+ Windows 10

DE CYBER-BEVEILIGING PRAKTIJK-HANDLEIDING

Tien stappen die ieder bedrijf zou moeten toepassen om te beschermen tegen cyberaanvallen.

Zorg dat u continu beveiligd bent.

Het landschap van cyberbeveiliging verandert steeds en breidt steeds verder uit. Kleine en middelgrote bedrijven worden steeds vaker geconfronteerd met cyberaanvallen die hun informatie en de persoonsgegevens van hun klanten bedreigen. Deze handleiding is bedoeld als hulp voor kleine en middelgrote bedrijven met beperkte IT-bronnen om hun cyberbeveiliging vandaag nog te versterken, tegen geringe of geen kosten.

INHOUDSOPGAVE

Het Dreigings-landschap

Cyberbeveiligings-trends in kleine en middelgrote bedrij-ven

Dit zijn vijf van de toptrends in de cyberbeveiliging voor kleine en middelgrote bedrijven, volgens het Ponemon Institute[1]:

1. **Steeds meer bedrijven worden aangevallen.**
In de afgelopen 12 maanden zijn cyberaanvallen bij kleine en middelgrote bedrijven toegenomen met 11%, van 55% tot 61%. De meest voorkomende aanvallen bij kleine bedrijven zijn phishing/social engineering (48%) en webgebaseerd (43%). Tegelijkertijd worden cyberaanvallen steeds doelgerichter, ernstiger en geavanceerder.

2. **Aanvallen worden steeds kostbaarder.**
De gemiddelde kosten door onderbreking van de normale activiteiten zijn met 26% gestegen, van $955.429 tot $1.207.965. De gemiddelde kosten wegens schade of diefstal van IT-eigendommen en infrastructuur stegen van $879.582 tot $1.027.053.

3. **Menselijk falen is een hoofdoorzaak.**
Van de kleine en middelgrote bedrijven die een datalek hadden, gaf 54% aan dat onachtzame medewerkers de oorzaak waren, een toename van 48% ten opzichte van afgelopen jaar. En net als vorig jaar kon 1 van de 3 bedrijven bij dit onderzoek de oorzaak niet achterhalen.

4. **Sterke wachtwoorden en multi-factor authenticatie blijven onderbelicht.**
Wachtwoorden blijven een integraal onderdeel van cyberbeveiliging. Maar 59% van de respondenten geeft aan dat ze geen zicht hebben op de wachtwoordpraktijken van hun medewerkers, zoals het gebruik van unieke of sterke wachtwoorden en het delen van wachtwoorden met anderen - hetzelfde als vorig jaar.

> 59% geeft aan dat ze geen zicht hebben op de wachtwoordprak-tijken van hun medewerkers

5. **Malware wordt steeds geavanceerder.**
Steeds meer bedrijven zijn slachtoffer van aanvallen en malware die door hun bestaande bescherming zijn gedrongen, zoals indringersdetectie (66%, gestegen van 57%) en antivirusoplossingen (81%, gestegen van 76%).

1—Rapport: 2017 Staat van cyberbeveiliging in kleine en middelgrote bedrijven. Ponemon Institute LLC, 2017

De vijf meest voorkomende aanvallen bij kleine en middelgrote bedrijven.

1

Phishing/social engineering

Social engineering valt menselijke interactie aan om informatie te verkrijgen over een organisatie of de daar gebruikte computersystemen. Zo kan een aanvaller zich presenteren als nieuwe medewerker, reparateur of onderzoeker. Door vragen te stellen kan hij of zij stukjes informatie verzamelen om te kunnen infiltreren in het netwerk van een organisatie.[2]

Phishing is een vorm van social engineering. Bij een phishing-aanval doet de aanvaller zich voor als betrouwbare organisatie, en wordt gebruikgemaakt van e-mail of kwaadaardige websites om persoonsgegevens te bemachtigen.[2]

2

Webgebaseerde aanvallen

Bij webgebaseerde aanvallen krijgt de aanvaller toegang tot een legitieme website en plaatst daar malware. De legitieme website doet dienst als verspreider naar nietsvermoedende bezoekers. Een van de meest voorkomende soorten van webgebaseerde aanvallen is een 'drive-by-download', waarbij de schadelijke inhoud automatisch wordt gedownload naar de pc van de gebruiker als die alleen de website maar bezoekt. Daarbij is geen gebruikershandeling nodig.[3]

3

Malware

Malware is een breed begrip dat verwijst naar alle software die bewust is ontworpen om schade toe te brengen aan een apparaat of netwerk.[4] Dit omvat virussen, spyware, ransomware en alle andere '-ware'. Naast webgebaseerde aanvallen kan dit op een computer van een slachtoffer terechtkomen via een USB-schijf of besmette netwerkverbinding.[5]

4

Aangetaste/gestolen apparaten

Een apparaat dat is gecompromitteerd of gestolen kan zowel waardevolle informatie als lokaal opgeslagen accountgegevens bevatten waarmee verdere toegang tot het netwerk of de informatie van een bedrijf mogelijk is. Zwakke wachtwoorden en gegevensencryptie kunnen zo'n aanval verder versterken.

5

Denial of service-aanvallen

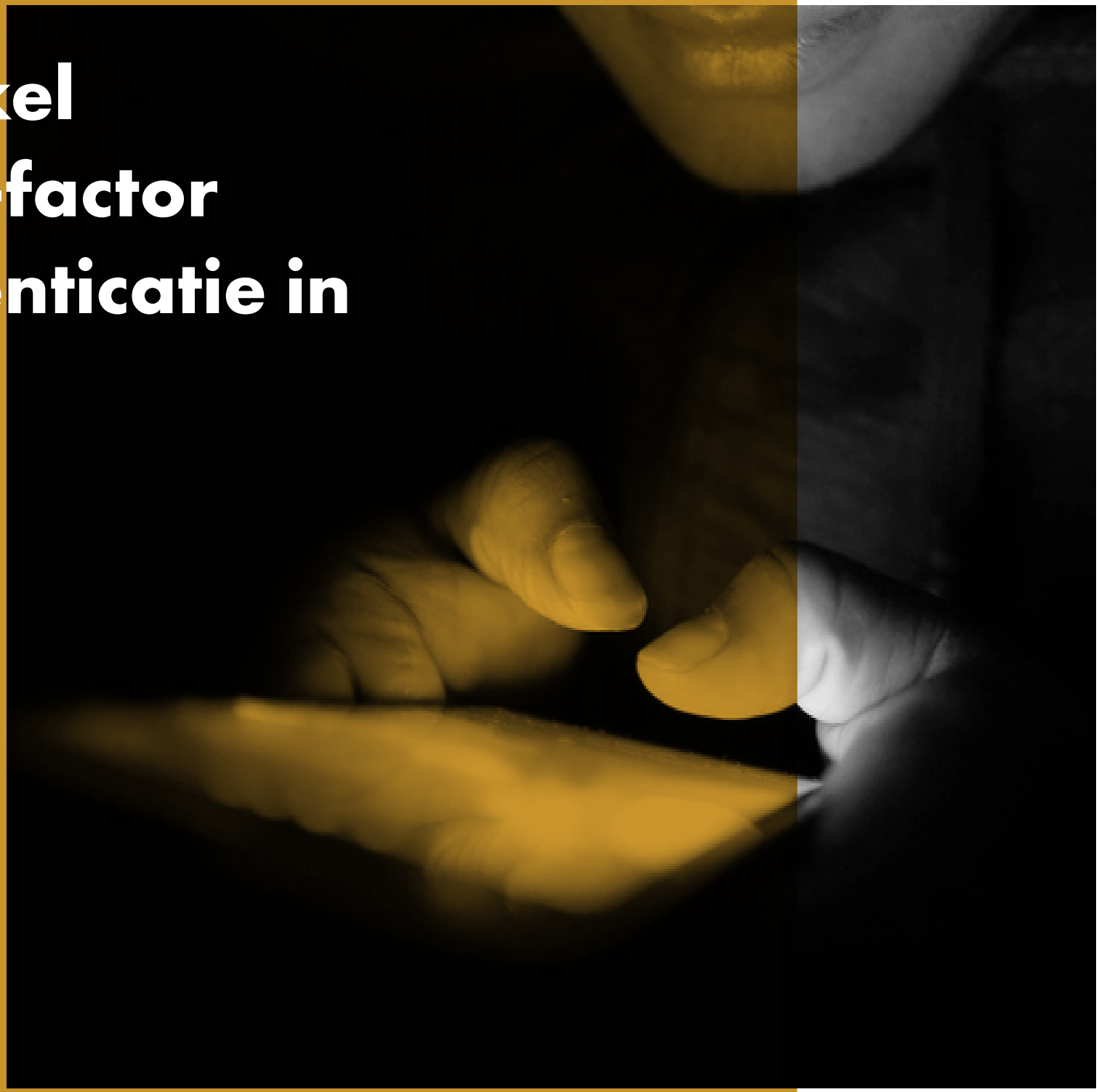
Denial of service-aanvallen worden uitgevoerd door het beoogde netwerk te bestoken met verkeer totdat dit niet meer kan worden verwerkt en het netwerk crasht, waarna toegang voor de legitieme gebruikers onmogelijk is. Een gedistribueerde denial of service-aanval (DDoS) vindt plaats als meerdere machines samenwerken om een doel aan te vallen, waarmee de kracht van een aanval toeneemt. DDoS maakt het ook moeilijker om de echte bron te vinden.[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

Tien manieren om uzelf te beschermen

Sectie 1:

Schakel multi-factor authenticatie in



Gebruikersnamen en wachtwoorden zijn een hoofddoel voor hackers, en met een goede reden - uw identiteit is uw kostbaarste bezit. Met sterke en veilige wachtwoorden komt u een heel eind, maar wachtwoorden alleen zijn niet het meest veilige authenticatiemechanisme. En in een wereld met toenemende commerciële hacking kunnen dieven die geen expert zijn dat uitbesteden aan anderen. Hackers kunnen speciaal ontwikkelde hardware kopen voor het kraken van wachtwoorden, ruimte huren bij openbare cloudaanbieders of een botnet maken om de verwerking te doen.

- 90% van de gestolen gegevens met phishing zijn gebruikersgegevens[7]
- 80-90% van de wachtwoorden kan binnen 24 uur gehackt worden[8]

Multi-factor authenticatie (MFA) vereist dat u twee of meer onafhankelijke aanmeldmethoden gebruikt om uw identiteit te bevestigen, waarmee uw beveiligingsniveau enorm verhoogd wordt. Aanmeldgegevens kunnen iets zijn dat de gebruiker **weet** (wachtwoord of PIN-code), iets dat de gebruiker **heeft** (Bluetooth®-telefoon of smartcard), of iets dat de gebruiker **is** (gezichtsherkenning of vingerafdruk). Als een onderdeel gelekt of gekraakt is, moet de aanvaller nog een tweede en andere manier van toegang doorbreken.

HP MFA en Intel® Authenticate ondersteunen beide meerdere authenticatiemethoden die vereist zijn bij elke aanmeldpoging.

7—Verizon, 2016 Data Breach Investigations Report, 2016
8—Bron: Brian Contos, CISO bij Verodin, Inc. Geciteerd met toestemming. https://www.csoonline.com/article/3236716/authentication/how-hackers-crack-passwords and-why-you-cant-stop-them.html

Instellen van multi-factor authenticatie met HP.

Moderne HP Pro of Elite-apparaten ondersteunen het instellen van MFA via de HP Client Security Manager.[9]

1. Open Client Security Manager (u heeft hiervoor beheerdersrechten nodig). Als u deze opent binnen HP's Manageability Integration Kit (MIK), dan kunt u uw MFA-beleid doorvoeren binnen uw gehele computerpark.[10]
2. Klik vanaf het Dashboard op Standaard Gebruiksbeleid.
3. Kies de twee of drie methoden waarvoor u het aanmeldbeleid wilt instellen, en volg de aanwijzingen zoals gevraagd om de aanmeldgegevens of aanmeldcombinatie in te stellen — zoals scannen van een vingerafdruk van de vingerafdruklezer van de computer of het invoeren van een PIN-code.

Wissel af met Windows Hello.

Veel moderne Windows 10 Pro-apparaten met een ingebouwde webcam zijn compatibel met Windows Hello, waaronder een hele reeks HP-notebooks en tussenapparaten. Windows Hello geeft u de mogelijkheid om uw gezicht te scannen en biedt daarmee een alternatief op uw wachtwoord als een van uw MFA-aanmeldgegevens.

1. Open Instellingen> Accounts> Aanmeldopties
2. Selecteer onder 'PIN' de optie 'Toevoegen' als u dit nog niet heeft ingesteld.
3. Selecteer onder 'Windows Hello' de optie 'Instellen', en volg de instructies op het scherm om uw gezicht te scannen.

9—HP Client Security Manager Gen4 vereist Windows- en Intel®- of AMD-processoren van de 8ste generatie.
10—De HP Manageability Integration Kit kan worden gedownload via http://www.hp.com/go/clientmanagement.

Sectie 2:

Versterk uw wachtwoorden

Wachtwoorden zijn overal in ons dagelijks leven aanwezig. We gebruiken ze voor bijna elk apparaat, dienst en account, privé of zakelijk. Omdat ze de eerste en vaak de enige stap zijn in het beschermen van identiteit en gegevens, kan het gebruik van slechte wachtwoorden desastreuze gevolgen hebben. Ondanks dat gebruiken de meeste mensen geen sterke en unieke wachtwoorden.

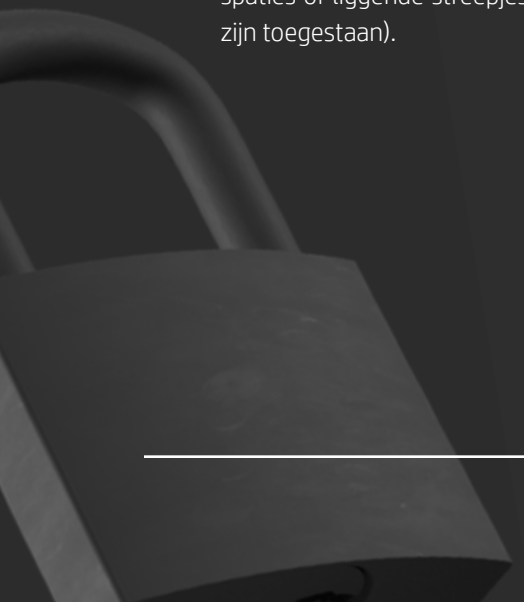
- 59% weet dat een veilig wachtwoord belangrijk is, maar slechts 41% gebruikt een wachtwoord dat eenvoudig te onthouden is
- 91% begrijpt het risico van het hergebruik van wachtwoorden, maar 55% doet het toch
- Millennials gebruiken doorgaans sterkere wachtwoorden dan Baby Boomers (65% t.o.v. 45%)[11]

Als uw apparaat of dienst MFA niet ondersteunt, is de beste oplossing om een zo moeilijk mogelijk wachtwoord te gebruiken. De meeste mensen hebben geen sterke wachtwoorden omdat ze gewoon niet weten hoe ze die moeten aanmaken, omdat ze denken dat het een willekeurige combinatie van letters, cijfers en tekens moet zijn. Maar er zijn sterkere en eenvoudigere manieren om uw niveau van wachtwoordbescherming enorm te verbeteren.

11—Bron: LastPass, "Nieuw onderzoek: Psychology of Passwords, Neglect is Helping Hackers Win", Katie Petrillo, 1 mei, 2018

Ezelsbruggetjes in plaats van getallen.

Wachtwoordzinnen met een ezelsbruggetje zijn veiliger dan eenvoudige wachtwoorden en eenvoudiger te onthouden dan een getallencombinatie.
Een ezelsbruggetje, in tegenstelling tot een eenvoudig wachtwoord, is haast onmogelijk te kraken voor hackers.



1 Maak een wachtwoord met een ezelsbruggetje.

De eerste zes woorden van Abraham Lincoln's bekende Gettysburg Address-toespraak, "Four score and 7 years ago" is bijvoorbeeld een eenvoudige wachtwoordzin. Deze voldoet aan het merendeel van de wachtwoordstandaarden: 8-32 tekens in lengte en met hoofdletters en kleine letters, minimaal één getal en een speciaal teken (de spaties of liggende streepjes als spaties niet zijn toegestaan).

2 Zorg voor maximale moeilijkheid.

Verhoog het aantal getallen en speciale tekens. Pas bijvoorbeeld de tekst van ons vorige voorbeeld aan naar:
'4 $core @nd 7 Ye@rs ago'.

3 Pas dit zelf aan, kopieer het niet.

Door een eenvoudig achtervoegsel achter elke wachtwoordzin te plaatsen kunt u uw hoofdwachtwoord hergebruiken zonder het gevaar van dubbel gebruik. Voor een Facebook-account kunt u 'FB' aan het einde toevoegen of u kunt 'IG' voor Instagram gebruiken.

Gebruik een wachtwoordmanager.

Wachtwoordmanagers zijn een van de meest veilige manieren die door beveiligingsexperts worden aanbevolen. Ze werken door het maken en opslaan van lange, moeilijke wachtwoorden voor elk van uw online accounts; die u niet meer hoeft te onthouden. U hoeft nog maar één wachtwoord te onthouden, het hoofdwachtwoord naar uw 'kluis'. Instellen van een wachtwoordmanager is eenvoudig en het proces is vaak hetzelfde:

1. Download en installeer de software en een plugin voor uw browser. U kunt ook een app downloaden voor uw mobiele apparaat.
2. Stel uw account in met een e-mailadres en uw hoofdwachtwoord.
3. Voer de details van uw verschillende accounts in.

De meeste wachtwoordmanagers vereisen dat u handmatig uw oude wachtwoorden bijwerkt: meld u aan bij uw account, ga naar de accountinstellingen en laat uw wachtwoordmanager een nieuw, veiliger wachtwoord maken. Vervangen van uw oude zwakke wachtwoorden kan tijd kosten, maar de significante verbetering van uw beveiliging is het waard.

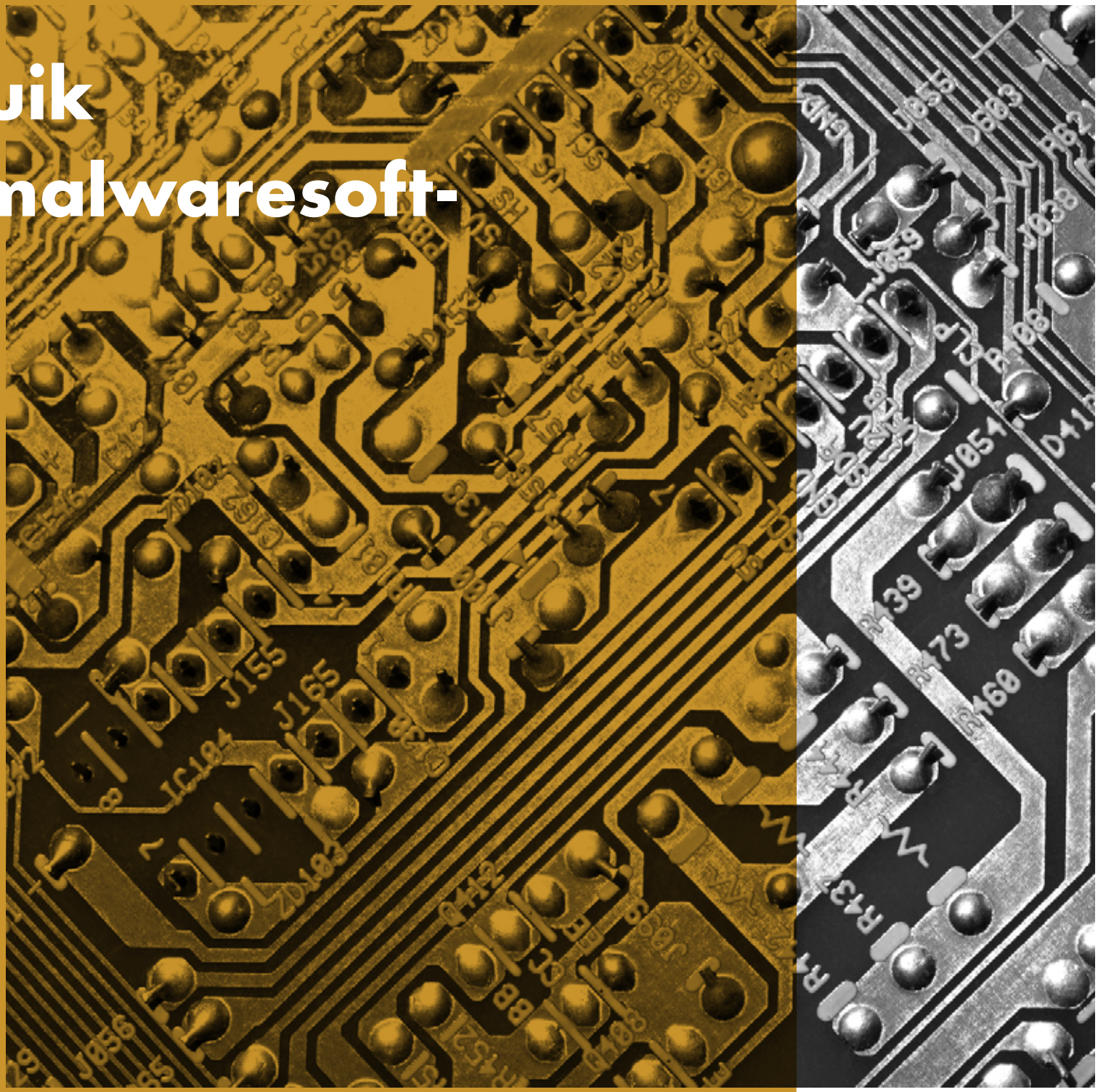
Kiezen van een wachtwoordmanager.

Er zijn talloze gratis wachtwoordmanagers beschikbaar, waaronder Bitwarden, Dashlane en Enpass. Kies in het algemeen een wachtwoordmanager die:

- Eenvoudig te integreren is in de browser die u het meest gebruikt
- U in staat stelt het wachtwoordbestand versleuteld op te slaan, onleesbaar voor gebruikers zonder de vereiste aanmeldgegevens. Kies specifiek een wachtwoordmanager die gebruikmaakt van AES-256-encryptie of sterker.
- Two-factor authenticatie mogelijk maakt om de wachtwoordkluis te openen.
- Een contact voor noodgevallen toewijst die ook toegang heeft tot de wachtwoordkluis.
- Aanvullende inloggegevens samen met een wachtwoord opslaat (zoals beveiligingsvragen, telefoonnummers, accountdetails, enz.)

Sectie 3:

Gebruik Anti-malwaresoft-ware



Zonder antivirusbescherming zou een pc binnen enkele minuten na verbinding met het internet besmet kunnen raken met malware.

Malware in alle soorten en maten kan worden gehost op schijnbaar betrouwbare websites of worden verborgen in e-mailbijlagen, en elke dag komt er nieuwe malware bij. De stroom van virussen richting uw pc is constant, dus moet een tool die bescherming biedt sterk en diepgaand zijn en regelmatig worden bijgewerkt. Een goed anti-malwareprogramma is alle drie.

Kort samengevat is anti-malwaresoftware een programma of set van programma's die bescherming bieden tegen en zoeken naar softwarevirussen, en ze detecteren of verwijderen (en andere schadelijke software zoals wormen, Trojaanse paarden, adware en meer). Een standaard anti-malwareprogramma scant uw systeem regelmatig en verwijdert automatisch de malware die het vindt, en geeft ook meldingen over gevaarlijke downloads en software-updates.

Zorg dat u het ook gebruikt.

Er zijn veel anti-malwareproducten beschikbaar. Als u op uw computer Windows 10 Pro geïnstalleerd heeft, is daarop al Windows Defender Antivirus geïnstalleerd en actief. U kunt ook een anti-malwareprogramma van derden aanschaffen. Volg echter wel de instructies van de fabrikant voor het instellen van automatische updates, zodat u altijd het meest actuele virusbestand gebruikt.

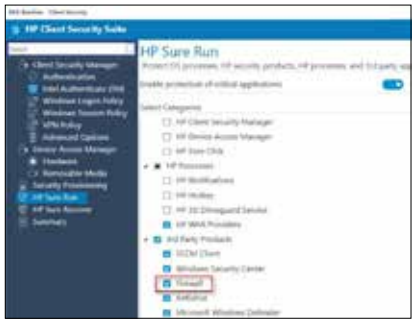
Altijd actief.

Het is uiterst belangrijk dat anti-malwaresoftware altijd moet draaien om zijn werk te kunnen doen. Omdat het gebruikelijk is dat aanvallers met malware zich eerst richten op beveiligingsprogramma's zoals anti-malware, is deze stap niet zo eenvoudig als het lijkt. In Windows 10 Pro kunt u controleren of uw antivirusprogramma momenteel is ingeschakeld door te kijken in het Windows Defender Beveiligingscentrum.

1. Ga vanuit het Startmenu naar het Windows Defender Beveiligingscentrum en ga naar Home.

2. Onder de instelling 'Virus- en bedreigingsbescherming' ziet u een groen vinkje als er een antivirusprogramma draait. Als u gebruikmaakt van een antivirusprogramma van derden, klikt u op 'Bekijk Antivirusleveranciers' om aanvullende beveiligingsgegevens te zien in het Windows Configuratiescherm over de status van uw antivirusprogramma.

En houd het actief.



HP Elite-producten omvatten ook HP Sure Run[12], een extra beveiligingslaag die waarborgt dat al uw kritieke processen op uw pc, waaronder uw antivirussoftware, blijven draaien. Elk proces dat Sure Run in de gaten houdt, wordt automatisch herstart als het uitgeschakeld wordt - zodat uitgeschakelde of vastgelopen antivirussoftware ervoor zorgt dat u kwetsbaar bent.

HP Sure Run moet lokaal ingeschakeld zijn in HP Client Security Manager Gen4.

12—HP Sure Run is beschikbaar op HP Elite-producten die uitgerust zijn met 8ste generatie Intel®- of AMD®-processoren.

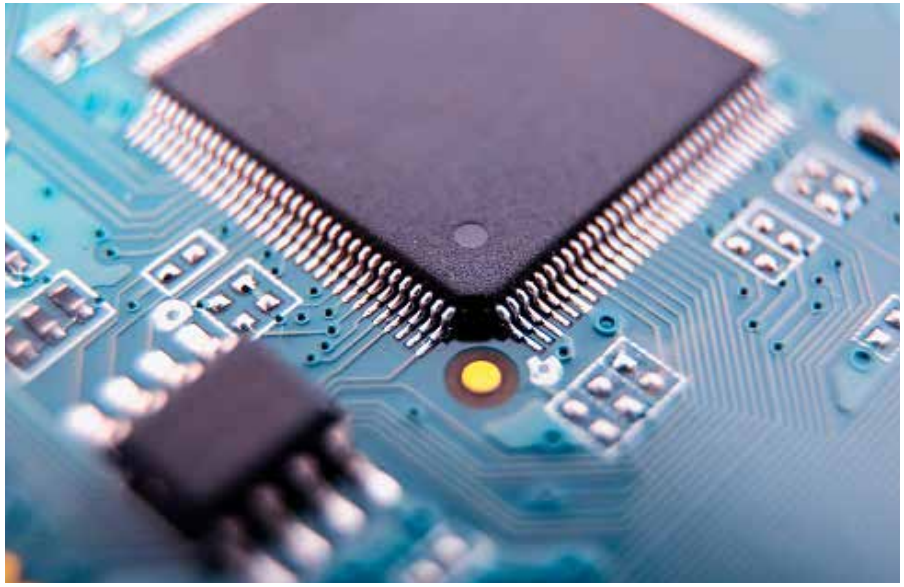
Sectie 4:

Houd uw software up-to-date

Anti-malware is niet de enige soort software die toenemende dreiging ervaart; het is belangrijk dat u al uw software up-to-date houdt. Als uw software niet up-to-date is, kan er belangrijke informatie ontbreken van onlangs ontdekte kwetsbaarheden. Dit is van toepassing op zowel het besturingssysteem (OS) als Windows® en alle applicaties die op de pc draaien, zoals internetbrowsers, Office-toepassingen, boekhoudsoftware, antivirussoftware, enz.

De gebruiker moet zich er ook van bewust zijn dat oudere of niet meer ondersteunde software niet langer wordt voorzien van updates. Cybercriminelen vinden op een gegeven moment kwetsbaarheden in uitgebrachte software en profiteren daarvan. Zo kan er bijvoorbeeld bij het controleren op een update voor Windows 7 Pro geen nieuwe software gepresenteerd worden, maar dan wordt over het hoofd gezien dat Windows 7 Pro niet de meest actuele versie van Windows is. Patchen van oudere software is niet hetzelfde als updaten naar de laatste versie; hoe ouder uw software, hoe minder veilig het is.

> Hoe ouder de software, hoe minder veilig het is



Controleer of u updatet.

Als softwareleveranciers oplossingen vinden voor kwetsbaarheden, bieden ze die oplossingen aan via software-updates. De meeste applicaties hebben een updateservice ingebouwd, die ervoor zorgt dat u een melding krijgt als er een update of patch beschikbaar is. Sommige softwarefabrikanten installeren de updates zelfs automatisch als deze beschikbaar zijn.
Windows 10 Pro, de meest recente versie van Windows (en dus de veiligste), heeft een geautomatiseerd mechanisme voor software-updates - en alle andere Microsoft-applicaties zoals Microsoft Office ook.

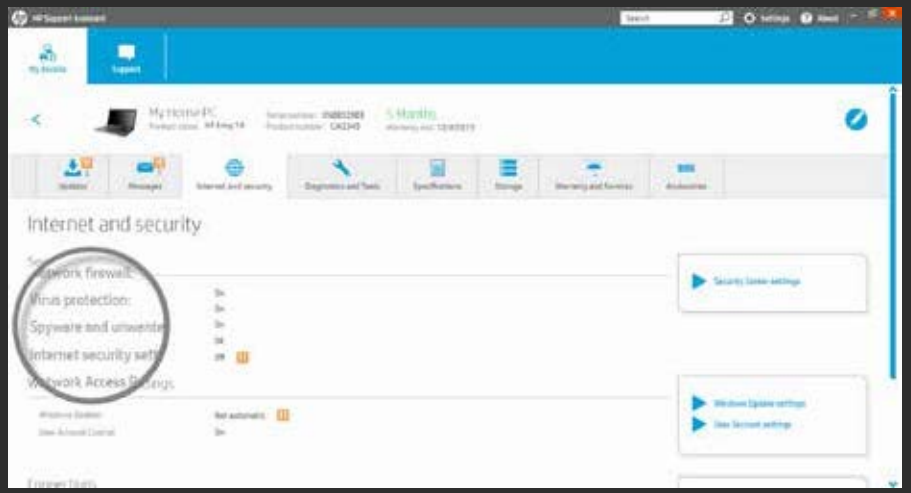
Om te controleren of automatische updates ingeschakeld zijn:

1. Ga naar instellingen en kies 'Beveiliging bijwerken'.
2. Kies onder 'Windows Update' voor 'geavanceerde opties' en zorg dat 'Automatisch' geselecteerd is onder 'Kiezen hoe updates geïnstalleerd worden.'
3. Zorg ervoor dat 'Automatisch' is geselecteerd onder 'Kiezen hoe updates geïnstalleerd worden.'

Gebruik een updatemanager.

De vele programma's op uw pc kunnen het lastig maken om ervoor te zorgen dat *alles* bijgewerkt is. Om die reden bieden veel pc-fabrikanten vooraf geïnstalleerde tools om automatisch alle software- en firmware-updates voor het systeem te verzamelen. Op HP-systemen heet deze tool de HP Support Assistant.

Voor applicaties van derden wordt de updatefunctie vaak uitgevoerd voor een kleine updatetoepassing die wordt gestart bij het opstarten. Deze tools zorgen voor een iets langere opstarttijd, maar dan hoeft u niet meer op de websites van de fabrikanten te zoeken naar updates. Als u software heeft die niet automatisch controleert op updates, of als u dat niet zeker weet, vergelijk dan het versienummer met dat op de website van de fabrikant en update indien nodig.



Sectie 5:

Beveilig uw browser

Browsers, zoals Internet Explorer of Chrome™, zijn de eerste stap waarmee we het internet op gaan, en daarmee het belangrijkste doelwit voor hackers. Deze aanvallen vinden vaak plaats doordat er per ongeluk of onbedoeld op een link geklikt wordt die schadelijke code, ook wel bekend als malware, opent.

Er zijn enkele eenvoudige stappen die u kunt uitvoeren om de kansen om een malware-aanval via de browser drastisch te verlagen.

Gebruik een veilige browser.

Internet Explorer, Edge en Chrome™ bieden allemaal sterke beveiliging voor Windows. Edge en Internet Explorer 11, bijvoorbeeld, gebruiken Microsoft SmartScreen om een reputatiecheck te doen op elke website, en ze blokkeren alles wat wordt gezien als phishing. Daarnaast profiteert Internet Explorer op commerciële pc's van HP van de aanvullende beveiliging van HP Sure Click: als er een tabblad geopend wordt, voert HP Sure Click deze uit in een geïsoleerde virtuele machine. Dit betekent dat alle schadelijke code in dat tabblad blijft en wordt verwijderd als u uw browser sluit[13].

Zorg dat u de laatste versie gebruikt.

Schakel automatische browserupdates via Instellingen in. Zoals eerder verteld, zorgt u er daarmee voor dat alle beveiligingsupdates in uw browser worden verwerkt, waardoor deze veel veiliger wordt en de kans dat aanvallen zullen mislukken wordt vergroot.

In Edge worden updates toegepast als Windows wordt geüpdatet. Als u wilt controleren of u een update nodig hebt voor Edge, gaat u naar

- Start
- Instellingen
- Updates en beveiliging
- Windows Update
- Controleren op updates

13—HP Sure Click is beschikbaar op de meeste HP pc's en ondersteunt Microsoft® Internet Explorer en Chromium™. Ondersteunde bijlagen zijn Microsoft Office (Word, Excel, PowerPoint) en pdf-bestanden in alleen-lezen-modus, als Microsoft Office of Adobe Acrobat geïnstalleerd zijn.

Neem waarschuwingen in acht.

De meeste standaard en moderne browsers hebben een basisfunctionaliteit voor het detecteren van kwaadaardige websites en zullen een waarschuwing tonen als er een dreiging wordt vermoed. Sommige browsers bieden ook automatische correctie voor websiteadressen om te voorkomen dat u navigeert naar een vaak verkeerd gespelde domeinnaam (waar schadelijke software en websites vaak op worden geplaatst).

Ga in Edge naar Geavanceerde instellingen> Privacy, en schakel de instelling 'Gebruik een webservice om te helpen bij navigatiefouten' in

Beperk content en plug-ins.

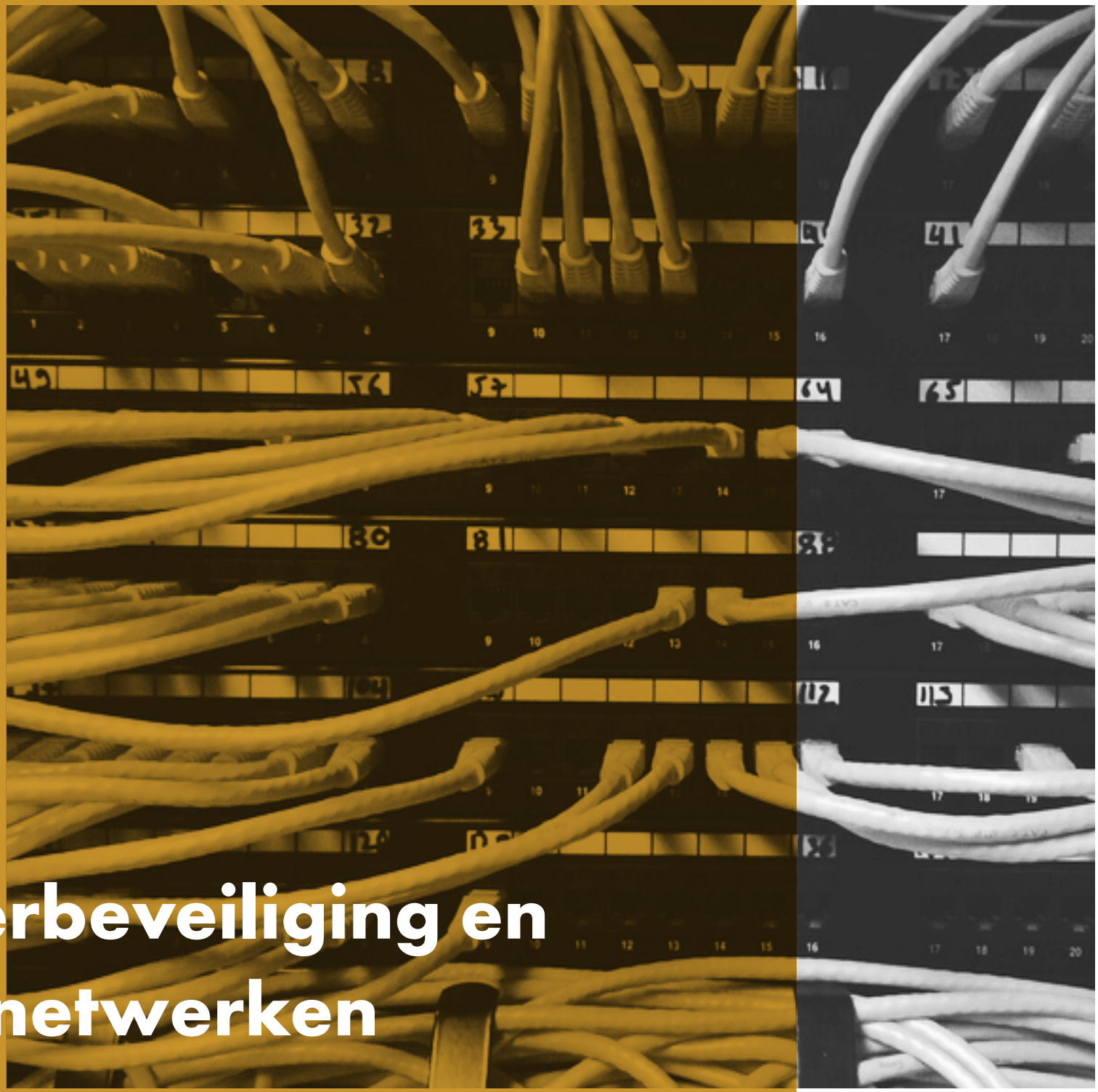
Veel van deze browseruitbreidingen (zoals Flash of JavaScript) zijn nodig voor uitgebreide websites en webtoepassingen, maar de uitgebreidere toegang tot uw systeem maakt ze ook kwetsbaarder.

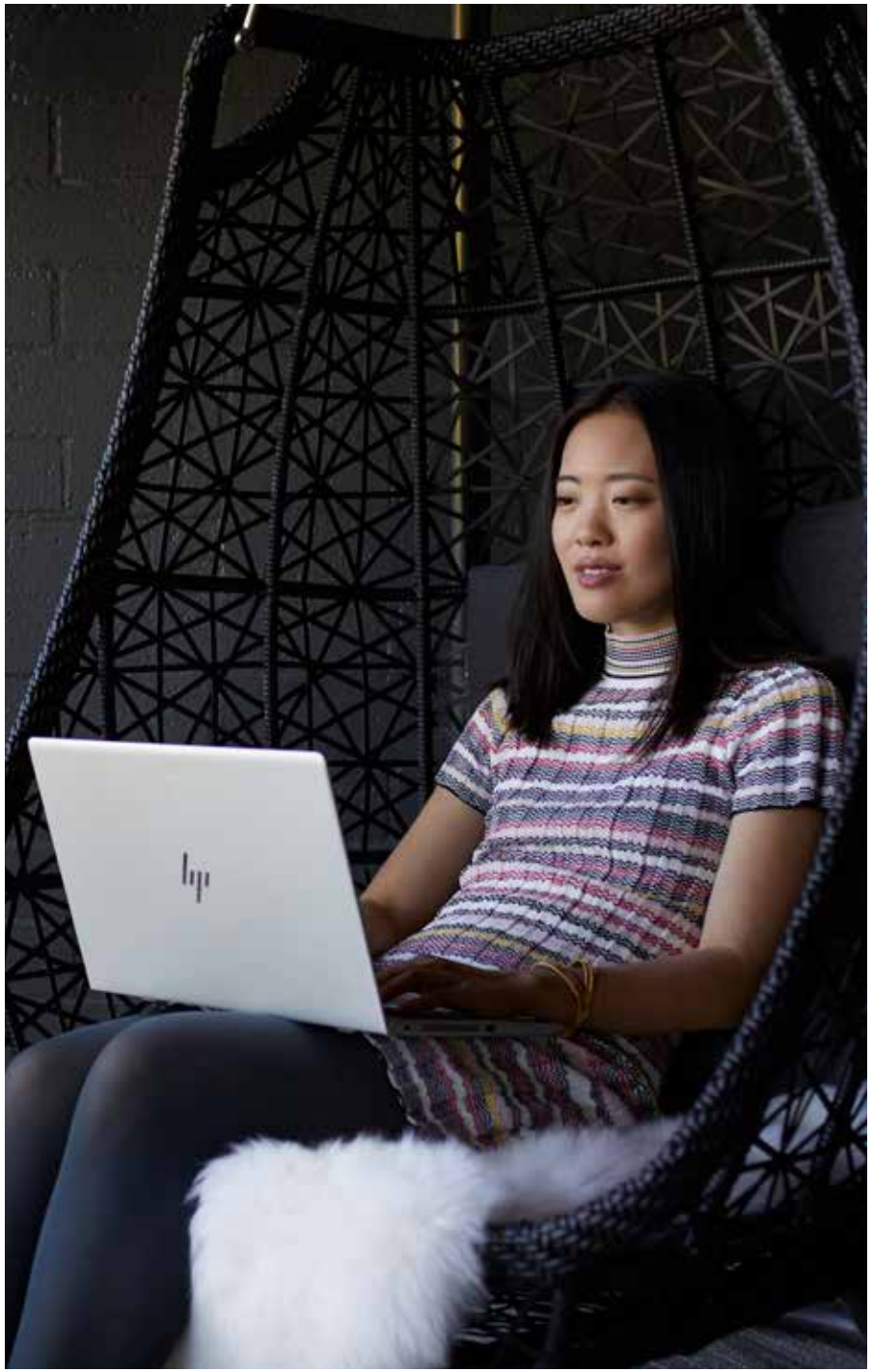
Schakel ze standaard uit, waardoor een website moet vragen om toestemming voor het gebruik ervan. Zo kunnen alleen websites die u vertrouwt deze functies gebruiken.

Ga in IE naar Extra (tandwielpictogram) -> Internetopties -> Beveiliging -> Internet -> Aangepast niveau... -> Scripting. U kunt JavaScript uitschakelen door gewoon te klikken op 'Uitschakelen', of instellen dat IE vraagt om het te gebruiken door te kiezen voor 'Vragen'.

Sectie 6:

Routerbeveiliging en privénetwerken





De router is de eerste beveiliging tegen indringers op een netwerk. Iedereen die verbinding maakt met internet doet dat via een router. Dit apparaat, bekabeld of draadloos (Wi-Fi®), zorgt ervoor dat de communicatie tussen uw lokale netwerk (dus uw pc of andere verbonden apparaten) en het internet mogelijk wordt. Het hoogste niveau van beveiliging op de router is de beste manier om uw pc's, printers en gegevens te beschermen tegen kwaadaardige aanvallen.

> Routers werden genoemd als de meest aangevallen apparaten bij IoT-aanvallen.[14]

Omdat routers ALLE gegevens doorsturen die van en naar uw bedrijf of huis gaan, waaronder e-mail en creditcardgegevens, waren routers lang een favoriet doelwit van hackers. In Symantec's 2018 Rapportage over internetbeveiligingsdreiging werden routers genoemd als het meest aangevallen apparaat bij IoT-aanvallen. Hackers kunnen gebruikmaken van malware of ontwerpfouten om hun identiteit te verbergen, bandbreedte te stelen of uw apparaten in te zetten als botnet-zombies... of erger. Ze kunnen ook profiteren van onbeveiligde apparaten.

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

Beveilig uw netwerk.

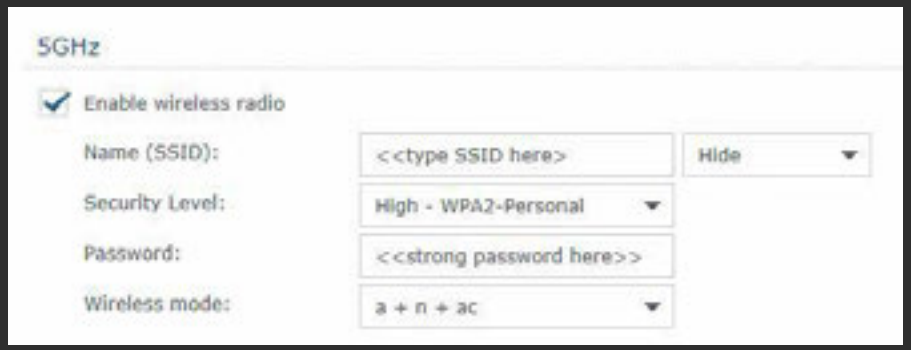
Helaas blijven veel leveranciers zowel beveiligde als niet beveiligde routerconfiguraties aanbieden. Als een router niet beveiligd is (dus verbindingen toestaat zonder een beheerwachtwoord) kan iedereen verbinding maken met de router en zo uw lokale netwerk bereiken. Een hacker zou uw wachtwoorden kunnen wijzigen, u kunnen bespioneren of zelfs de bestanden op uw aan het netwerk gekoppelde harde schijf kunnen openen.

Beveilig uw routers altijd met niet standaard beheerwachtwoorden op basis van de tips in Sectie 2: Versterk uw wachtwoorden. Hieronder staat een schermafbeelding van hoe de meeste routers u een wachtwoord laten instellen voor beveiliging op het netwerk.

Configureer encryptie.

Voor een draadloze router is een goed wachtwoord maar de helft van het verhaal - het kiezen van het juiste encryptieniveau is net zo belangrijk. De meeste draadloze routers beschikken over vier draadloze encryptiestandaarden: WEP (zwakste), WPA (sterk), WPA2 (sterker) en WPA3 (sterkste). Gebruik de sterkste encryptiestandaard die door uw router wordt ondersteund.

Hieronder ziet u een schermafbeelding van hoe u het juiste encryptieniveau op uw router instelt. Daarvoor moet u zich aanmelden als routerbeheerder en navigeren naar de encryptie-instellingen (verschilt per routerfabrikant).



Houd de firmware up-to-date.

Veel routerfabrikanten bieden regelmatig software-updates aan om beveiligingsproblemen op te lossen. Net als bij computersoftware is een router met de meest actuele updates het minst vatbaar voor besmetting met malware. De meeste routerfabrikanten passen firmware-updates automatisch toe zonder dat de gebruiker hier iets voor hoeft te doen. Nieuwere modellen hebben wellicht ook een mobiele app, waarmee u vanaf uw telefoon net als in elke andere app kunt controleren op updates. Als automatische firmware-updates echter niet worden aangeboden door uw routerfabrikant, dient u naar de website van de routerfabrikant te gaan en via Support of Ondersteuning te zoeken naar de juiste update op basis van het model en serienummer (doorgaans te vinden op de router zelf).

Gebruik Virtual Private Netwerken (VPN's).

Als u meer wilt dan alleen de beveiliging binnen uw bedrijf, dan kunt u een Virtual Private Network (VPN) gebruiken waarmee u op een veilige manier kunt verbinden van buiten het netwerk. VPN's kunnen uw identiteit en informatie beschermen en beveiligen. Het doel van VPN is om een eenvoudige manier te bieden om privé te internetten (maar niet altijd anoniem). Al het verkeer dat via de VPN-verbinding gebeurt is veilig en kan in theorie niet worden onderschept door derden; een geweldige oplossing dus voor zowel lokale als openbare netwerken. Meer over VPN en de voordelen ervan in Sectie 7.

Sectie 7:

Bescherm uzelf op openbare Wi-Fi®-netwerken

Tegenwoordig is openbare Wi-Fi® bijna overal. Luchthavens, lokale restaurants, winkelcentra en zelfs openbare parken bieden gratis internet aan via hotspots. Ze zijn ontzettend handig... en gevaarlijk.

Gebruikers die verbinding hebben met deze hotspots delen hetzelfde netwerk, dus is er een reële kans dat iemand profiteert van het onbeveiligde verkeer. Een hacker kan zelfs een hotspot opzetten en mensen naar dat (gelijknamige) nepnetwerk lokken. Zo kunnen ze niet-versleutelde gegevens zien of een gebruikersgerichte aanval plegen om encryptie te omzeilen.

Het is belangrijk om altijd aan te nemen dat uw communicatie onbeveiligd en openbaar is als u gebruikmaakt van een open netwerk. Als er echter geen andere mogelijkheid is, dan zijn er manieren om uw risico te verminderen.

Beperk uw activiteit.

Verzend geen zeer gevoelig materiaal zoals bedrijfsmaterialen, e-mails of wachtwoorden en maak geen gebruik van bank-/betaaltoepassingen of -portalen.

Bedenk een plan B.

Gebruik indien mogelijk semi-open netwerken die minimaal zijn beveiligd met een wachtwoord. Dit zijn meestal beheerde netwerken waar de leverancier een belang bij heeft om het veilig te houden (zoals in lounges op luchthavens)

Bezoek alleen websites met encryptie.

Zorg ervoor dat u verbonden bent met een webserver die versleuteld verkeer ondersteunt via het HTTPS-protocol (https://), in tegenstelling tot het niet beveiligde, plain text HTTP-protocol. Kijk in de bovenste balk waar het webadres staat; een moderne browser heeft doorgaans een pictogram in de adresbalk als er HTTPS beschikbaar is en het certificaat geldig is (vaak een slotje of groene kleur). Als u daarop klikt, verschijnt er een scherm met meer informatie over de mate van encryptie.

Verstuur alles via VPN.

Zoals in de vorige sectie vermeld, kan een VPN helpen uw gegevens te beschermen als u uw netwerkverbinding niet kunt vertrouwen; en een openbaar Wi-Fi®-netwerk is daar een perfect voorbeeld van. Een VPN-tunnel versleutelt uw gegevens van begin tot eind, om ervoor te zorgen dat iemand die ze onderschept ze niet kan lezen. Niet alle VPN's zijn gelijk, dus u dient de juiste te kiezen die bij uw budget en apparaatsoort past. Gratis VPN's hebben vaak beperkt beschikbare bandbreedte en eenvoudige encryptieprotocollen, zodat u langzamere snelheden ervaart bij het browsen en nog steeds kwetsbaar kunt zijn. Maar een betrouwbare gratis VPN-dienst is waarschijnlijk beter dan helemaal geen VPN.

Sectie 8:

Stop visuele hackers

Visueel hacken gebeurt als gevoelige informatie op het scherm wordt getoond in openbare plekken, waardoor concurrenten, identiteitsdieven of kwaadwillende personen dit kunnen zien, opslaan en misbruiken. Zelfs de nieuwsgierige toevallige meekijker is een mogelijke dreiging. Alles, van wachtwoorden en rekeningnummers tot financiële gegevens en bedrijfsinformatie, wordt bedreigd, en geen enkele beveiligingssoftware kan deze meekijkers ervan weerhouden dat te doen.

Nu er steeds vaker buiten traditionele kantoren op afstand en op openbare plekken gewerkt wordt, is de kans om 'visueel gehackt' te worden groter dan ooit. Misschien is visueel hacken wel de meest onderbelichte en eenvoudigste dreiging waarmee bedrijven nu te maken hebben. Het is eenvoudig, effectief en wordt vaak niet opgemerkt tot het te laat is.

Volgens onderzoek gepubliceerd door het Ponemon Institute[1]:

- 91% van de pogingen tot visueel hacken waren succesvol
- 68% van de pogingen tot visueel hacken werden door het slachtoffer niet opgemerkt
- 52% van de gevoelige informatie werd direct van apparaatschermen gehaald

Let op uw omgeving.

Als u werkt op openbare plekken, ga er dan altijd vanuit dat er iemand over uw schouder meekijkt en handel daarnaar.

Beperkt uw blootstelling.

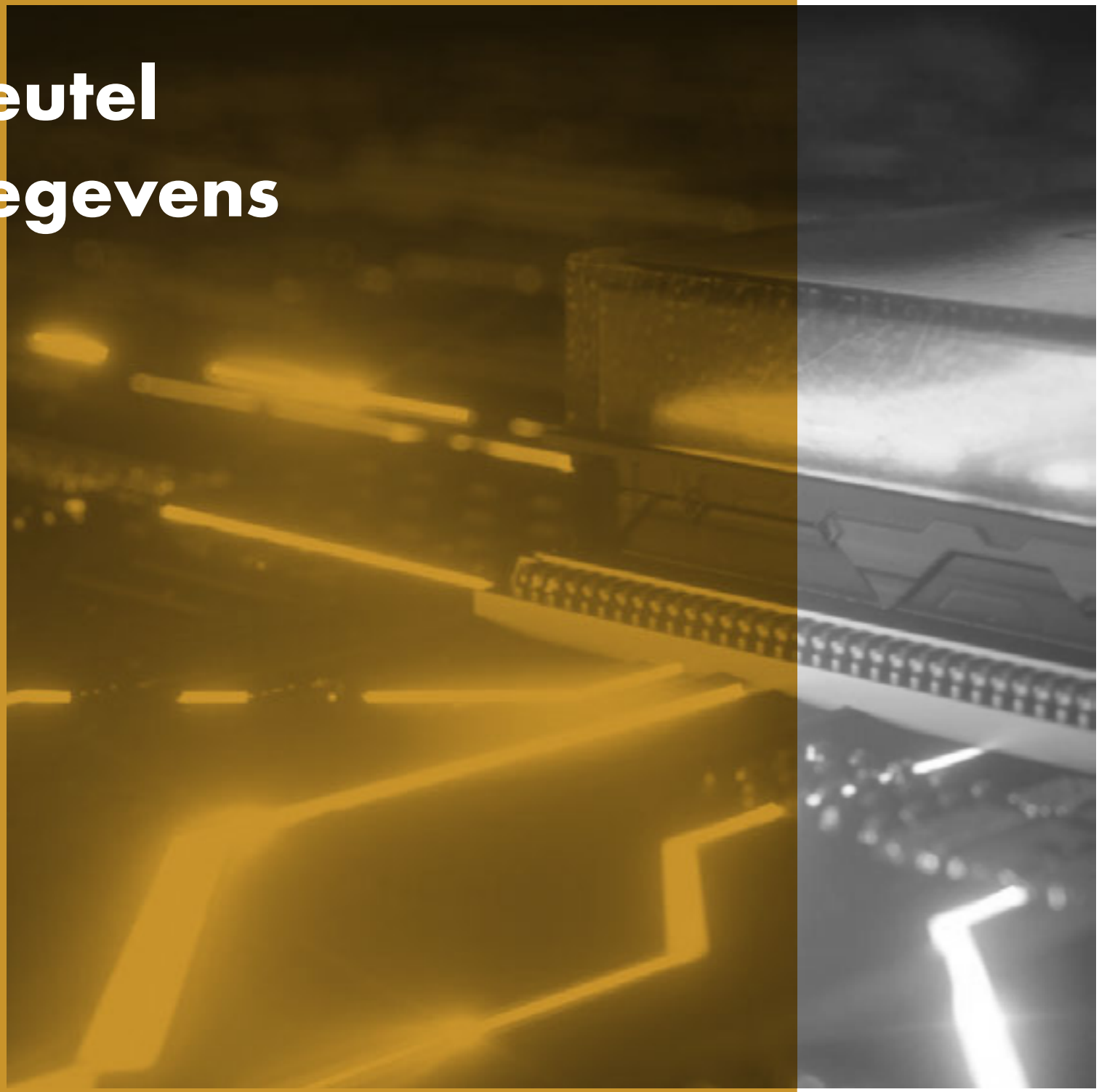
Privacyschermen zijn ontworpen om de inkijkhoek van het scherm te verkleinen, zodat een mogelijke visuele hacker niet kan zien wat erop staat als hij of zij er niet midden voor zit. Een extern filter is een eenvoudige manier om deze beveiliging toe te voegen. Het wordt aangebracht over uw scherm en kan worden verwijderd als u het scherm moet delen met een groter publiek.

Een geïntegreerd privacyscherm vergemakkelijkt dit proces, omdat u geen externe beschermer hoeft toe te passen, mee te nemen of te vervangen. Veel HP pc's bieden HP Sure View Gen2[15], een geïntegreerd privacyscherm dat ontworpen is om visueel hacken minder makkelijk te maken, als optie aan. Het werkt door dynamisch de structuur van de lcd-pixels op moleculair niveau aan te passen, waardoor het met een druk op de knop wordt ingeschakeld of uitgeschakeld, en waarmee de prestatie in zowel lichte als donkere omgevingen wordt verbeterd.

15—HP Sure View geïntegreerd privacyscherm is een optionele functie die bij aankoop moet worden geconfigureerd en is bedoeld om in horizontale schermstand te werken.

Sectie 9:

Versleutel uw gegevens



Als een pc zoekraakt of gestolen wordt, is de harde schijf het eerste doelwit. Deze wordt met slechts enkele schroeven op zijn plaats gehouden en kan op een andere pc worden aangesloten. Als u uw gegevens niet voldoende hebt beveiligd, is het lezen van een schijf als het openslaan van een boek.

Encryptie zorgt ervoor dat alles wat is opgeslagen volkomen onbegrijpelijk is voor buitenstaanders. Encryptie is het proces van versleutelen van gegevens om deze onleesbaar te maken voor iedereen die niet de encryptiesleutel heeft. Dus een computer met een versleutelde harde schijf kan worden gestolen, maar niet worden misbruikt. Dat is verreweg beter dan dat uw zakelijke en persoonlijke informatie voor eeuwig in verkeerde handen valt.

Schakel software-encryptie in.

Windows 10 Pro ondersteunt wachtwoord-encryptie van uw harde schijf met uw aanmeldgegevens als sleutel. Zodoende heeft een hacker uw gebruikersnaam en wachtwoord nodig om uw gegevens te kunnen lezen.

Zorg dat u een sterk wachtwoord voor uw gebruikersaccount gebruikt:

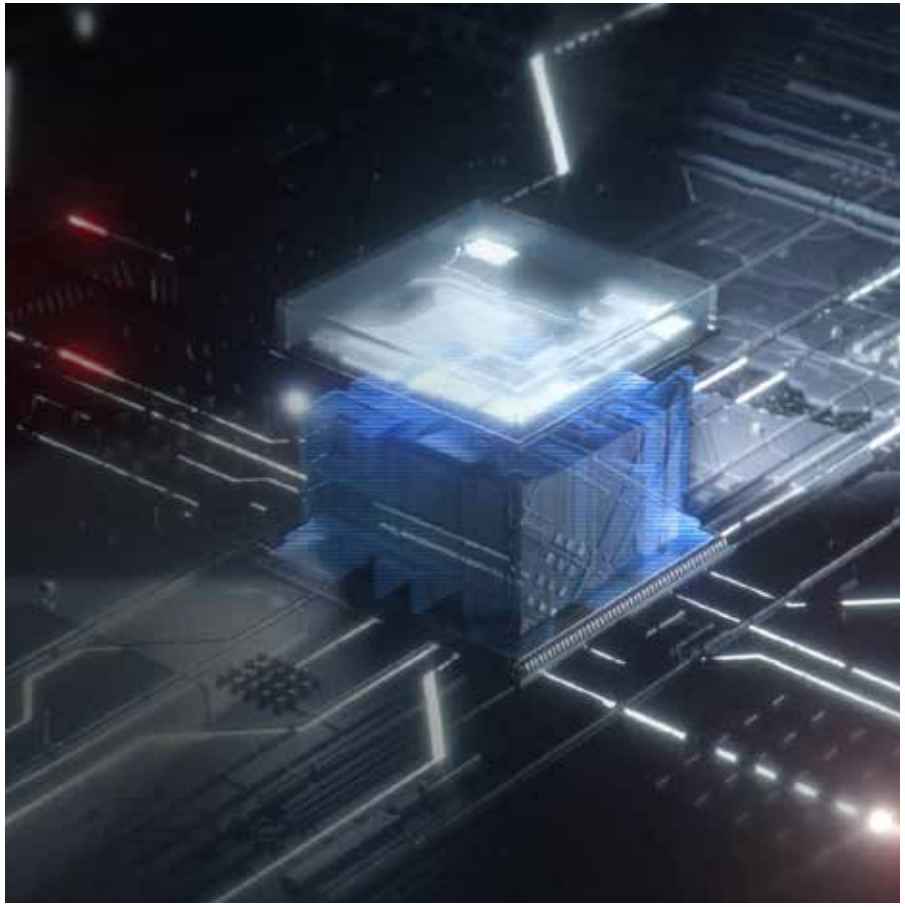
1. • Instellingen> Accounts> Aanmeldopties> Wachtwoord

2. Schakel, indien beschikbaar, Trusted Platform Manager (TPM) in, waarmee een beveiligingschip wordt geactiveerd binnen uw pc om uw nieuwe wachtwoorden en gegevens op de schijf te versleutelen:
   • Instellingen> Update en beveiliging> Windows Beveiliging> Apparaatbeveiliging> Processor

3. Schakel encryptie in om ervoor te zorgen dat uw gegevens niet kunnen worden bekeken of gekopieerd zonder uw aanmeldgegevens:
   • Instellingen> Update en beveiliging> Schijfencryptie

Profiteer van hardware-encryptie.

BitLocker is een functie van Windows 10 Pro die software-encryptie biedt die wordt ontsloten met een hardwaresleutel. Apparaten met een TPM-chip, zoals HP-notebooks, kunnen encryptie toepassen zonder extra hardware. De TPM voorkomt toegang tot versleutelde gegevens als hij merkt dat er met het systeem is geknoeid toen het was uitgeschakeld. Apparaten zonder TPM kunnen ook gebruikmaken van BitLocker, maar die vereisen een verwijderbaar apparaat zoals een USB-schijf om als sleutel te dienen.



Sectie 10:

Beveilig uw pc onder het besturingssysteem

De BIOS (Basic Input Output Software) is software die de computer opstart en helpt bij het laden van het besturingssysteem. Door deze basissoftware te besmetten, kunnen spionnen malware aanbrengen die blijft bestaan en niet wordt gedetecteerd door antivirusprogramma's. Het blijft zelfs op de harde schijf staan als de schijf gewist wordt of het besturingssysteem opnieuw wordt geïnstalleerd.

Als een hacker toegang krijgt tot uw BIOS, krijgt hij toegang tot elk onderdeel van uw pc.

Hierdoor krijgt de hacker een manier om gegevens te laden of het systeem vast te laten lopen door de firmware te wijzigen, waardoor het gehele moederbord moet worden vervangen.
Voor HP Elite en Pro pc's kan HP Sure Start automatisch de BIOS zelf herstellen van malware, rootkits of beschadiging, door een extra laag van bescherming toe te voegen en een vertrouwde basis te leggen voor de beveiliging van uw pc[16].

Laat geen update achterwege.

Zoals eerder genoemd in sectie 4 zorgen software-updates ervoor dat nieuw gevonden kwetsbaarheden worden opgelost; en de BIOS is geen uitzondering. Omdat de meeste BIOS-implementaties dezelfde broncode delen binnen een personeelsbestand of aantal gebruikers, is een ontdekt lek waarschijnlijk aanwezig op veel meer pc's van de leverancier. OEM-tools zoals HP Support Assistant controleren automatisch op updates, of u kunt de website van de fabrikant bezoeken voor BIOS-updates.

Verken de BIOS.

De BIOS-fabrieksinstellingen gelden als balans tussen beveiliging en gebruiksvriendelijkheid. Maar om het systeem te beschermen tegen de vele mogelijkheden van bedreiging, wilt u misschien wat van die functies verwijderen.

Hoe u de BIOS-instellingen aanpast kan van fabrikant tot fabrikant verschillen, maar u komt er meestal in door tijdens het opstarten op een toetscombinatie te drukken (zoals F10 of FN-10 op HP-notebooks).

16—HP Sure Start Gen4 is beschikbaar op HP Elite- en HP Pro 600-producten die zijn uitgerust met 8ste generatie Intel®- of AMD-processoren.

Stel een BIOS-wachtwoord in.

Om te voorkomen dat een BIOS-instelling wordt gewijzigd door ongeautoriseerde gebruikers, raden wij aan een BIOS-wachtwoord te gebruiken:

- Bijvoorbeeld: Beveiliging> Beheergereedschappen> Maak BIOS-beheerwachtwoord

Het is belangrijk het beheerwachtwoord te onthouden, omdat het is gemaakt om niet hersteld te kunnen worden.

Stel een opstartwachtwoord in.

Voor nog meer beveiliging kan een opstartwachtwoord worden aangemaakt.
Als de pc wordt ingeschakeld en voordat het systeem iets uitvoert, wordt eerst het opstartwachtwoord gevraagd. Net als het BIOS-wachtwoord is dit niet eenvoudig te herstellen of te resetten, en als u het vergeet is uw machine dus onbruikbaar.

Beperk ongebruikte functies.

In de BIOS zijn er enkele instellingen die u moet overwegen voor maximale beveiliging. Hoewel ze bepaalde functionaliteit verwijderen of de toegankelijkheid verminderen, is de onderstaande OS-beveiliging niet makkelijk met software na te bootsen:

1. Verwijder externe en optische schijven uit de opstartvolgorde (via: Geavanceerd> Opstartopties). In het bijzonder starten vanaf USB-opslag, Network (PXE)-opstarten en opstarten van een optische schijf, omdat daarmee malware kan worden geladen van externe bronnen. Als opstarten van deze apparaten nodig is, kan de functie per geval worden ingeschakeld.
2. Schakel Legacy Support uit (via Geavanceerd> Secure Boot configuratie) en schakel Secure Boot in.
3. Activeer de functie 'Opslaan/herstellen GPT van systeemhardeschijf' (via: Beveiliging> Hardeschijfgereedschappen).
4. Activeer DriveLock en stel een wachtwoord in.

Conclusie

Tegenwoordig zijn digitale dreigingen meer dan ooit gericht op kleine en middelgrote bedrijven. Het goede nieuws is dat veel van de hardware en software die u bezit onderbelichte beveiligingsfuncties bevat waarmee u die kunt bestrijden. Er is ook een ontelbaar aantal producten en diensten beschikbaar met hoogwaardige beveiligingsinnovaties om te beschermen tegen het onbekende van morgen. Van op hardware gebaseerde beveiliging op moderne apparaten tot zelf-updatende software, een slimme investering voor verbonden, beveiligde apparaten betaalt zich tot ver in de toekomst zeker uit. HP ontwerpt beveiligingsoplossingen die profiteren van de sterke kanten van Windows 10 Pro, met ondersteuning van de ingebouwde beveiligingsfuncties met discrete hardware-uitbreidingen en softwareondersteuning die altijd up-to-date is. De dreigingen die u ervaart veranderen elke dag, en de juiste beveiligingsstrategie verhoogt uw weerstand ertegen.

BEDANKT.

Ga voor meer informatie naar:
www.hp.com/go/windows10now

Zorg dat u continu beveiligd bent.