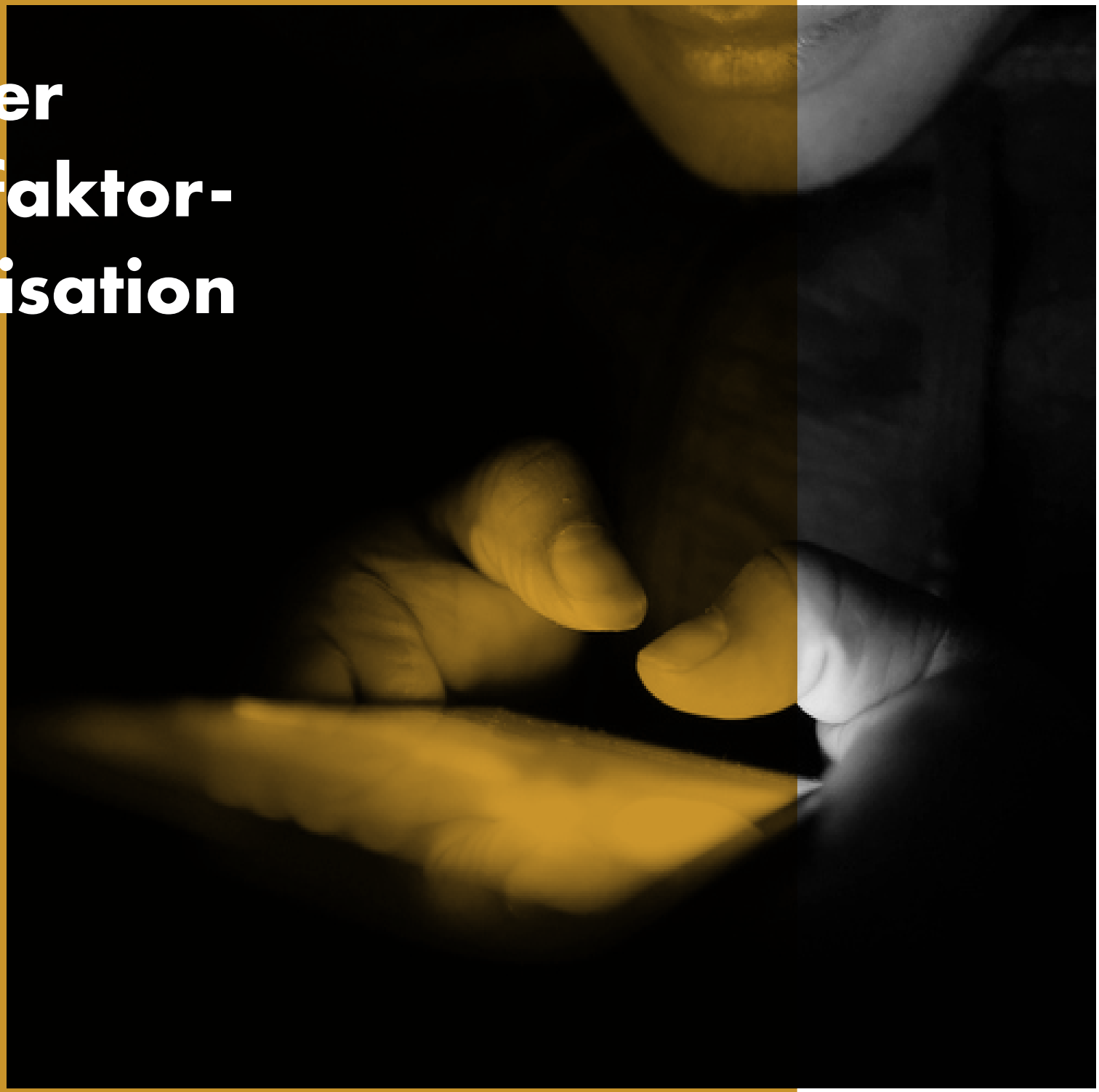
Afvisning af serviceangreb udføres ved at oversvømme netværket med trafik, indtil det ikke kan svare eller bryder sammen, hvilket forhindrer adgang for legitime brugere. Denial of service-angreb (DDoS) forekommer, når mange maskiner samarbejder for at angribe et mål, hvilket øger angrebets styrke. DDoS gør det ligeledes vanskeligere at finde kilden til angrebet.[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

Ti måder at beskytte dig selv på

Afsnit 1:

Aktiver multifaktor-autorisation



Brugernavne og adgangskoder er oplagte mål for hackere og med god grund. Din identitet er dit mest kostbare aktiv. Stærke og sikre adgangskoder hjælper meget, men adgangskoder alene er langt fra den sikreste autorisationsmekanisme. Og i en verden med kommercialiseret hacking kan de kriminelle, som ikke selv er eksperter, udlicitere arbejdet til andre. Hackere kan købe specialbygget hardware, der er beregnet til at stjæle adgangskoder, leje plads fra offentlige udbydere af cloud-lagring eller oprette en botnet til at gøre arbejdet.

- 90 % af data, der stjæles ved phishing, er brugeroplysninger[7]
- 80-90 % af adgangskoder kan hackes på under 24 timer[8]

Multi-factor authentication (MFA) kræver, at du bruger to eller flere uafhængige brugeroplysninger til at bevise, hvem du er, og dermed øges dit sikkerhedsniveau betydeligt. Brugeroplysninger kan være noget, brugeren **kender** (adgangskoder eller PIN-koder), noget brugeren **har** (Bluetooth® telefoner eller smartcards), eller noget brugeren **er** (ansigtsgenkendelse eller fingeraftryk). Hvis en faktor bliver kompromitteret eller brudt, så skal den kriminelle stadigvæk overkomme endnu en barriere af en anden type.

HP MFA og Intel® Authenticate muliggør begge, at der påkræves brug af flere autorisationsfaktorer ved login.

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

Opsæt multifaktor-autorisation med HP.

Moderne HP Pro- eller Elite-enheder understøtter opsætning af MFA gennem HP Client Security Manager.[9]

1. Åbn Client Security Manager (du skal have administratorrettigheder for at udføre dette). Hvis du åbner den med HPs Manageability Integration kit (MIK), så kan du bruge dine MFA-politikker til alle dine pc'er.[10]
2. På dashboardet skal du klikke på Standardbruger-politikker.
3. Vælg de to eller tre faktorer, som du ønsker at konfigurere med en login-politik, og følg vejledningen som anmodet for at tilmelde identifikation eller identifikationspar - eksempelvis scanning af fingeraftryk fra pc'ens fingeraftrykslæser eller indtastning af en PIN-kode.

Gør afvekslende med Windows Hello.

Mange moderne Windows 10 Pro-enheder med indbygget webcam er kompatible med Windows Hello, indbefattet hele udvalget af HP notebooks og convertibles. Ved at scanne dit ansigt giver Windows Hello dig et alternativ til en adgangskode som en af dine MFA-brugeroplysninger.

1. Åbn indstillinger > Konti > Log på valgmuligheder
2. Under 'PIN' skal du vælge 'Tilføj', hvis du ikke allerede har oprettet en.
3. Under 'Windows Hello' skal du vælge 'Opret' og følge vejledningen på skærmen for at scanne dit ansigt.

9—HP Client Security Manager Gen4 kræver Windows og Intel® eller AMD 8. generation-processorer.
10—HP Manageability Integration Kit kan hentes fra http://www.hp.com/go/clientmanagement.

Afsnit 2:

Styrk dine adgangskoder

Adgangskoder er allestedsnærværende i vores dagligdag. Vi bruger dem til stort set alle personlige eller professionelle enheder, tjenester og konti. Eftersom de er de første og alt for ofte de eneste forsvarsværker, når det gælder beskyttelse af identitet og data, så kan brugen af svage adgangskoder give katastrofale konsekvenser. På trods af dette bruger de fleste mennesker alligevel ikke stærke og unikke adgangskoder.

- 59 % ved, at en stærk adgangskode er vigtig, men alligevel vælger 41 % en adgangskode, der er nem at huske
- 91 % forstår, at der er en risiko ved at genbruge adgangskoder, men 55 % gør det alligevel.
- Millenniumgenerationen bruger normalt stærkere adgangskoder end Baby Boomers (65 % mod 45 %).[11]

Hvis din enhed eller service ikke understøtter MFA, så er den næstbedste mulighed at gøre din adgangskode så sikker som mulig. De fleste mennesker anvender ikke stærke adgangskoder, fordi de ikke ved, hvordan man opretter dem, de formoder, at det ville være en vilkårlig kombination af bogstaver, tal og symboler. Men der findes bedre og enklere måder at øge beskyttelsesniveauet betydeligt på.

11—Kilde: LastPass, "New Research: Psychology of Passwords, Neglect is Helping Hackers Win", Katie Petrillo, 1. maj 2018

Mnemoteknisk i stedet for numerisk.

Mnemotekniske adgangskoder er sikrere end almindelige adgangskoder og nemmere at huske end en numerisk kode.
Når de anvendes i stedet for en enkel adgangskode, er mnemotekniske adgangskoder næsten umulige for hackere at bryde.

1 Start med en vending du kan huske.

For eksempel de første seks ord fra Abraham Lincolns berømte Gettysburg Address "Four score and 7 years ago" er en enkel adgangskode. Citatet opfylder de fleste standarder for adgangskoder: 8-32 bogstaver i længde og indeholder store og små bogstaver, mindst et tal og et specialtegn (mellemrum eller underscore, hvis mellemrum ikke er tilladt).

2 Maksimer sikkerheden.

Øg antallet af tal og specialtegn, der anvendes. Prøv for eksempel at ændre bogstaverne i dit forrige eksempel til
"4 $core @nd 7 Ye@rs ago."

3 Brugertilpas men kopier ikke.

Ved ganske enkelt at kombinere vedhæftningen af et enkelt suffiks til enden på hver adgangskode, kan du nemt genbruge din master-adgangskode uden fare for at kopiere. Til en Facebook-konto kan du prøve at tilføje "FB" til enden af adgangskoden eller "IG" til Instagram.

Brug en adgangskodeadministrator.

Adgangskodeadministratorer er en af bedste sikkerhedsforanstaltninger, der anbefales af sikkerhedseksperter. De fungerer ved, at de genererer og gemmer lange, komplicerede adgangskoder for hver af dine online-konti - så undgår du at skulle huske dem. Generelt skal du blot huske en adgangskode, nemlig master-adgangskoden til din boks. Opsætningen af adgangskodeadministratoren er enkel, og processen er normalt den samme:

1. Download og installer softwaren og en udvidelse til din browser. Du kan også hente en app til din mobile enhed.
2. Opret din konto med en e-mailadresse og din master-adgangskode.
3. Indtast dine oplysninger for dine forskellige konti.

De fleste adgangskodeadministratorer kræver, at du manuelt opdaterer dine gamle adgangskoder: log på din konto, gå til dine kontoindstillinger og lad din adgangskodeadministrator generere en ny og mere sikker adgangskode. At udskifte dine gamle adgangskoder kan tage lang tid, men den øgede sikkerhed gør, at det er tiden værd.

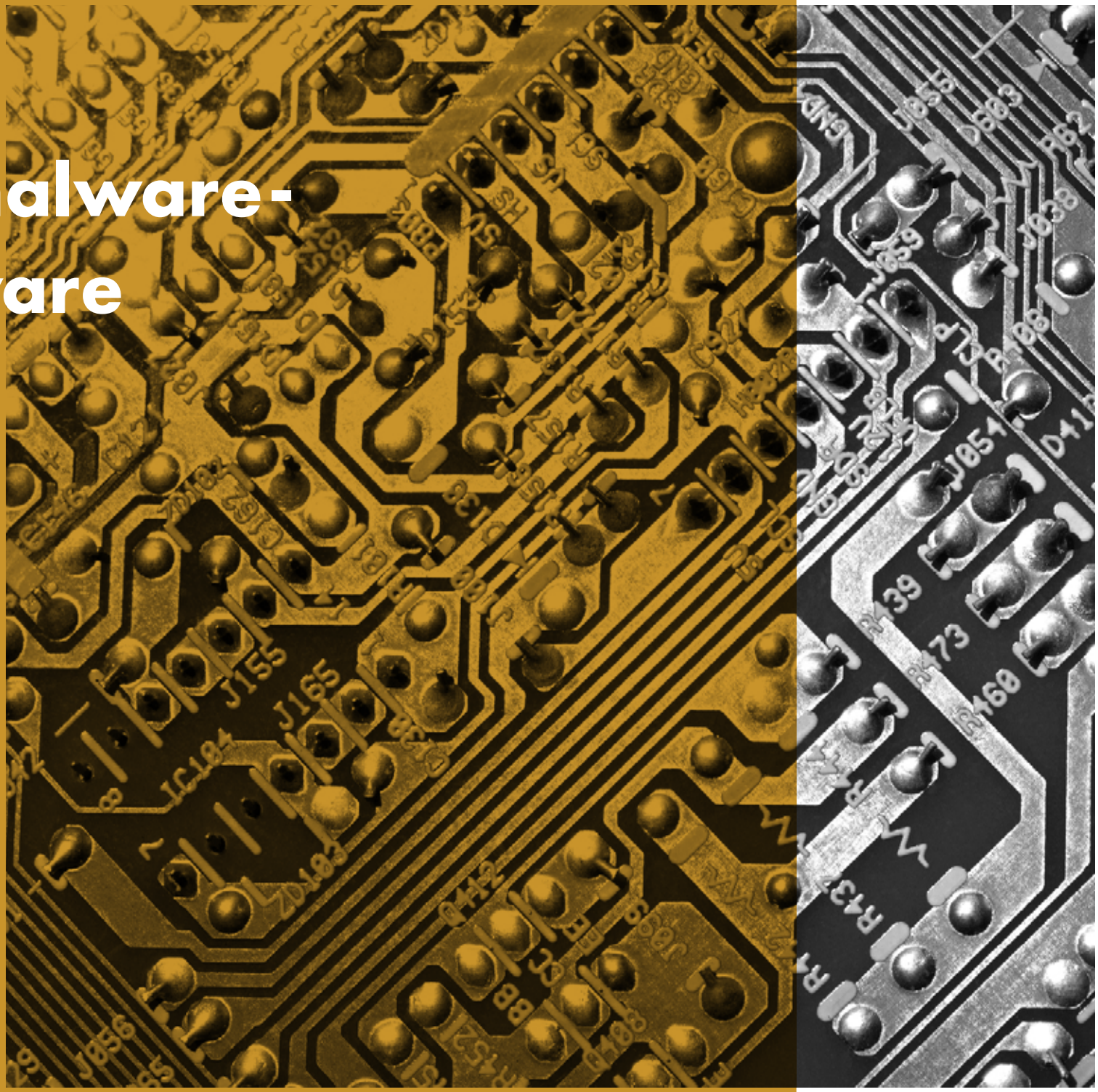
Valg af adgangskodeadministrator.

Der findes en lang række tilgængelige adgangskodeadministratorer indbefattet Bitwarden, Dashlane og Enpass. Generelt bør du kigge efter en adgangskodeadministrator, som:

- Integrerer nemt med hvilken som helst browser, du oftest benytter
- Muliggør, at du kan gemme adgangskodefilen som en krypteret fil, der er ulæselig for brugere uden godkendelse af din identitet. Du bør i særdeleshed vælge en adgangskodeadministrator, der bruger AES-256 kryptering eller bedre.
- Tillader 2-faktor-autorisation for at tilgå adgangskodeboks.
- Tildeler en nødkontakt, som også kan få adgang til adgangskodeboksen.
- Gemmer yderligere log-in-oplysninger sammen med adgangskoden (dvs. sikker-hedsspørgsmål, telefonnumre, kontooplysninger m.m.)

Afsnit 3:

Brug antimalware-software



Uden antivirusbeskyttelse kan en pc blive inficeret med malware i løbet af få minutter efter forbindelse til internettet.

Malware i alle former kan blive hostet på tilsyneladende pålidelige sites eller gemt i e-mailvedhæftninger, og der bliver udviklet ny malware hver eneste dag. Din pc bliver ustandseligt bombarderet med vira, så du har brug for et værktøj, der er stærkt, rodfæstet, og som opdateres jævnligt. Et godt antimalware-program opfylder alle tre krav.

Kort sagt er antimalware-software et program eller en række programmer, der er udformet til at forhindre, søge efter, registrere og fjerne software-vira (samt andet skadeligt software som orme, trojanske heste, adware m.m.). Et typisk antimalware-program scanner dit system med jævne mellemrum og fjerner automatisk malware, der bliver fundet såvel som informerer dig om farlige downloads og software-opdateringer.

Har du det? Ellers anskaf det!

Der findes mange antimalware-produkter på markedet. Hvis du kører Windows 10 Pro på din pc, så har du allerede Windows Defender antivirus-programmet installeret og aktiveret. Du kan også vælge at købe et antimalware-program af en tredjepart. Du skal imidlertid sørge for at følge forhandlerens vejledning til opsætning af automatiske opdateringer, således at du altid har den nyeste virusbeskyttelse.

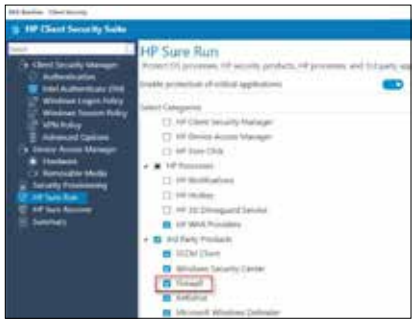
Skal altid køre.

Det er uhyre vigtigt, at antimalware-software altid kører for at være effektivt. Eftersom det er almindeligt, at malware-angreb rettes mod sikkerhedsprogrammer først som antimalware, er dette trin ikke helt så enkelt. I Windows 10 Pro kan du undersøge om dit antivirus-program p.t. er aktiveret ved at kontrollere Windows Defender Security Center.

1. Fra Startmenuen åbnes Windows Defender Security Center og gå derefter til Start.

2. Under overskriften "Virus- og trusselsbeskyttelse", hvis antivirus kører, vil du se et grønt flueben. Hvis du bruger et antivirus-program fra en tredjepart, skal du klikke på "Vis producenter af antivirusprogrammer" for at få vist yderligere sikkerhedsoplysninger på Windows-kontrolpanelet om din antivirus-programstatus.

Og lad det fortsat køre.



HP Elite-produkter indeholder også HP Sure Run[12], der er et ekstra sikkerhedslag, som sikrer, at alle dine vigtige processer på din pc indbefattet din antivirus-software forbliver opdateret og kører. Alle processer, der overvåges af Sure Run, bliver automatisk genstartet, hvis programmet bliver deaktiveret, dette forhindrer, at du bliver sårbar pga. deaktiveret eller nedlukket software.

HP Sure Run skal aktiveres lokalt i HP Client Security Manager 4. gen.

12— HP Sure Run er tilgængelig på HP Elite-produkter udstyret med 8. generation af Intel®- eller AMD®-processorer.

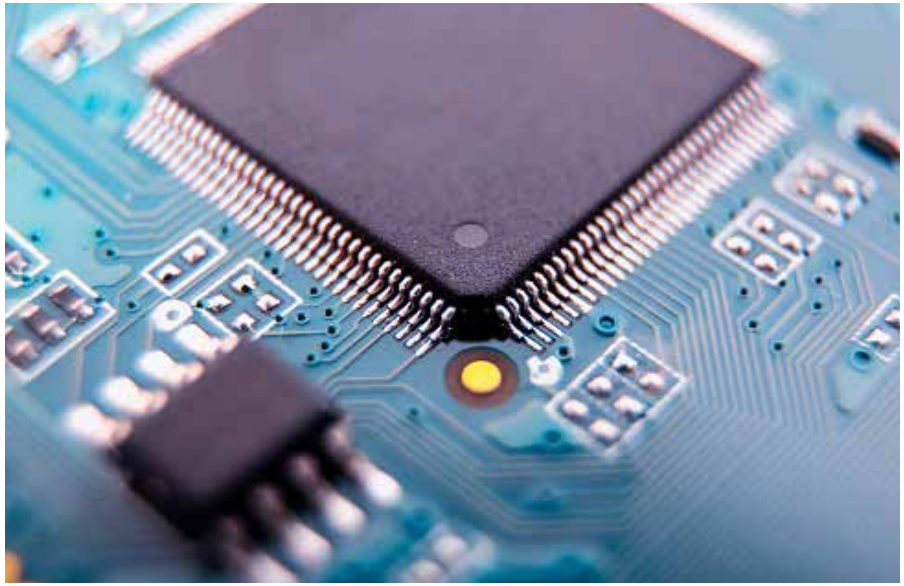
Afsnit 4:

Sørg for, at din software er opdateret

Antimalware er ikke den eneste slags software, der udsættes for trusler, derfor er det vigtigt, at du opdaterer al din software. Hvis din software ikke er opdateret, kan der mangle vigtige sikkerhedsprogramrettelser til nylige sårbarheder. Dette gælder både for operativsystemet (OS) som Windows® og alle de programmer, der køres på pc'en som for eksempel internet-browsere, Office-programmer, regnskabs-software, antivirus-software osv.

Brugeren skal også huske på, at ældre eller udløbet software måske ikke længere modtager sikkerhedsopdateringer. Med tiden finder cyber-kriminelle sårbarheder i udgivet software og udnytter fordelene af disse opdagelser. Hvis vi bruger OS som et eksempel, søger man efter en opdatering til Windows 7 Pro, er det ikke sikkert, at der findes en opdatering, men det er måske, fordi Windows 7 Pro ikke er den nyeste version af Windows. Reparation af gammel software er ikke det samme som opdatering til den nyeste version. Jo ældre din software er, desto mere usikker er den.

> Jo ældre din software er, desto mere usikker er den



Godkend, at du opdaterer.

Når software-forhandlere finder løsninger til sårbarheder, så gør de disse løsninger tilgængelige gennem software-opdateringer. De fleste programmer har en indbygget opdateringsservice i deres software, som garanterer dig, at du bliver informeret, når der er en tilgængelig programrettelse. Nogle software-forhandlere installerer endda automatisk opdateringer, når de er tilgængelige.
Windows 10 Pro, som er den aktuelle udgivelse af Windows (og dermed også den sikreste), har en automatisk software-opdateringsmekanisme til at sørge for, at operativsystemet bliver opdateret og ligeledes alle andre Microsoft Office-programmer.

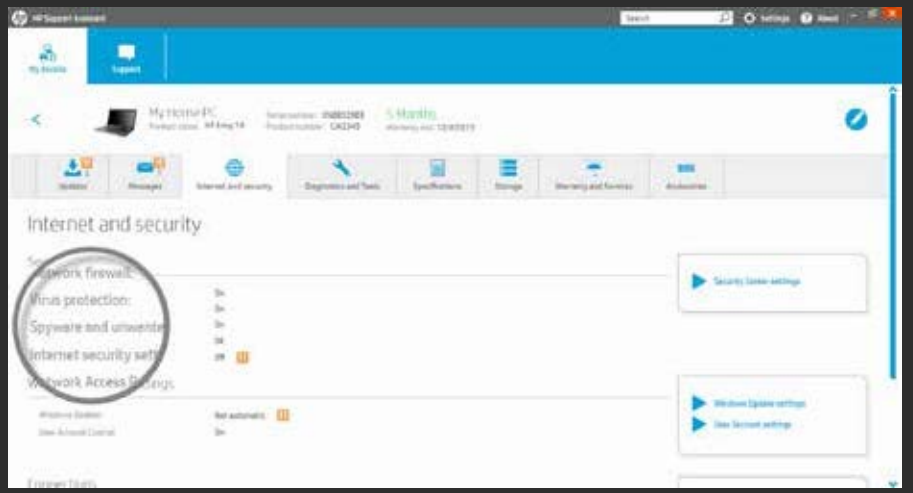
Sådan undersøger man, om automatiske opdateringer er aktiverede:

1. Gå til indstillinger og vælg "Opdater sikkerhed".
2. Under "Windowsopdatering" skal du vælge "avancerede muligheder" og sørge for, at "Automatisk" er valgt under "Vælg hvordan opdateringer skal installeres".
3. Sørg for, at "Automatisk" er valgt under "Vælg hvordan opdateringer skal installeres".

Brug opdateringsstyring.

Udvalget af software, der leveres sammen med din pc, kan gøre det vanskeligt at sikre, at *alt* bliver opdateret. Af denne grund tilvejebringer mange pc-forhandlere præinstallerede værktøjer til automatisk indsamling af alle software- og firmware-opdateringer til systemet. På HP-systemer kaldes dette værktøj for HP Support Assistant.

For tredjepartprogrammer køres opdateringsfunktionen ofte under bootning vha. et lille opdateringsprogram. Disse hjælpeværktøjer bevirker, at bootning varer et par sekunder længere, men det sparer dig for at skulle browse efter opdateringer på forhandlerens websites. Hvis du har software, som ikke automatisk kontrollerer for opdateringer, eller hvis du ikke er sikker, så kontroller versionsnummeret og sammenlign det med udviklerens website og opdater om nødvendigt, så det passer.



Afsnit 5:

Gør din browser sikker

Browsere som Internet Explorer eller Chrome™ er blandt de hyppigst anvendte metoder til at få adgang til internettet, hvilket gør dem til foretrukne mål for hackere. Disse angreb opstår typisk utilsigtet eller ved et uheld, fordi du klikker på et link, der starter en skadelig kode kendt som malware.

Der findes nogle få enkle trin, du kan tage til betydeligt at reducere faren for et malware-angreb via din browser.

Brug en sikker browser.

Internet Explorer, Edge, og Chrome™ tilbyder alle effektive sikkerhedsfunktioner til Windows. Edge og Internet Explorer 11 anvender f.eks. Microsoft SmartScreen til at udføre en vurdering af omdømme på hvert site og blokerer ethvert site, der mistænkes for at være et phishing-site. Derudover drager Internet Explorer fordel på HP commercial pc'er af yderligere sikkerhed i kraft af HP Sure Click: når en fane bliver åbnet, kører den på en isoleret virtuel maskine med HP Sure Click. Det betyder, at skadelig kode bliver fanget i fanen og bliver destrueret, når du lukker din browser.[13]

Overholdelsesadvarsler.

En sikker browser skal have en grundlæggende grænse for registrering af skadelige websites og vil vise en advarsel, hvis det betragtes, at der er en rimelig stor trussel. Nogle tilbyder også URL-"autokorrektionsfunktioner" for at forhindre navigering til et domæne, der ofte bliver stavet forkert (hvor skadelig software og sites ofte findes).

På Edge bedes du gå til Avancerede indstillinger > Privathed og derefter aktivere indstillingerne "Brug en webservice til at hjælpe med at løse navigationsproblemer"

Hold den opdateret.

Aktiver automatiske browser-opdateringer under Indstillinger. Som nævnt tidligere så sikrer man på denne måde, at alle sikkerhedsopdateringer bliver anvendt i din browser, hvilket gør den meget sikrere og øger chancen for, at malware-angreb vil mislykkes.

I Edge anvendes opdateringer samtidig med Windows-opdateringer. Hvis du imidlertid ønsker at kontrollere, om du har brug for en opdatering til Edge, bedes du gå til

- Start
- Indstillinger
- Opdateringer og sikkerhed
- Windows-opdatering
- Kontroller for opdateringer

Begræns indhold og plug-ins.

Mange af disse browseradd-ons (som Flash eller JavaScript) er nødvendige for udbytterige sites og webprogrammer, men den øgede adgang til dit system gør dem ligeledes sårbare.

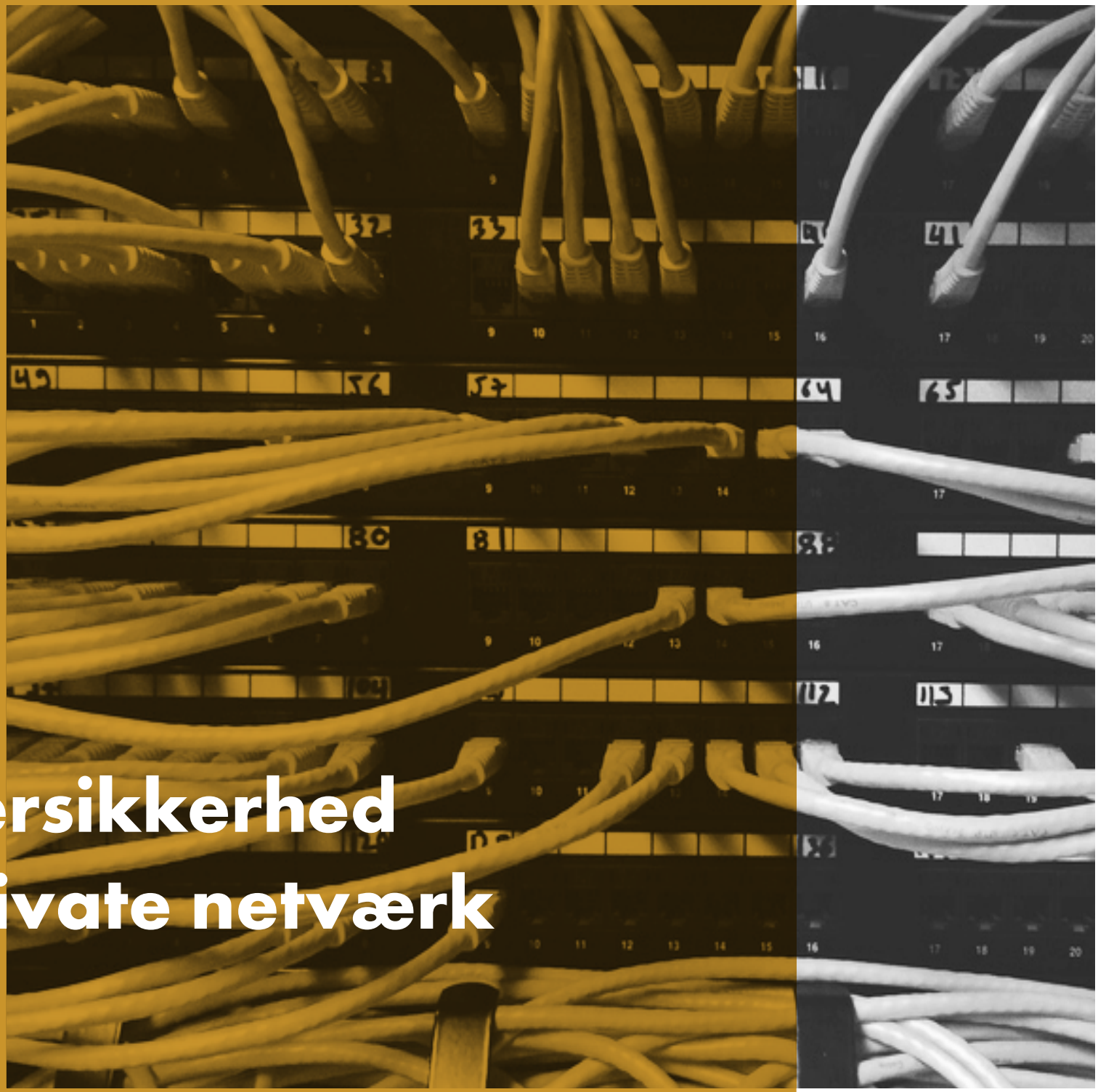
Microsoft Edge deaktiverer dem som standard og kræver, at et site anmoder om tilladelse til at anvende dem og sikrer, at det kun er sites, som du har tillid til, der kan bruge deres funktioner.

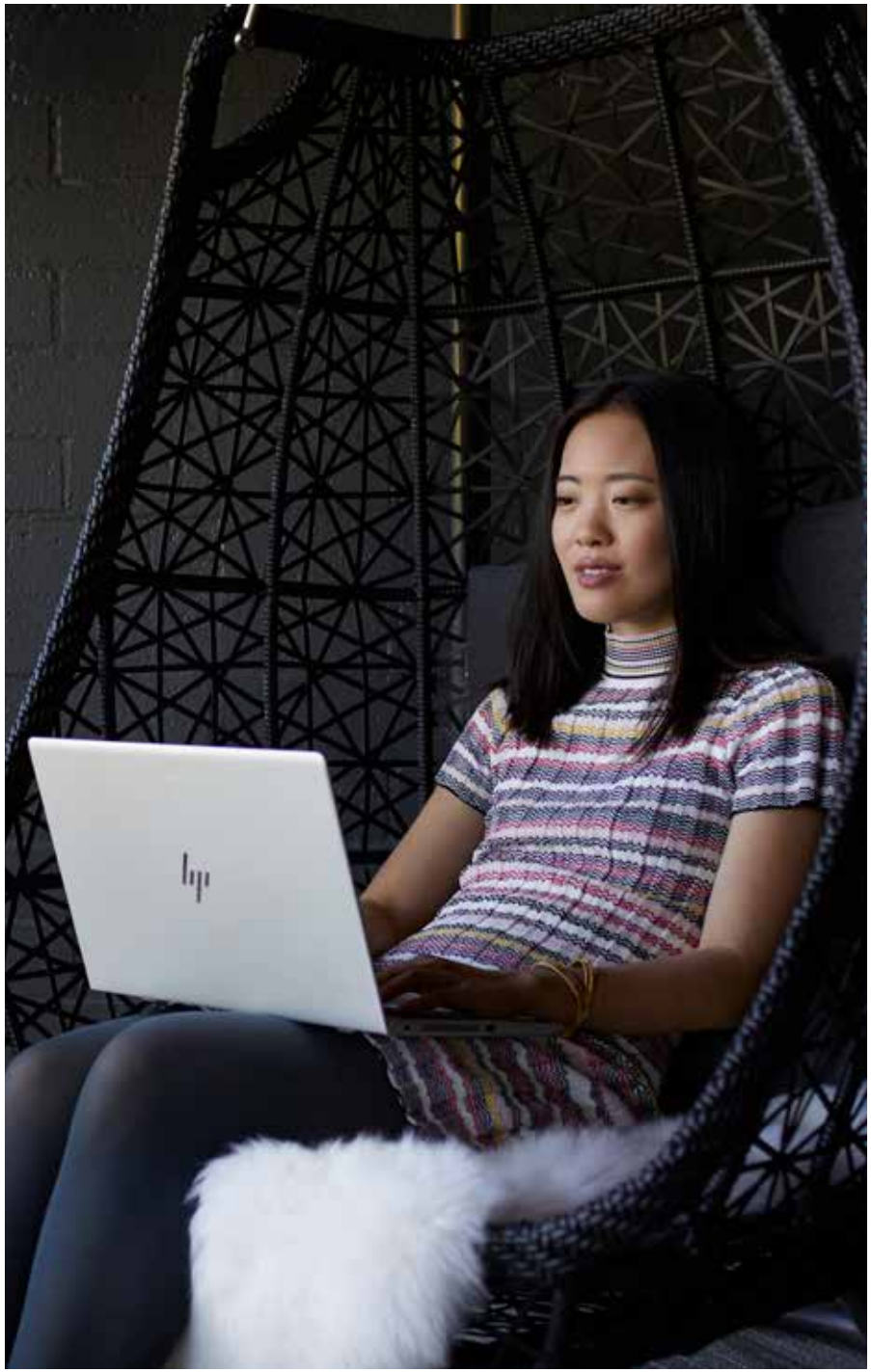
I IE, gå til Værktøj (gearikon) -> Internet indstillinger -> Sikkerhed -> Internet -> Brugerniveau... -> Scripting. Du kan deaktivere JavaScript ved blot at vælge "Deaktiver", eller du kan anmode IE om at forespørge, inden et site forsøger at bruge den ved at vælge "Prompt."

13—HP Sure Click er tilgængelig på de fleste HP pc'er og understøtter Microsoft® Internet Explorer og Chromium™. Understøttede vedhæftninger omfatter Microsoft Office (Word, Excel, PowerPoint) og skrivebeskyttede PDF-filer, hvis Microsoft Office eller Adobe Acrobat er installeret.

Afsnit 6:

Routersikkerhed og private netværk





Routeren er den første sikkerhedsforanstaltning mod indtrængen på ethvert netværk. Alle, som forbinder til internettet, gør det via en router. Denne hardware, enten forbundet eller trådløs (Wi-Fi®), der muliggør, at du kan kommunikere mellem dit lokale netværk (dvs. din pc og evt. andre tilsluttede enheder) og internettet. Som sådan er aktivering af det højeste sikkerhedsniveau på routeren den bedste måde at beskytte din pc, printer og data mod ondsindede angreb.

> Routere blev nævnt som den hyppigst misbrugte type enhed i loT-angreb.[14]

Eftersom routere transmitterer ALLE data, der strømmer ind og ud af dit hjem eller virksomhed indbefattet e-mail og kreditkortinformationer, har routere længe været et oplagt mål for hackerangreb. I Symantecs 2018 Internet Security Threat Report blev routere nævnt som den hyppigst anvendte type af enhed til loT-angreb. Hackere kan bruge malware eller defekter i design til at skjule deres identitet, stjæle båndbredde, konvertere dine enheder til botnetzombier eller det, der er værre. Så kan de også drage fordel af alle usikrede enheder.

14—Kilde: Symantec Corporation, 2018 Internet Security Threat Report, 2018

Gør dit netværk sikkert.

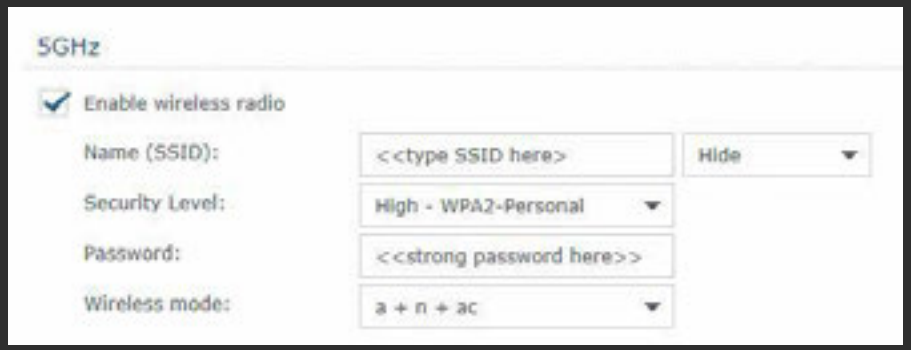
Desværre fortsætter mange forhandlere med at tilbyde både usikre og sikre router-konfigurationer. Hvis en router er usikker (dvs. tillader forbindelser til den uden at kræve en administrator-adgangskode), så kan alle tilslutte til den router og dermed få adgang til dit lokale netværk. En hacker kan ændre din adgangskode, udspionere dig eller få adgang til filerne på en netværksvedhæftet harddisk.

Du bør altid sikre dine routere med ikke-standard administrator-adgangskoder vha. tips fra afsnit 2: Styrk dine adgangskoder. Nedenfor er der et skærmbillede, der viser, hvordan de fleste routere tillader, at man indstiller adgangskoder for at sikre dem på netværket.

Opsæt kryptering.

Med trådløse routere udgør adgangskoder kun halvdelen af anstrengelserne, at vælge det passende krypteringsniveau er lige så vigtigt. De fleste trådløse routere understøtter fire trådløse krypteringsstandarder: WEP (svagest), WPA (stærk), WPA2 (stærkere), og WPA3 (stærkest). Vælg den højeste krypteringsstandard, som din router understøtter.

Nedenfor vises et skærmbillede af, hvordan du indstiller et passende krypteringsniveau på din router. For at gøre dette skal du logge på som router-administrator og navigere til krypteringsindstillingerne (varierer afhængig af router).



Sørg for, at firmwaren er opdateret.

Mange producenter af routere lancerer software-opdateringer i løbet af året for at håndtere sikkerhedsproblemer. Ligesom da vi talte om pc-software, så er en router med de seneste opdateringer meget mindre udsat for angreb med malware. De fleste forhandlere af routere bruger automatiske firmware-opdateringer uden at anmode kunden om at skulle foretage sig noget. De nyere router-modeller tilbyder evt. også en mobil app, som du kan hente på en telefon ligesom så mange andre apps, og du kan bruge den til at tjekke opdateringer. Hvis automatiske firmware-opdateringer ikke tilbydes af din routerforhandler, så skal du åbne producenten af routerens website, gå til Support og finde den rigtige opdatering afhængig af din routers specifikke modelnavn og id-nummer (findes normalt på selve routeren).

Brug virtuelle private netværk.

Hvis vi skal gå lidt videre end sikring af hardwaren på dit netværk, så er en Virtual Private Network (VPN) en server, som du forbinder til for at omdirigere dine eksterne internetaktiviteter. VPN kan beskytte og sikre din identitet og informationer. Formålet med en VPN er at tilvejebringe en mainstream måde at browse på internettet privat (men ikke altid anonymt). Al trafikken, som passerer gennem din VPN-forbindelse, er sikker og kan teoretisk ikke blive opfanget af nogen andre, det vil sige, at de er gode at anvende både på lokale netværk og offentlige. Du kan få mere at vide om VPN og deres fordele i Afsnit 7.

Afsnit 7:

Beskyt dig selv på offentlig Wi-Fi®

Nu til dags er offentlig Wi-Fi® nærmest allestedsnærværende. Lufthavne, lokale barer, shoppingcentre, ja endog parker tilbyder gratis internetforbindelse via hotspots. De er uhyre praktiske - og farlige.

Brugere, som er tilsluttet disse hotspots, deler samme netværk, dvs. at der er en stor fare for, at nogen kan misbruge den usikrede forbindelse. En hacker kan endog oprette en hotspot og forsøge at narre personer til at tilslutte på deres eget (falske) netværk. Dette kan resultere i ukrypterede datastrømme eller gennemførelse af replayangreb for at omgå kryptering.

Det er vigtigt altid at formode, at dine kommunikationer er usikrede og offentlige, når du bruger et åbent netværk. Hvis du imidlertid ikke har andre muligheder, kan du gøre noget for at reducere din eksponeringsgrad.

Begræns din aktivitet.

Undlad at transmittere meget følsomme oplysninger som virksomhedsdokumenter, e-mails eller adgangskoder, og anvend ikke nogen typer af bank- eller regnskabsprogrammer eller portaler.

Søg efter en plan B.

Om muligt brug et halvtåbent netværk, der som minimum er adgangskodebeskyttet. Disse er normalt et administreret netværk, hvilket vil sige, at udbyderen har en interesse i at bevare netværket sikkert (fx en salon i lufthavn).

Bliv på krypterede sites.

Sørg for, at du er tilsluttet til en webserver, der understøtter krypteret trafik via HTTPS-protokoller (https://), i modsætning til de usikrede almindelige tekst-HTTP-protokoller. Se overskriften på websitets URL. En moderne browser vil typisk have en ikon på URL-panelet, der angiver, når HTTPS er til stede, og om certifikatet er gyldigt (normalt et lille hængelåssymbol eller farven grøn). Hvis du klikker på dette sted, fremkommer der en dialogboks, der forklarer nærmere om krypteringsniveauet.

Send al trafik via en VPN.

Som vi nævnte i det forrige afsnit, kan en VPN hjælpe dig med at beskytte dine data, når du ikke har tillid til din netværksforbindelse, og et offentligt Wi-Fi®-netværk er et perfekt eksempel. En VPN-tunnel krypterer dine data fra start til slut og sørger for, at en mulig interceptor ikke kan forstyrre dine aktiviteter. Ikke alle VPN er ens, og derfor skal du vælge den rette ud fra pris og enhedstype. Gratis VPN har ofte begrænset tilgængelig båndbredde og anvender enkle krypteringsprotokoller, det betyder, at du vil opleve langsommere hastigheder, når du browser, og du kan stadigvæk være udsat. Når det er sagt, er det klart, at en velanskrevet og gratis VPN er bedre end ingen VPN overhovedet.

Afsnit 8:

Stop visuelle hackere

Visuel hacking forekommer, når følsomme oplysninger vises på skærmen på et offentligt sted, og virksomhedskonkurrenter, identitetstyve eller skruppelløse individer ser, indsamler eller udnytter oplysningerne. Selv den mest uskyldige tilskuer kan udgøre en potentiel trussel. Alt fra adgangskoder og kontonumre til finansielle data og proprietære virksomhedsoplysninger er i fare, og det bedste sikkerheds-software kan ikke forhindre, at disse individer får adgang til dine oplysninger.

Efterhånden som den moderne arbejdsplads fortsætter med at flytte ud af de traditionelle kontorlokaler til fjerne og offentlige steder, er faren for at blive offer for "visuel hacking" større end nogensinde. Faktisk er visuel hacking måske den mest undervurderede lavteknologiske trussel, virksomheder står overfor i dag. Det er enkelt, effektivt og foregår ofte ubemærket, indtil det er for sent.

Ifølge forskningsresultater der blev udgivet af Ponemon Institute[1]:

- Så var 91 % af alle visuelle hackingforsøg vellykkede
- 68 % af visuelle hackingforsøg foregik, uden ofret opdagede det
- 52 % af de følsomme oplysninger blev indsamlet direkte fra enhedens skærm

Vær opmærksom på dine omgivelser.

Når du arbejder på et offentligt sted, skal du altid formode, at nogen kunne kigge dig over skulderen, og vælg dine opgaver som følge heraf.

Begræns din eksponering.

Privathedsskærme er udformet til at reducere skærmens visningsvinkler, sådan at en mulig visuel hacker ikke kan se, hvad der står på skærmen, medmindre vedkommende befinder sig direkte foran skærmen. Et eksternt filter er en enkel måde at højne sikkerheden på. Det fastgøres over dit display og kan fjernes, når du ønsker at dele din skærm med et stort publikum.

Alternativt forenkler en indbygget privathedsskærm denne procedure samtidig med at fjerne behovet for at anvende, opbevare og udskifte en ekstern beskytter. Mange HP pc'er tilbyder HP Sure View 2. generation[15], som er en indbygget privathedsskærm, der er udformet til at forhindre muligheden for visuel hacking. Den fungerer ved at dynamisk ændre strukturen af LCD-pixels på molekylært niveau og muliggør, at den kan aktiveres og deaktiveres ved at trykke på en knap og forbedrer ydelsen både i lyse og mørke omgivelser.

15—HP Sure View indbygget privathedsskærm er en valgfri funktion, der skal konfigureres ved køb, og som er beregnet til at fungere i liggende retning.

Afsnit 9:

Krypter dine data

Når en pc bliver glemt eller stjålet, er harddisken det første, tyven går efter. Den kan udtages ved blot at løsne nogle få skruer og indsættes i en anden pc. Hvis du ikke har beskyttet dine data ordentligt, er det ligeså nemt at læse en harddisk, som det er at læse en bog.

Kryptering sørger for, at alt, der er blevet eksponeret, forbliver helt uforståeligt. Kryptering er en proces med kodning af data for at gøre disse ulæselige af andre, som ikke har den hemmelige dekrypteringsnøgle. Med andre ord kan en computer med en krypteret harddisk blive stjålet, men uden at tyven kan få adgang til dataene. Dette er langt bedre, end at dine virksomheds- eller personoplysninger ender i de forkerte hænder.

Aktiver software-kryptering.

Windows 10 Pro understøtter adgangskode-kryptering på din harddisk vha. dine loginbrugeroplysninger som nøglen. Dette betyder, at en hacker skal have dit brugernavn og adgangskode for at få adgang til dine data.

Sørg for at bruge en sikker adgangskode til din brugerkonto:

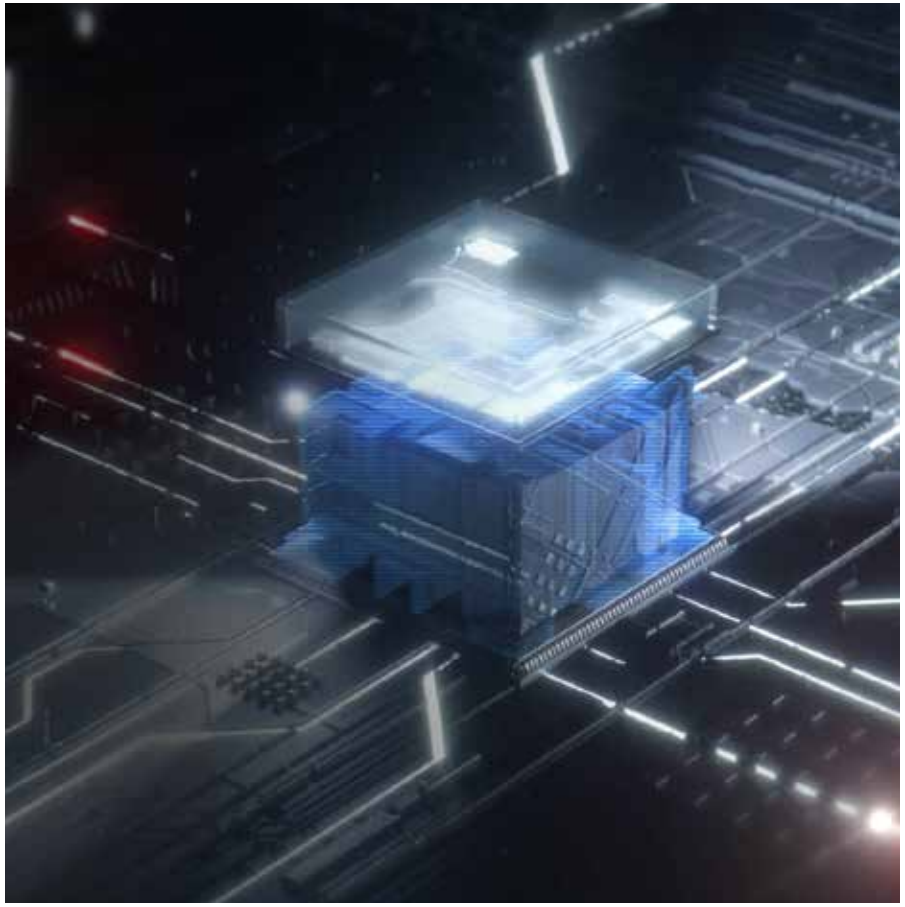
1.
   - Indstillinger > Konti > Log på muligheder > Adgangskode

2. Hvis tilgængelig så slå Trusted Platform Manager (TPM) til, hvilket aktiverer en sikkerheds-chip på din pc, så dine nye adgangskoder og data på harddisken bliver krypteret:
   - Indstillinger > Opdater og sikkerhed > Windowssikkerhed > Enhedssikkerhed > Processor

3. Slå kryptering til, hvilket sikrer, dine data ikke kan blive vist eller kopieret uden dine brugeroplysninger:
   - Indstillinger > Opdater og sikkerhed > Harddiskkryptering

Udnyt fordelene ved hardwarekryptering.

BitLocker er en funktion i Windows 10 Pro, der giver softwarekryptering, som åbnes med en hardwarenøgle. Enheder med en TPM-chip som HP notebooks kan krypteres uden brug af ekstra hardware. TPM'en forhindrer adgang til krypteret data, hvis den detekterer, at der er blevet pillet ved systemet, mens det var afbrudt. Enheder uden TPM kan også bruge BitLocker, men det kræver en udtagelig enhed såsom et USB-drev, der kan tjene som nøgle.



Afsnit 10:

Gør din pc sikker under OS

BIOS (Basic Input Output Software) er den software, der booter en computer og hjælper med at indlæse operativsystemet. Ved at inficere denne software kan spioner anbringe malware, der forbliver aktivt og ikke opdages af antivirusprogrammer. Den forbliver der, selvom harddisken bliver formateret eller operativsystemet bliver geninstalleret.

Hvis en hacker får adgang til din BIOS, ejer vedkommende i realiteten din pc.

Dette giver den kriminelle en mulighed for at infiltrere data eller hacke systemet ved at ændre firmwaren, hvilket kunne betyde udskiftning af hele motherboardet. For HP Elite og Pro pc'er, HP Sure Start kan automatisk selvudbedre BIOS fra malware, rootkits eller korruption, idet der tilføjes et ekstra beskyttelseslag, og der oprettes et pålideligt grundlag for din pc's sikkerhed.[16]

Husk at opdatere.

Som nævnt i afsnit 4 så sikrer software-opdateringer, at nye sårbarheder bliver fejlrettet, og BIOS'en er ingen undtagelse. Eftersom de fleste BIOS-implementeringer deler den samme kildekode med medarbejderstaben eller brugerbasen, så vil enhver sårbarhed, der bliver opdaget, udgøre en trussel i mange implementeringer blandt pc-forhandlerne. OEM-værktøjer som HP Support Assistant kontrollerer automatisk for opdateringer, eller du kan kontrollere producentens website for BIOS-opdateringer.

Udforsk BIOS'en.

BIOS-fabriksindstillingerne kan betragtes som en balance mellem sikkerhed og brugbarhed. For at beskytte systemet mod de mange trusler i forbindelse med overførsel af skadelig kode kan det være, at du vil fjerne nogle af værktøjerne.

Måden, man får adgang til BIOS-indstillingerne, varierer en smule fra producent til producent, men normalt foregår det ved at trykke på en funktionstast under bootning (F10 eller FN-10 på HP notebooks).

16—HP Sure Start 4. generation er tilgængelig på HP Elite- og HP Pro 600-produkter udstyret med 8. generation af Intel- eller AMD-processorer.

Indstil en BIOS-adgangskode.

For at beskytte BIOS-indstillingerne mod at blive ændret af uvedkommende anbefales det at oprette en BIOS-adgangskode:

- For eksempel: Sikkerhed > Administratorværktøjer > Opret BIOS Administratoradgangskode

Det er vigtigt at huske BIOS-adgangskoden, eftersom den ikke kan omgås eller genskabes.

Opret en adgangskode til start af computer.

Hvis du ønsker et endnu højere sikkerhedsniveau, kan du oprette en adgangskode til start af din computer. Hver gang pc'en tændes, og inden systemet udfører nogen handling, bliver du anmodet om en start-adgangskode. Ligesom BIOS-adgangskoden kan denne heller ikke genskabes eller nulstilles, og hvis du glemmer den, er maskinen ubrugelig.

Begræns brugen af ubenyttede funktioner.

I BIOS er der nogle få indstillinger, du bør overveje af hensyn til maksimal sikkerhed. Skønt de kan fjerne visse funktioner eller reducere adgangen, så kan nedenstående OS-sikkerhed, de aktiverer, ikke kopieres med software:

1. Fjern eksterne og optiske enheder fra bootningrækkefølgen (fx Avanceret > Bootningegenskaber). Specielt USB Storage Boot, Network (PXE) boot og optisk drevboot, da disse gør det muligt for malware at blive indlæst fra eksterne kilder. Hvis bootning fra disse enheder er påkrævet, kan denne funktion slås til efter behov.
2. Deaktiver Legacy Support (fx: Avanceret > Sikker bootkonfiguration) og aktiver Sikker bootning.
3. Aktiver funktionen "Gem/Genopret GPT af systemets harddisk" (fx: Sikkerhed > Harddiskværktøjer).
4. Aktiver DriveLock og opret en adgangskode.

Konklusion

Nu til dags er flere digitale trusler rettet mod små og mellemstore virksomheder end nogensinde tidligere. Det gode ved det er, at meget af hardwaren og softwaren, du ejer, indeholder underudnyttede sikkerhedsfunktioner, der hjælper med at bekæmpe truslerne. Der findes derudover et uhørt antal af tilgængelige produkter og tjenester med de mest avancerede sikkerhedsfunktioner, der beskytter mod fremtidens ukendte trusler. Fra hardwarebaseret sikkerhed på nutidens enheder til selvopdaterende software, en smart investering på tilsluttede, sikre enheder vil kunne betale sig på længere sigt. HP designer sikkerhedsløsninger, der drager fordel af styrkerne i Windows 10 Pro og understøtter de indbyggede sikkerhedsfunktioner med diskrete hardwareforøgelser og opdateret software-support. De trusler, du bliver konfronteret med, udvikles hele tiden, og den rigtige sikkerhedsstrategi øger betydeligt dine chancer overfor dem.

TAK.

Hvis du ønsker at få mere at vide, så besøg
www.hp.com/go/windows10now

Vær mere sikker, fra du tænder, og indtil du slukker.