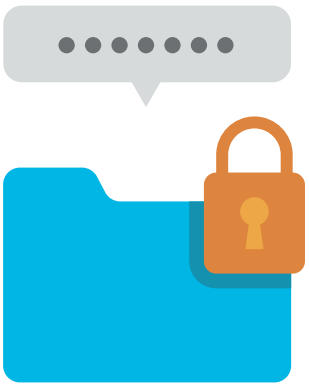
Business white paper

Beveiliging begint bij het eindpunt

De case voor het prioriteren van eindpuntbeveiliging

U gebracht door

Managementsamenvatting



82% van de organisaties heeft in de afgelopen 12 maanden een cyberbeveiligingsdreiging/-inbreuk ervaren.[1] Cybercriminaliteit neemt toe in aanvalfrequentie, ernst en kosten.

Het paradigma van voorkomings- en beschermingsbeveiliging, het verdedigen van een netwerkperimeter met een firewall, is verleden tijd. Opsporen en reageren is veel effectiever.

Maar IT-budgetten slagen er niet in het nieuwe gezicht van cyberbeveiliging bij te houden. 77% van de uitgaven is nog steeds voor voorkomen en beschermen.[2] Slechts 36% van IT-beveiligingsmanagers heeft het gevoel voldoende budget te hebben voor effectieve eindpuntbeveiliging.[3]

Solide gegevensbescherming is mogelijk. Met de juiste technologie, van beveiligingsoplossingen voor het opsporen en reageren tot en met individuele apparaten, en de juiste strategie en voldoende hulpmiddelen kunnen organisaties zich beschermen tegen cybercriminaliteit.

Verzuimen om meer te investeren in cyberbeveiliging en investeringen voor werkelijk doelgerichte verdediging opnieuw af te stemmen, zal een hogere frequentie van beveiligingsinbreuken en hogere kosten voor de organisatie tot gevolg hebben.

Inleiding

Cyberbeveiliging in het tijdperk van vormloze netwerken
60% van IT-leiders heeft het gevoel dat de toenemende omvang en verfijning van cybercriminaliteit het wint van hun verdediging. 80% van beveiligingsleiders neemt de dreiging van Advanced Persistent Threats (APT's), criminele ondernemingen, door de staat gesponsorde hackers en hacktivisten waar als groeiende en als de topuitdaging voor IT-beveiliging.[4]

Ze hebben niet ongelijk. In het Verenigd Koninkrijk schat de regering de economische kosten van cybercriminaliteit op £ 27 miljard, een cijfer dat 'aanzienlijk en waarschijnlijk groeiende is', met een verlies voor bedrijven van rond de £ 21 miljard.[5] In Ponemon's 2016 State of the Endpoint Report meldde 78% van bedrijven een toename in de ernst van malware-aanvallen. In 2011 was dat 47%.

Maar de focus op externe bedreigingen is enigszins misleidend en kan leiden tot een impulsieve concentratie van hulpmiddelen in voorkomings- en beschermingsverdediging van de perimeter.

Hoewel externe aanvallen - virussen, malware, phishing - meer voorkomen, zorgen interne aanvallen voor meer kosten.[6] En veel van die externe aanvallen worden veroorzaakt door interne zwakke punten; slordige medewerkers die beveiligingsprotocollen negeren, met het netwerk verbonden onbeveiligde apparaten. 81% van de respondenten van de Ponemon-enquête identificeerde dat als de grootste bedreiging voor IT-beveiliging.

Dit wordt met de tijd alleen maar erger. Het eindpunt is het zwakste knooppunt in ieder netwerk, en met de stijging in BYOD, werken op afstand en internet der dingen, vermenigvuldigen de eindpunten zich. Dat betekent dat het aantal ingangen voor hackers zich ook vermenigvuldigt.

Ver van het voormalige gecontroleerde netwerk van bureaucomputers die een snoerverbinding hadden met Ethernet, zijn bedrijfsnetwerken vormloos geworden, een wirwar van apparaten, zowel zakelijk als privé, die toegang hebben tot gegevens via meervoudige interne en externe wifi-knooppunten.

Het gaat niet om een verloren zaak. Het houdt alleen in dat een vernieuwde aanpak van cyberbeveiliging moet worden aangenomen. Nieuwe strategieën die reageren op het veranderende gezicht van cybercriminaliteit. Nieuwe technologie die in staat is om steeds grotere verfijning af te buigen van een groeiende dreiging.

In deze white paper onderzoeken we de aard en schaal van de dreiging, zodat we onze vijand beter leren kennen voordat we ons bezig houden met de vraag hoe we cyberbeveiliging aanpakken in het tijdperk van meervoudige apparaten, onbeveiligde netwerken en de cloud.

[1] HPI Printer Security Research 2016 (Spiceworks)
[2] PAC Incident Response Management 2015: https://www.pac-online.com/download/19443/155514
[3] Ponemon 2016 State of the Endpoint Report
[4] IBM CISO Assessment 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

De schaal van de dreiging

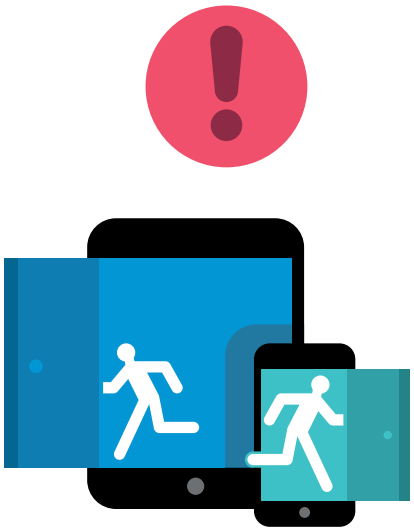
Herstel van een informatie-inbreuk kost bedrijven gemiddeld $ 907.053, naast 13% verlies aan inkomsten. Gemiddeld heeft een organisatie negen weken nodig om te herstellen.[7]

Ongeveer 85% van de geënquêteerde bedrijven in de HP Printer Security Report 2015 zei een beveiligingsdreiging/-inbreuk te hebben ervaren in de voorgaande 12 maanden. 80% van de geënquêteerde IT-professionals verwachtte toename van de dreiging in de komende drie jaren.[8]

Cybercriminaliteit kost echt geld. Verloren waarde vanwege hetgeen gestolen of beschadigd is. Verloren inkomsten vanwege reputatieschade en verloren productiviteit. Verloren hulpmiddelen die worden besteed aan herstel: tijd van support-desk, implementatie van nieuw beveiligingsbeleid, verlies van personeel en andere interne reacties. Boetes van regelgevingsinstanties. Daling in aandelenwaarde.

De dreiging zal alleen maar groeien met het aantal apparaten dat met het netwerk verbonden is. Gartner voorspelt dat dankzij het internet der dingen er tegen 2018 11,4 miljard verbonden apparaten zijn. In 2016 waren dat er 6,4 miljard. Tegen 2020 is 25% van geïdentificeerde aanvallen in ondernemingen IoT-gerelateerd, maar het internet der dingen omvat minder dan 10% van beveiligingsbudgetten.[9]

De dreiging van cybercriminaliteit is groot, en wordt groter.



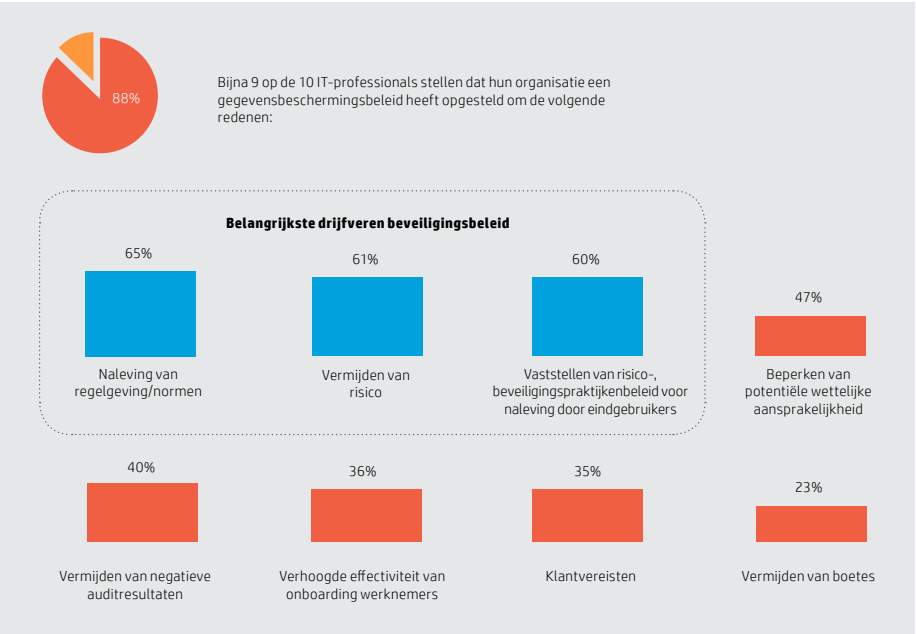
De vorm van de dreiging

Bedrijven hebben dagelijks last van talloze cyberaanvallen. De meeste betreffen laagniveauvirus- en malware-aanvallen. 99% van door Ponemon in 2016 geënquêteerde organisaties ervoer malware in de 12 voorgaande maanden. Dergelijke externe webgebaseerde aanvallen zijn relatief goedaardig en kosten organisaties gemiddeld $ 4.639.[10]

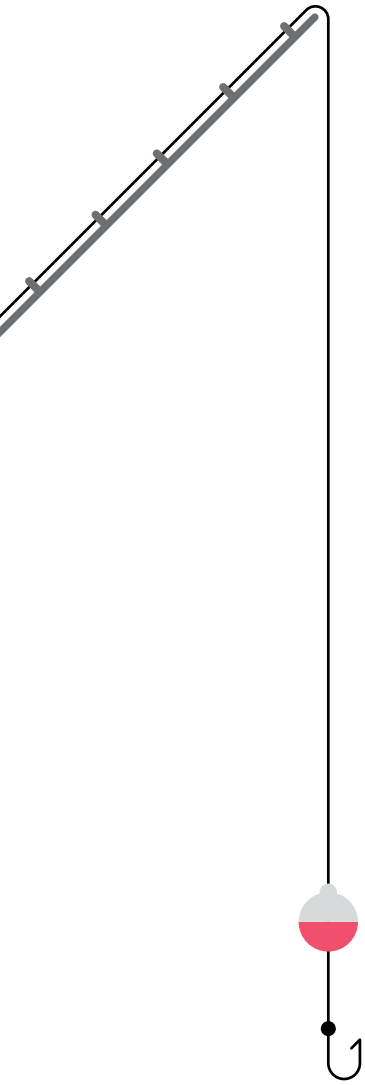
Maar ernstigere aanvallen komen steeds meer voor. 51% van in 2015 geënquêteerde organisaties had Direct Denial of Service-aanvallen (DDoS-aanvallen) ervaren, die verwoestend kunnen zijn en gemiddeld $ 127.000 kosten. Nog alarmerender is dat 35% een kwaadaardige insideraanval van gemiddeld $ 145.000 had ervaren.[9]

Het plaatje dat naar voren komt toont meedogenloze kleinere aanvallen van buitenaf, met niet-frequente maar schrikwekkend waarschijnlijke grote aanvallen, die waarschijnlijk het gevolg zijn van achteloosheid of kwaadwilligheid van insiders. 62% van organisaties had phishing-/social engineering-aanvallen ervaren, waarbij zwaktes van werknemers worden uitgebuit, met gemiddelde kosten van $ 86.000.[11]

Een aparte enquête door Spiceworks, namens HP, ontleedde in 2014-2015 90 door organisaties in het VK ervaren aanvallen.[12]



[7] NTT Security Risk:Value Report 2016
[8] HP 2Printer Security Report 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] HPI Printer Security Research, Spiceworks 2016



Hoe inbreuken plaatsvinden

De krantenkoppen geven het beeld van ondernemende hackers die verfijnde beveiligde netwerken van overheden en ondernemingen hacken, maar de werkelijkheid is meestal nuchterder.

Virussen kunnen profiteren van gecompromitteerde netwerken, maar malware heeft meestal een soort gebruikersfout nodig. Phishing-/social engineering-aanvallen zijn daarvan afhankelijk. Grote DDoS- en informatiediefstalaanvallen zijn ook meestal het gevolg van gebruikersslordigheid.

De inmiddels beruchte Dropbox-hack was het vermoedelijke resultaat van een slordige Dropbox-medewerker die hetzelfde wachtwoord voor interne systemen gebruikte als voor zijn LinkedIn-account.[13] De vermeende Russische hacking van de DNC was kennelijk te danken aan John Podesta, voormalig adviseur van mevr. Clinton, die klikte op een link in een phishing-e-mail die per abuis als 'legitiem' werd benoemd door een naaste medewerker[14]

Hackers hebben geen actieve assistentie nodig om te slagen. Net zo gevaarlijk is het niet op de hoogte zijn van, of het negeren van, beveiligingsprotocollen. Een toenemende dreiging is dat werknemers hun eigen apparaten meenemen naar het werk en commerciële cloudsoftware gebruiken. Beide introduceren onbeveiligde elementen in een verder beveiligd netwerk; ze liggen buiten het controlegebied van bedrijfs-IT en creëren een ongekende kwetsbaarheid.

Meestal hoeven hackers geen verfijnde algoritmes of geavanceerde technologie toe te passen, ze hebben alleen maar iemand nodig die een beetje slordig is.

De firewall is doorbroken

Tot voor kort was antivirus- en firewallsoftware de hoeksteen van cyberbeveiliging. Voorkomen en beschermen. Creëren van een beveiligde perimeter. In de huidige werkomgeving is dat gewoon geen geloofwaardige strategie.

81% van Ponemon-respondenten zegt dat mobiele apparaten op hun netwerk het doelwit zijn geweest van malware. Andere verhoogde beveiligingsrisico's omvatten werknemersgebruik van commerciële cloudapplicaties (genoemd door 72% van de respondenten) BYOD (69%) en werknemers die vanaf thuis en externe locaties werken (62%).[15]

Simpel gezegd: een firewall had zin toen je als netwerkbeheerder controle had over de verbonden apparaten. Maar in een tijdperk waarin werknemers hun eigen apparaten meenemen naar het werk - vaak meerdere, vaak zonder dat IT op de hoogte is - en steeds meer werkers op afstand verbinding maken, kunt u eenvoudigweg de perimeter niet beschermen. Ieder niet gescreend apparaat is een kwetsbaar eindpunt dat hackers kunnen uitbuiten.

[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach
[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0
[15] Ponemon 2016 State of the Endpoint Report

Het HP perspectief: verder gaan dan netwerkbeveiliging

Michael Howard, HP's wereldwijde beveiligingspraktijkenmanager over het zorgen voor eindpuntbeveiliging

Een belangrijke en actuele zorg is dat bedrijven worstelen om elk eindpunt te beveiligen vanwege gebrek aan bewustzijn en kennis van bepaalde apparaten en het risico dat die apparaten met zich meedragen. Ze voelen zich veilig achter een firewall, hoewel dit niet langer genoeg is om te beschermen tegen een aanval. Beveiligingsteams moeten elk eindpunt binnen hun infrastructuur kennen en ervoor zorgen dat elk eindpunt meerdere beveiligingslagen heeft ter bescherming tegen steeds subtielere aanvallen.

Het is van wezenlijk belang voor beveiligingsteams om iedere hoek van hun IT-bedrijfsinfrastructuur te onderzoeken en een extra beschermingslaag aan standaard netwerkperimeters toe te voegen. Alleen firewalls zijn niet bestand tegen subtiele aanvallen en een verdedigingsbeleid met meervoudige beschermingslagen op ieder eindpunt is een must-have om ervoor te zorgen dat uw bedrijf kan voldoen aan regelgevingseisen en zware boetes kan vermijden.

Het beleid van HP is erop gericht dat met de ontwikkeling van elke nieuwe oplossing, dienst of product, het eerst gekeken wordt naar beveiliging. De ontwikkelingsteams weten dat ze de beveiligingsvragen moeten beantwoorden en ze moeten weten hoe ze die antwoorden op een beveiligde manier op het netwerk gaan zetten.

Meer dan ooit moet beveiliging een eerste prioriteit zijn in plaats van een optie. Dat is al jaren HP's beleid.

Gelaagde beveiliging

Een nieuwe aanpak voor cyberbeveiliging moet meerdere lagen hebben.
Netwerkbeveiliging is nog steeds belangrijk, maar die moet zelf zijn gevormd door discrete netwerken. Veel inbreuken zijn het gevolg van allereerst de ingang die toegang verschaft tot alles in het systeem. Denk aan de phishingfout die John Podesta maakte. Het is van wezenlijk belang om gevoelige informatie te omheinen met meervoudige toegangslagen, zodat het stelen van één sleutel niet de verovering van het kasteel betekent.

Voor apparaten moet rekenschap worden gegeven. Een belangrijk element voor IT-managers is ervoor te zorgen dat ieder apparaat dat verbonden is met het netwerk wordt beschermd door regelmatig bijgewerkte beveiligingssoftware, tegen virussen, malware en spyware, en regelmatig wordt gescand op onregelmatigheden. Beter nog is de apparaten zelf als sensoren te gebruiken en real-time informatie te verzamelen om een alert af te geven voor inbreuken op de netwerkperimeter waar ze deel van uitmaken.

Er moet uitgebreid beveiligingsbeheer opgesteld zijn, waarbij iedere werknemer is getraind in cyberbeveiligingsprotocollen. Menselijke fouten, van het klikken op de verkeerde link tot het verbinden met een consumentenapparaat, vormen de nummer 1-dreiging voor het netwerk. Menselijke fouten kunnen worden teruggebracht door training.

Apparatuurbeveiliging

Misschien is controle over welke apparaten toegang hebben tot het netwerk wel het grootste probleem waarmee hedendaagse cyberbeveiliging te maken heeft.
De eerste, eenvoudige, veelgebruikte oplossing is gebruik te maken van separate wifi-netwerken voor gasten en werknemers, zodat niet-beveiligde externe apparaten geen toegang hebben tot het hoofdnetwerk. Dit gaat samen met het trainen van werknemers opdat ze dit netwerk gebruiken voor hun privé-apparaten.

De tweede oplossing is ervoor te zorgen dat u controle heeft over werknemersapparaten. Deze zorg moet opgenomen zijn in het bedrijfsbeleid over BYOD of CYOD, waarbij CYOD sterk de voorkeur heeft omdat die meer controle geeft over welke apparaten worden gebruikt, het mogelijk maakt die apparaten te kiezen die betere beveiligingskenmerken hebben, hoe ze zijn geconfigureerd en het beheer en de bewaking van die apparaten.

Het gebruik van bijvoorbeeld een van onze HP Elite pc's heeft de voorkeur boven een budget-laptop. Iedere HP Elite pc heeft HP SureStart-technologie die iedere 15 minuten de BIOS controleert en de machine in zijn originele staat reset om onregelmatigheden op te sporen en ongewenste indringers te blokkeren. Dankzij dit kenmerk - en vele andere- werden computers uit onze HP Elite 800 serie onlangs benoemd tot 'de best beveiligde pc's ter wereld'.[16] Maar het is onwaarschijnlijk dat werknemers zelf een HP Elite pc bezitten.

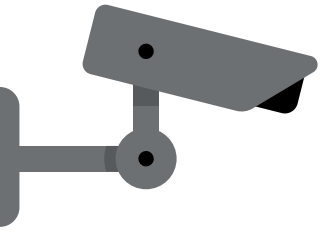
Werknemers geven om twee redenen vaak de voorkeur aan het gebruik van hun eigen apparaten:
1. Consumententechnologie is vaak beter dan die welke de werkgever verschaft
2. Werknemers gebruiken graag technologie waarmee ze vertrouwd zijn

Door een CYOD-beleid te bieden met goede hulpmiddelen en met de nieuwste apparaten die een regelmatige bijwerkingscyclus hebben, kunnen organisaties betere apparaten verstrekken dan die van de werknemers zelf en grotere controle uitoefenen op de beveiliging van die apparaten. Daarom verkopen we onze HP Device as a Service (DaaS).

Het is van wezenlijk belang alle apparaten op te nemen in de beveiligingsstrategie, zelf die apparaten die vaak worden vergeten. In een IDC-enquête zei 80% van de respondenten dat IT-beveiliging belangrijk is voor hun bedrijf, maar slechts 59% zag printbeveiliging als belangrijk, terwijl meer dan de helft in de 12 voorgaande maanden een beveiligingsinbreuk had ervaren betreffende printbeveiliging. Dit is een overduidelijke blinde vlek.

Het gemiddelde aantal beveiligingsinbreuken voorafgaand aan de implementatie van een printbeveiligingsbeleid was 9,9 per jaar met gemiddelde kosten van $ 521.400 (inclusief boetes). Na implementatie van printbeveiliging zakte het gemiddelde aantal inbreuken naar 1,5, met besparing van 200 werkuren per jaar en $ 250.000 aan gerelateerde kosten, waaronder audit en naleving.[17]

[16] http://www8.hp.com/us/en/campaign/computersecurity/
[17] IDC The Business Value of Printer Security 2015



Proactief opsporen en reageren

77% van IT-beveiligingsuitgaven gaat naar voorkomings- en beschermingstechnologie, zoals antivirussoftware en firewalls, volgens onderzoek door PAC. Maar deze aanpak is niet effectief. Het onderzoek liet ook zien dat 67% van de geënquêteerde firma's een cyberinbreuk in de voorgaande 12 maanden had gehad en 100% op een bepaald moment in het verleden.[18]

Met name antivirussoftware is schrikbarend ineffectief. Damballa voerde een proef uit waarbij opzettelijk een netwerk werd aangevallen om de antivirusrespons te meten. Het duurde meer dan zes maanden voordat 100% van kwaadaardige bestanden was geïdentificeerd.[19] Dit komt overeen met een andere PAC-constatering dat het tussen één en zes maanden duurde voor firma's om te herstellen van een aanval.

Preventie kan niet langer voldoen aan het beveiligd houden van eindpunten. Het groeiende aantal virus-/malware-incidenten, plus de inherente onzekerheid van de BYOD/mobiele manier van werken, betekent dat inbreuken onvermijdelijk zijn. Niemand suggereert dat preventie en bescherming helemaal moeten worden losgelaten, maar duidelijk is dat opsporen en reageren hoger op de agenda moeten komen te staan.

"Geen enkele technologie kan beveiliging leveren als mensen die ondermijnen."

– Joseph Steinberg [21]

Voortdurende real-time monitoring is noodzakelijk, liefst met gebruik van eindpunten zelf als sensoren, die de rest van het netwerk alarmeren als ze geschonden zijn. Hierdoor kan IT-beveiliging op afstand reageren met processen zoals:

- Op afstand een apparaat afsluiten
- Een geïnfecteerd proces of een proces dat malware verspreidt doden
- Een specifiek bestand of specifieke groep bestanden in quarantaine brengen
- Netwerkcommunicatie onderbreken om geïnfecteerde apparaten te isoleren[20]

Accepteren dat inbreuken zullen plaatsvinden en de juiste responsprotocollen vaststellen, naast implementatie van de noodzakelijke technologie voor de uitvoering ervan, is de enige manier om te zorgen voor cyberbeveiliging als niet langer vertrouwd kan worden op preventie.

Werknemersbeveiliging

Net zo belangrijk als beveiliging van het apparaat zelf, zo niet belangrijker, is de persoon te beveiligen die het gebruikt.
Iedere werknemer moet worden getraind in cyberbeveiliging. Ze moeten zich bewust zijn van de risico's van phishing. Van het surfen op verdachte websites. Van het downloaden van verdachte bijlagen. Ze moeten zich bewust zijn van het beleid betreffende beveiligde wachtwoorden, het gebruik van sterke, unieke wachtwoorden voor het inloggen in gevoelige gegevens en het gebruik van de juiste wachtwoordbeheerder voor de opslag.

Er moet hen bewustwording worden bijgebracht over het belang van regelmatige bijwerking van de beveiligingssoftware op hun apparaat, om de monitorende taak van IT te verlichten. Ze moeten waakzaam zijn alleen beveiligde apparatuur te gebruiken voor toegang tot de netwerken van de organisatie en het gebruik van privé-apparaten op externe, onveilige netwerken voor toegang tot gevoelige gegevens vermijden.

Vele topcyberbeveiligingsdeskundigen bevelen simulatie van phishing-aanvallen aan en zelfs het bouwen van nep-fishing-websites om iedere werknemer te drillen en zo cyberbeveiligingstraining te formaliseren. Want de meeste aanvallen zijn gebaseerd op het uitbuiten van menselijke zwakheden, of door slordigheid of door kwaadaardigheid.

Want mensen zijn de zwakste schakel in ieder netwerk.

[18] PAC Incident Response Management 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] The Essential Endpoint Detection Checklist – HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Conclusie

IT-beveiligingsuitgaven moeten verschuiven van preventie en bescherming naar eindpunt opsporen en reageren

Het verdedigen van bedrijfsgegevens in het huidige IT-klimaat, geconfronteerd met een stijgende cyberbeveiligingsdreiging en een verlies van controle over de netwerkperimeter, vereist twee dingen: een conceptionele sprong en betere hulpmiddelen.

Het concept van een netwerk moet veranderen. Het idee van een netwerk als een hek rond een verzameling apparaten is niet meer van toepassing. Het is tijd de realiteit onder ogen te zien. 'Het netwerk' is een waanbeeld. Het komt voort uit verbonden apparaten, ieder op zich een eindpunt. Het netwerk beveiligen betekent het eindpunt beveiligen. En ieder eindpunt bestaat uit twee elementen: het apparaat en de persoon die het gebruikt. Ze moeten beide worden overwogen.

Maar het handhaven van beveiliging in dit nieuwe paradigma is veel gecompliceerder dan de simpele bureaucomputers-verbonden-met-ethernet-omgeving van weleer. Het vereist betere hulpmiddelen en die moeten worden bevorderd. Dit wordt erkend door 61% van Ponemon-respondenten.

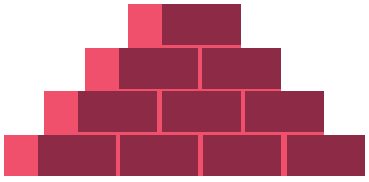
Het lastige is om de rest van de organisatie aan boord te krijgen. Slechts 36% van de respondenten had het gevoel genoeg budget en personeel te hebben voor eindpuntbeveiliging. 69% zegt dat de IT-afdeling niet kan voldoen aan de vraag van medewerkers naar betere ondersteuning. 71% zegt dat eindpuntbeveiligingsbeleid moeilijk uitvoerbaar is.22

80% van IT-beveiligingsmanagers beschouwt regelgevingsnaleving als de beste manier om de financiering van hun beveiligingsprogramma's te rechtvaardigen, maar beschouwen naleving tegelijkertijd als de minst belangrijke uitgavenpost. Naleving betekent voldoen aan het minimum.[23]

IT-besluitvormers moeten gekoppeld worden aan C-suite om het belang van beveiliging te onderstrepen. De kosten van een lakse beveiliging duidelijk maken, de onkosten voor herstel, de verloren inkomsten, de geslonken deelwaarde en de nadruk leggen op de langetermijnbesparingen. Veel beveiligingsoplossingen leiden ook elders tot verbeteringen. Denk aan de hogere productiviteit door het implementeren van printbeveiliging en de productiviteitsvoordelen van het regelmatig leveren van vernieuwde technologie in een flexibel CYOD-programma via een abonnement van een derde partij (zoals HP DaaS). Er kan een duidelijke bedrijfscase worden opgesteld.

De uitdaging is geweldig. En met de tijd, met de explosie van apparaten in het tijdperk van het internet der dingen en de toenemende verfijning van cybercriminaliteit, wordt het alleen maar beangstigender. Maar het is niet onoverkomelijk. Met de juiste technologie, de juiste strategie en de juiste hulpmiddelen kunnen we onze eindpunten verdedigen. We kunnen onze gegevens veilig houden.

Voor meer informatie en praktisch advies van HP's deskundigen. Om meer te weten te komen over HP Device as a Service en hoe dit u kan helpen een uitgebreid, flexibel en beveiligd CYOD-programma te draaien, bezoekt u ons **hier.**



Registreer voor updates
hp.com/go/getupdated

Delen met collega's

Beoordeel dit document

4AA7-1089NLE

[22] Ponemon 2016 State of the Endpoint Report

[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697