Cyberbeveiliging en uw bedrijf

De kosten van cybercriminaliteit en hoe u uw gegevens beschermt

U gebracht door

Inhoud

03 | Inleiding

05 | Mythes over cyberbeveiliging ontmaskerd

13 | De impact van cybercriminaliteit op bedrijven

24 | De toekomst van bedrijfscyberbeveiliging

29 | Woordenlijst en meer leesmateriaal

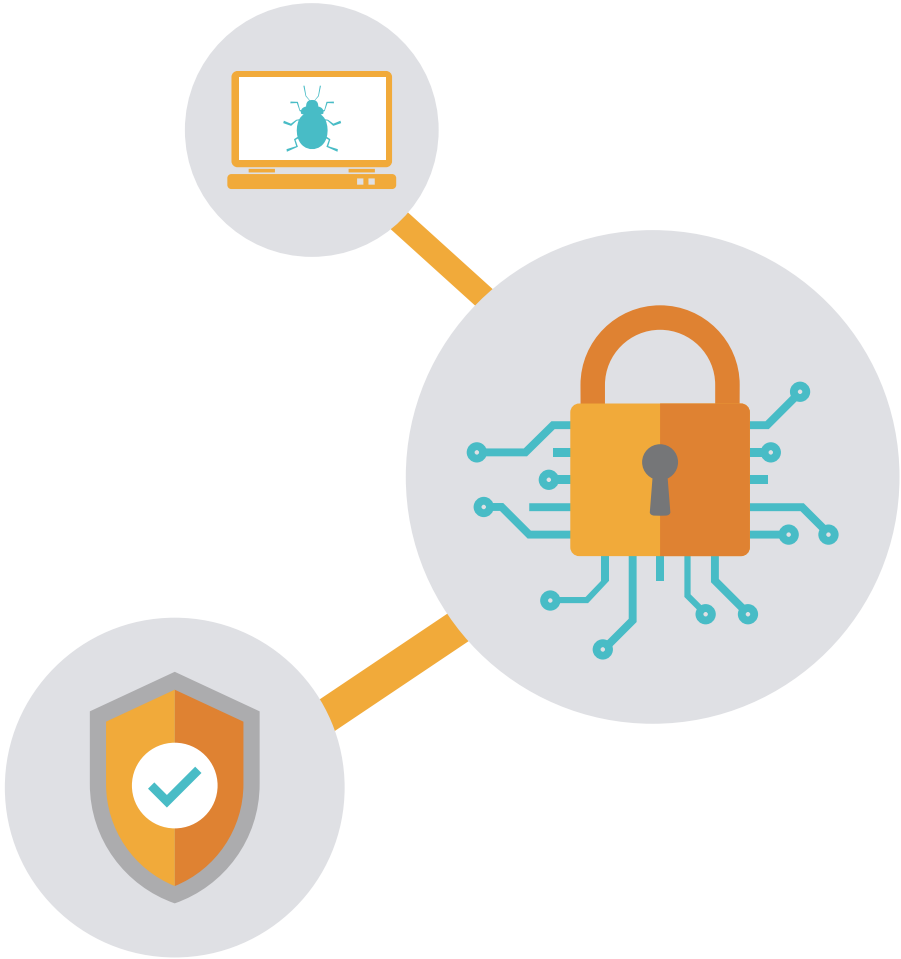
Inleiding

"Veel directeuren verklaren dat cyber het gevaar is dat bepalend zal zijn voor onze generatie." – Dennis Chesley, Global Risk Consulting Leading, PwC[1]

Cybercrime is op zich niet nieuw, maar neemt wel in omvang toe. Hackers worden beter. En ze hebben meer punten waar ze een netwerk kunnen binnendringen. The Internet of Things vermenigvuldigt het aantal eindpuntapparaten die vaak het gemakkelijkste toegangspunt zijn. Doelwitten nemen toe in volume en verstoring vindt plaats op grotere schaal.

Op 21 oktober 2016 onderging de in de VS gevestigde DNS-provider Dyn de grootste denial-of-service-aanval (DDoS-aanval) in de geschiedenis. Enkele van 's werelds grootste websites, waaronder Netflix,[2] Amazon en Twitter, waren noodgedwongen urenlang offline.

In januari 2017 onderging Lloyds Bank aanzienlijke online storingen. Klanten konden hun banksaldo niet controleren en geen betalingen verrichten. Mobiele toegang van apps lag er ook uit. Lloyds heeft niets bevestigd maar volgens hevige geruchten was een DDoS-aanval de oorzaak.[3]



Bronnen: [1] PwC: The Global State of Information Security Survey 2016 [2] http://thehackernews.com/2016/10/dyn-dns-ddos.html [3] https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Inleiding

Inbreuken als deze zijn niet alleen maar slechte publiciteit. Ze kosten echt geld.

In het 2016 Printer Security Survey Report van Spiceworks zei 34 procent van organisaties dat een inbreuk het aantal helpdesktelefoontjes en ondersteuningstijd verhoogt, 29 procent zei dat inbreuken productiviteit en efficiëntie verlagen, en 26 procent rapporteerde verhoging van systeemdefecten als een probleem.[4]

Bijna 60% van door een IBM CSO Assessment tijdschrift geïnterviewde beveiligingsleiders zei dat de geraffineerdheid van aanvallers het wint van de geraffineerdheid van het verdedigingsmechanisme van hun organisaties.[5] Bezorgde CIO's hebben cyberbeveiliging sinds 10 jaar tot een top-10-probleem benoemd, nu staat cyberbeveiliging op nummer twee in de jaarlijkse SIM Trends studie.[6]

Veel van deze schade kan worden voorkomen. In de volgende pagina's bespreken we verkeerde voorstellingen van cyberbeveiliging, kijken we meer gedetailleerd naar de impact van cybercriminaliteit op bedrijven en naar wat u kunt doen voor een betere verdediging tegen aanvallen. Tenslotte nemen we een kijkje in de toekomst en bespreken we wat we kunnen verwachten en hoe we ons daarop voorbereiden.

Bronnen: [4] HP Printer Security Research 2016, Spiceworks [5] IBM CSO Assessment 2014 [6] SIM IT Trends Survey 2015

Mythes over cyberbeveiliging ontmaskerd

Vijf veelvoorkomende verkeerde voorstellingen

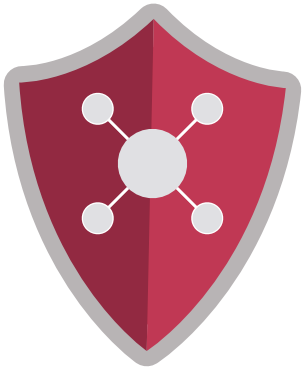
waardoor bedrijven risico lopen om slachtoffer te worden van cybercriminaliteit

De krantenkoppen over gegevensinbreuken bevatten namen die iedereen kent, maar alle soorten organisaties lopen risico. Hier zijn vijf mythes over cyberbeveiliging die bedrijven kwetsbaar maken voor hackers.

Beveiligings-inbreuk

Beveiligings-lekken

Beveiligings-beleid



Antivirus-software

Cyber-aanval

1 Bedrijven kunnen zich van iedere inbreuk snel herstellen

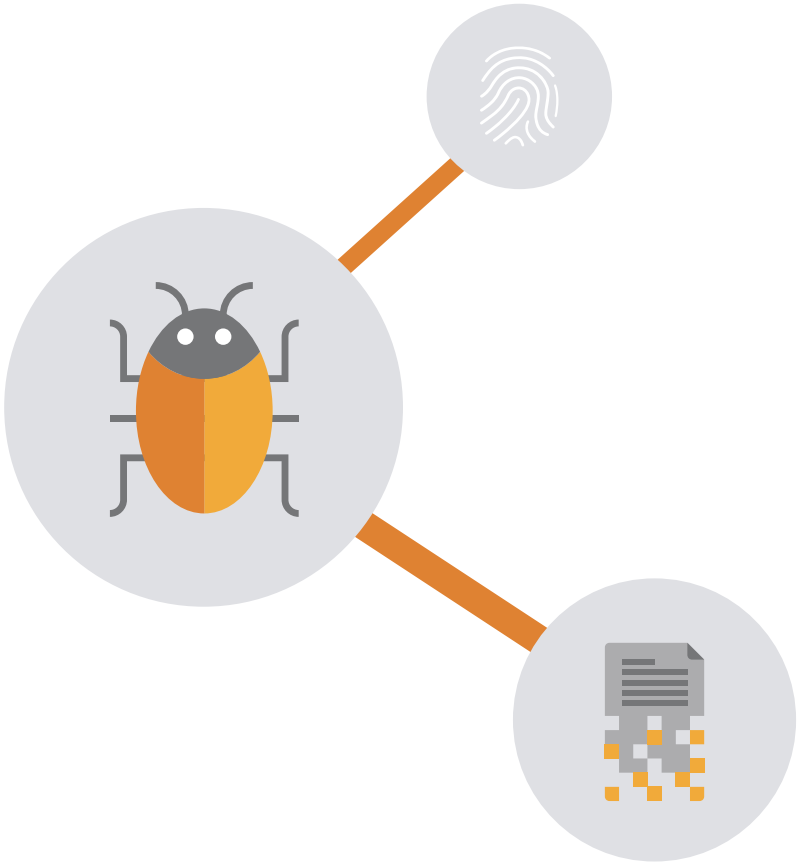
Het is nog steeds heel moeilijk om de kosten van cyberbeveiligingsinbreuken voor commerciële organisaties te meten. Men geloofde dat de impact van een inbreuk kon worden afgelezen aan de daling van aandelenwaarde.

Maar aandelenwaarde is maar een deel van het verhaal, het eerste deel. Waar de aandelenwaarde zich binnen enkele weken kan herstellen, stijgen langetermijnkosten daarentegen meer en meer. Het gaat dan om nieuwe beveiligingsprogramma's, de vervanging van personeel en juridische kosten.

Al deze factoren kunnen een bedrijf voor langere tijd na een inbreuk hinderen. En de kosten stijgen. Uit een recente studie van Ponemon bleek een verhoging van de algemene jaarlijkse kosten van een inbreuk van **$ 7,7 miljoen** in 2015 naar **$ 9,5 miljoen** in 2016.[7]

Bron: [7] Ponemon Institute Cost of Cyber Crime Study 2016

2 Beveiligingslekken vinden zelden plaats, dus serieuze bescherming is niet nodig



De IDC constateerde[8] dat het aantal bedrijven dat een inbreuk ervaren had in 2016 was gestegen tot 99 procent. Terwijl het aantal bedrijven dat rapporteerde 6 tot 10 keer in een jaar een inbreuk te hebben gehad omhoogschoot van 9% in 2014 naar 18,9% in 2016.[9]

Deze cijfers zijn wellicht aan de lage kant. Inbreuken worden aanzienlijk weinig gemeld omdat bedrijven proberen de daarmee gepaard gaande negatieve publiciteit te mijden. Een ander aspect dat ontbreekt aan deze mythe is de nasleep die een lek kan hebben. Misschien heeft uw organisatie maar één lek. Maar één lek kan de oorzaak zijn van aanzienlijke problemen.

Bronnen: [8] IDC [9] Ponemon Institute Cost of Cyber Crime Study 2016

3 We hebben een IT-specialist ingehuurd om beveiliging te regelen, dus we hoeven verder niets te weten

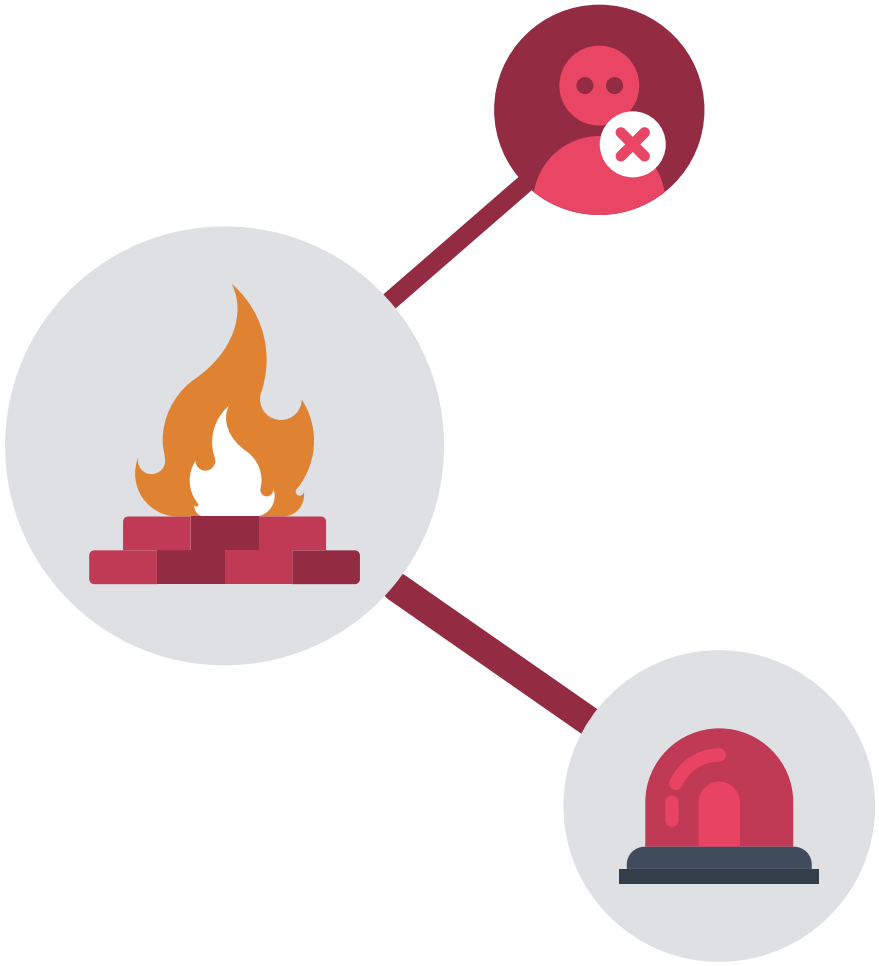
Inhuren van een deskundige is een goed idee, maar iedere werknemer in het bedrijf moet ook getraind worden in goed cyberbeveiligingsbeleid.

Denk aan de collega die argeloos een kwaadaardige bijlage van een e-mail opent of een onveilige website bezoekt en een bedrijfsnetwerk infecteert met malware die computers vertraagt of gevoelige informatie naar een cybercrimineel stuurt.

Volgens het 2016 Cyber Threat Report van CyberEdge rangschikten organisaties 'laag beveiligingsbewustzijn onder werknemers' als het leidende probleem dat verdediging tegen beveiligingsdreiging verhindert. Dit stond hoger dan 'gebrek aan budget' en 'gebrek aan vaardig personeel'.[10]

Bron: [10] Ponemon Institute Cost of Cyber Crime Study2016

4 We hebben krachtige antivirussoftware op onze systemen, dus we zijn goed beschermd



Antivirussoftware werkt door systemen te scannen op malware die is gedownload vanaf websites of e-mails. Maar aanvallers hebben andere middelen om die bescherming te omzeilen.

Cyberaanvallen die niet kunnen worden geblokkeerd door antivirussoftware omvatten gedistribueerde denial-of-service-aanvallen (DDoS-aanvallen), waarbij een website overspoeld wordt met junkverkeer, waardoor de website wordt vertraagd of stopgezet; webgebaseerde aanvallen, waarbij hackers kwaadaardige codes in een site injecteren voor doeleinden als gegevensdiefstal of spionage op afstand; en hackers die toegang krijgen via gestolen apparaten.

5 Als een indringer binnenkomt, merken we het meteen

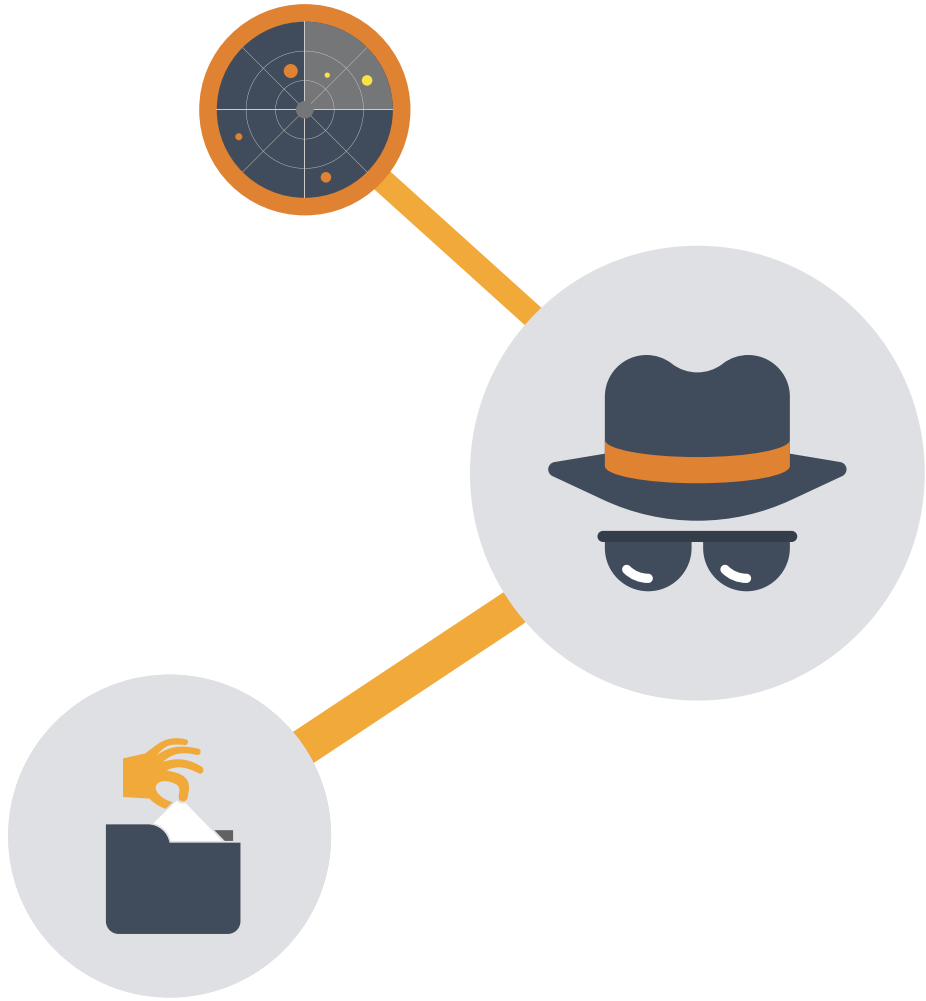
Het is niet gemakkelijk om een cyberaanval op te sporen. Malware die een systeem binnengaat verstoort wellicht niet onmiddellijk activiteiten; in plaats daarvan wordt mogelijk het systeem bespioneerd en krijgt de hacker informatie om meer gerichte aanvallen te plannen, vaak om toegang tot het volledige netwerk te krijgen.

Dergelijke aanvallen op specifieke systemen worden geclassificeerd als advanced persistent threats (APT). APT-aanvallen worden gekenmerkt door continue monitoring en gegevensverzameling van een specifieke computerinfrastructuur over een langere periode, meestal zonder dat het wordt opgemerkt.

IT consultancy Daisy Group schatte dat de helft van de bedrijven in het Verenigd Koninkrijk in minder dan een uur zou kunnen worden gehackt.

TIP:
Het monitoren van uitgaande gegevens voor verkeer dat intensiever dan gewoonlijk is kan helpen bij het identificeren van gegevensdiefstal. Het kan gaan om een APT-aanval.

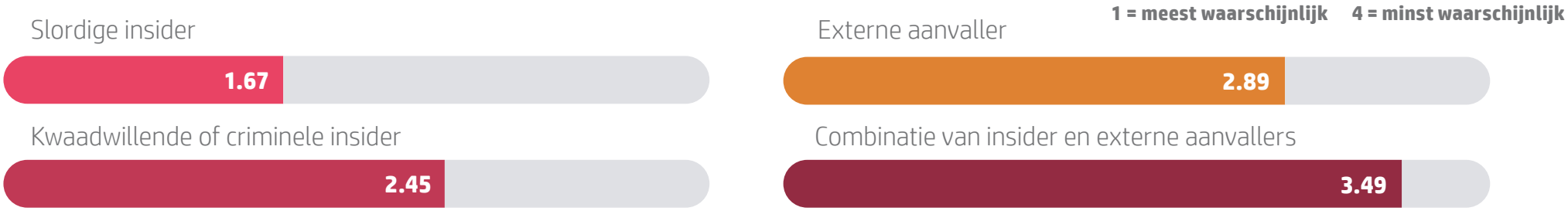
ACTIE ONDERNEMEN:
Kies beveiligingssoftware met gegevensbescherming, zoals HP SureStart, die automatisch het BIOS van een computer terugzet als een malware-aanval wordt ontdekt. Hierdoor worden inbreuken stopgezet voordat gegevens in gevaar komen.



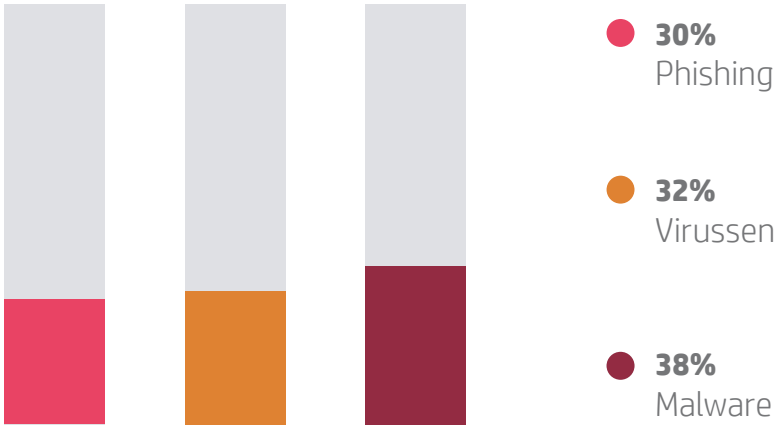
Waar komen dreigingen vandaan?

Beschermen van uw netwerk begint met weten wat uw zwakste schakels zijn

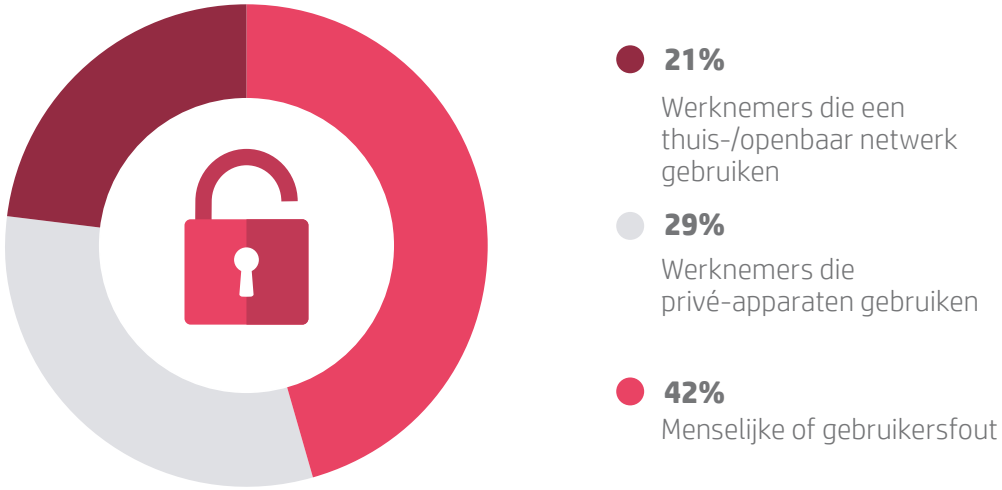
De meest waarschijnlijke oorzaak van gegevensinbreuk:[11]



Meest voorkomende soorten externe dreigingen:



Hoe interne inbreuken gebeuren:[12]



Bronnen: [11] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [12] Ponemon Institute Cost of Cyber Crime Study 2015

Wat kost het om te herstellen van cybercriminaliteit?

De soorten cyberaanvallen die het meest kosten:

25%

£1,000,000

Kwaadaardige code en malware

Software die een systeem beschadigt door gaten in de beveiliging te creëren, bestanden te beschadigen of gegevens te stelen (waaronder scripts, virussen en wormen)

24%

£960,000

Gedistribueerde Denial of Service

'DDoS'-aanvallen zijn overstromingen van webverkeer die de site en servers van een bedrijf neerhalen

16%

£640,000

Webgebaseerde aanvallen

Aanvallen gericht op bezoekers van uw site, zoals een geïnjecteerde code die browsers omleidt naar malware bevattende sites

13%

£520,000

Gestolen apparaten

Verloren werknemersapparaten met toegang tot inloggegevens van het bedrijf kunnen leiden tot gegevensdiefstal en identiteitsfraude

9%

£360,000

Phishing en social engineering

E-mails of pop-ups die zich voordoen als rechtmatige verzoeken om in te loggen

9%

£360,000

Kwaadwillende insiders

Werknemers die gevoelige informatie weggeven

4%

£160,000

Botnets

Netwerken van geïnfecteerde computers die worden beheerd voor kwaadwillende activiteiten zoals het verzenden van spam

Bron: [13] Ponemon Institute Cost of Cyber Crime Study 2015

De impact van cybercriminaliteit op bedrijven

De werkelijke kosten van cybercriminaliteit gaan verder dan het repareren van de schade van een hack

Beveiligingsinbreuken zijn ongelooflijk kostbaar. Grofweg zijn er drie manieren waarop een inbreuk uw bedrijfsfinanciën kan raken.

Bedrijfshulpmiddelen

Vanzelfsprekend moet u orde op zaken stellen. Daarvoor is een aanzienlijke hoeveelheid tijd van werknemers en geld nodig. Dat kan betekenen dat u ander, winstgevend werk enige tijd stop moet zetten.

Boetes

U kunt een boete krijgen voor niet-naleving (bijv. HIPAA). Als EU GDPR volgend jaar van kracht wordt kunnen bedrijven die worden beschuldigd van onachtzaamheid te maken krijgen met een totale boete van 4% van hun wereldomzet. U kunt zelfs het risico van rechtsgedingen lopen als het lek leidt tot een inbreuk van vertrouwelijke klantgegevens.

Beschadigde reputatie

Dit kan een van de meest schadelijke invloeden van een inbreuk zijn. Klanten, de media en het publiek vergeten beveiligingsinbreuken niet snel. Het kan lang duren om het vertrouwen terug te winnen.

Anatomie van de onverwachte hack

Toen Sony Pictures in 2014 werd gehackt, liepen de hackers gewoon door de voordeur naar binnen.[14]

Volgens 'Lena' van hackinggroep Guardians of Peace (GOP), die de verantwoordelijkheid opeist voor de aanval, "doet Sony niet meer aan fysieke beveiliging". Ze kregen toegang tot Sony's netwerk door fysiek het gebouw binnen te gaan en de inloggegevens te stelen van een systeembeheerder.

Eenmaal binnen plantten ze malware die privébestanden, broncodes en wachtwoorden stal voor databases van Oracle en SQL. Van daaruit stalen ze filmproductieschema's, e-mails, financiële documenten en meer, en publiceerden veel daarvan online.

De hackers dreigden verdere geheime en topgeheime gegevens te publiceren als het bedrijf de film 'The Interview' niet terughaalde uit bioscopen.

Sony capituleerde uiteindelijk, waardoor kaartverkoop (bedrag onbekend) verloren ging en ongelooflijk veel reputatieschade werd opgelopen.

Sony maakte twee fouten. Ze hielden geen rekening met fysieke toegang tot bedrijfsgegevens door indringers, en investeerden niet in meervoudige beveiligingslagen, die toegang tot gevoelige informatie na de eerste inbreuk hadden kunnen voorkomen.

Zoals beveiligingsdeskundige Bruce Schneier na de aanval schreef: "Tegenover een voldoende vaardige, kapitaalkrachtige en gemotiveerde aanvaller zijn alle netwerken kwetsbaar." Het lastige is te herkennen waar uw netwerk kwetsbaar is. Het kan de voordeur zijn.

ACTIE ONDERNEMEN:
Stel een inbreukresponsplan op voor iedere afdeling, van IT tot klantenservice, om de herstelperiode zoveel mogelijk te verkorten.

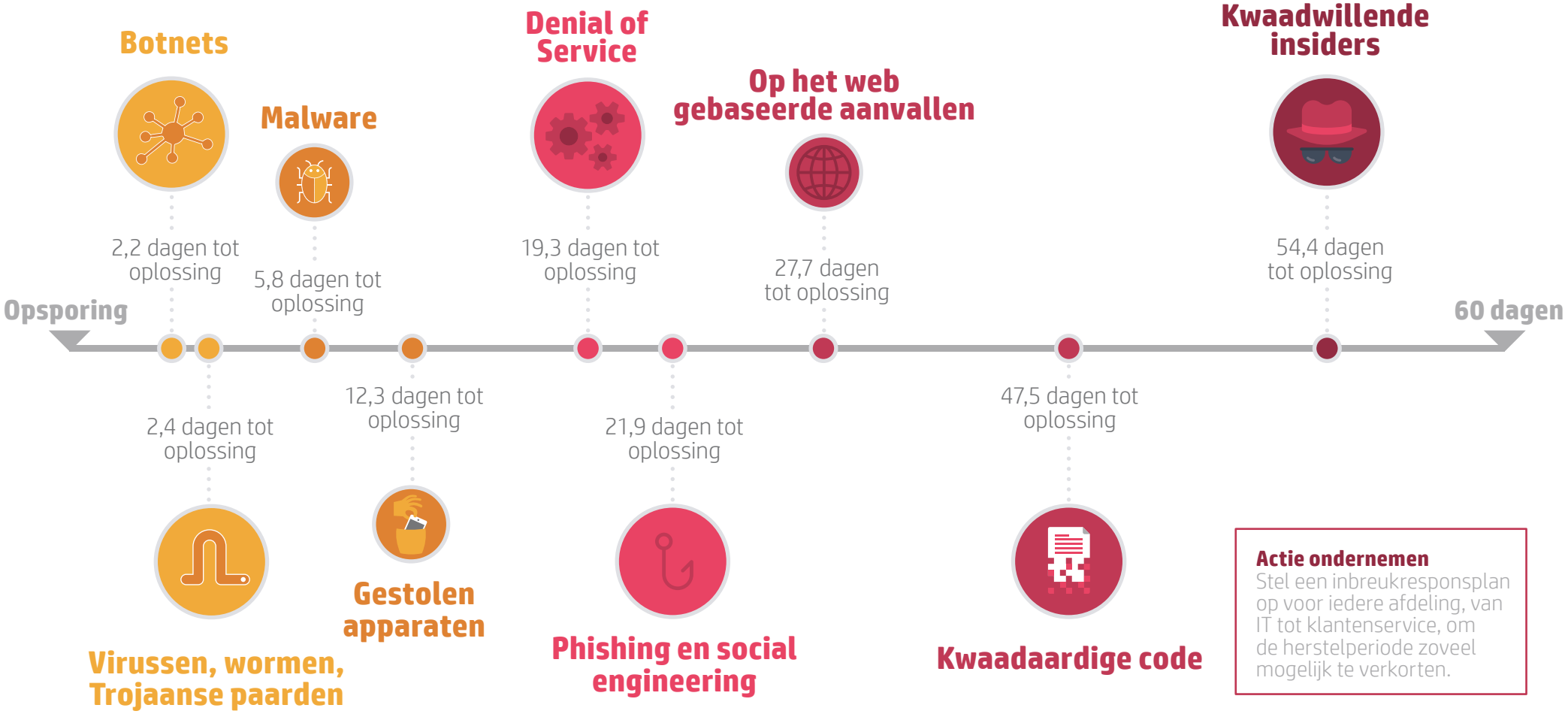
TIP:
Veel vormen van malware worden doorgegeven als e-mailbijlagen. Geef training aan personeel in het herkennen van verdachte bestanden die ontworpen zijn om eruit te zien als legitieme documenten.

- Geschatte kosten voor bedrijven in het Verenigd Koninkrijk vanwege cybercriminaliteit: $ 21 miljard[15]
- Gemiddelde kosten van cybercriminaliteit per bedrijf in het Verenigd Koninkrijk in 2016: £ 5,7 miljoen[16]
- Ondernemingen in het Verenigd Koninkrijk die een cyberinbreuk of -aanval ervoeren in 2015-2016: 66%[17]

Bronnen: [14] http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T [15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[16] https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ Stat is $7.21m – have converted to £
[17] https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

Cybercriminaliteit: de herstelperiode

Hoe lang duurt het om de schade van een gegevensinbreuk te repareren? The Ponemon Institute[18] stelt het gemiddelde op 46 dagen, een potentieel vernietigend cijfer voor mkb's in het Verenigd Koninkrijk die afhankelijk zijn van ononderbroken activiteiten



Actie ondernemen
Stel een inbreukresponsplan op voor iedere afdeling, van IT tot klantenservice, om de herstelperiode zoveel mogelijk te verkorten.

Bron: [18] Ponemon Institute Cost of Cyber Crime Study 2015

Hoe u uw bedrijf tegen cybercriminaliteit beschermt

Wezenlijke tips en strategieën voor bedrijfscyberbeveiliging

Hier zijn zes veelvoorkomende doelwitten voor hackers die inbreken in bedrijfssystemen en wat u daar vandaag de dag aan kunt doen.

Klant-databases

Cloud-diensten

Smartphones en tablets personeel

Fouten werknemers

Internet der dingen

Netwerk gateways

In de verschuiving naar een steeds digitalere wereld waar gegevens van steeds hogere waarde worden, kan cybercriminaliteit vele vormen aannemen. Cybercriminelen zitten meestal achter informatie aan, en met meer verbonden apparaten op de werkplek - van smartphones en tablets tot wifiprinters - groeit het aantal toegangspunten waar hackers op kunnen richten.

1 Klantdatabases

Financiële gegevens zijn lang niet het enige doelwit voor aanvallers. Informatie zoals namen en e-mailadressen kunnen worden gebruikt voor identiteitsfraude, spamming of om andere accounts te hacken.

Een grote prijs voor serieuze hackers is het kraken van bedrijven die diensten verlenen aan nog grotere bedrijven. Zie het als de digitale equivalent van een inbraak in een ijzerwinkel, alleen om toegang te krijgen tot de muur in het souterrain die tevens de muur is van de kluisruimte van de nationale bank ernaast.

Als aanvallers eenmaal binnen het kleinere systeem zitten, hebben ze meer kans om toegang te krijgen tot de klantgegevens die in het bezit zijn van grote bedrijfsklanten. Hoe kan uw klantdatabase in gevaar komen? Virussen, wormen en Trojaanse paarden, gedownload vanaf kwaadaardige sites of e-mails, kunnen de noodzakelijke code loskrijgen die een hacker nodig heeft om naar binnen te gaan en gegevens te stelen.

Hoe u de gegevens van uw klanten beschermt

- Gebruik beveiligingssoftware die ontworpen is voor bedrijven en netwerk-, e-mail- en eindpuntbescherming bieden.
- Werk uw beveiligingssoftware voortdurend bij om ontwikkelende malware te blokkeren.
- Download software-updates voor uw systeemprogramma's, omdat oudere programma's kwetsbaarheden kunnen bevatten die aanvallers kunnen uitbuiten.

2 Clouddiensten

Hoe u de gegevens van uw klanten beschermt

- Versleutel uw belangrijkste informatie met gebruikmaking van tools zoals PKWARE's Smartcrypt technologie, die toegangsbeleid gebruikt om de complexiteit van versleuteling vast te leggen. Op die manier zien bevoegde gebruikers de gegevens die ze behoren te zien en onbevoegde gebruikers zien niets.
- Maak een sterk wachtwoord aan voor uw cloudaccount. Definieer ook nauwkeurig in de instellingen voor uw cloudaccount wie toegang heeft tot uw gegevens en wat ze ermee kunnen doen.
- Eis tweezijdige authenticatie, zoals een smartphonecode en een wachtwoord, voor het aanbrengen van wijzigingen in cloudgegevens, zoals downloaden, verwijderen en verplaatsen van bestanden.

Cloud computergebruik is een basisartikel geworden in de bedrijfsinfrastructuur.

De 2016 IDG Cloud Computing Survey[19] constateerde dat 70 procent van ondernemingen minstens enige infrastructuur in de cloud heeft, terwijl Tripwire constateerde dat 90 procent de cloud gebruikt voor infrastructuur en/of gegevensopslag, waaronder missiegevoelige gegevens.[20]

Beveiliging is uiteraard een zorg, maar in werkelijkheid zijn gegevens beter beveiligd in de cloud, opgeslagen op externe servers door een bedrijf wiens reputatie afhangt van de bescherming van die gegevens.

Daarom ziet 64 procent van door Tripwire geënquêteerde ondernemingen de cloud als veiliger dan voormalige systemen.

Gelukkig is dit vertrouwen niet misplaatst. Volgens de 2015 BIS-enquête[21] onderging slechts 7 procent van bedrijven (klein en groot) een ernstige inbreuk op hun clouddiensten, en die zijn meestal het gevolg van toegangsbevoegdheden of wachtwoorden die niet afdoende zijn. Toch heeft een veilige cloud een solide intern beveiligingsbeheer nodig. Denk maar aan Sony's voordeur.

Bronnen:
[19] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey
[20] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/
[21] 2015 Enquête kleine bedrijven. Afdeling voor zaken, innovatie en vaardigheden

3 Smartphones en tablets personeel

Veel mensen gebruiken hun privé-apparaten voor kantoortaken.

De Bring-Your-Own-Device (BYOD) -beleidslijnen voor bedrijven zijn een effectieve manier om smartphones die werknemers al in hun bezit hebben beter te benutten. Deze trend neemt toe met 53,2 procent van organisaties die een BYOD-beleid binnen de komende twee jaar implementeren.[22] Maar deze apparaten kunnen een kant-en-klaar doelwit zijn voor hackers.

Naar schatting draagt een op de vijf Android-apps een vorm van binnendringende malware bij zich, die kan worden overgedragen naar bedrijfsbestanden en -systemen om activiteiten te monitoren of informatie te stelen.

Deze dreiging neemt toe met 64,9 procent van organisaties die stellen dat de omvang van bedreigingen voor hun mobiele apparaten is toegenomen.[23]

Werknemers van wie de telefoon gestolen is kunnen zonder het te weten een ingang zijn voor hackers. Een telefoondief kan een apparaat verkopen aan een koper op de zwarte markt die de telefoon kan ontleden om een inbreuk te plegen in het bedrijf van het slachtoffer, of om de systemen binnen te dringen van een grotere klant. 3,54 van de vijf organisaties achtten zich in staat zich te verdedigen tegen dreigingen die afkomstig zijn van mobiele apparaten. Dit was de laagste score voor alle potentiële bronnen van dreigingen die werden genoemd.[24]

Hoe u uw apparaten beveiligt die het eigendom zijn van personeel

- Installeer een tool die dreigingen opspoort zoals Duo's X-ray voor Android-apparaten om boosaardige apps en verdachte codes gemakkelijker te achterhalen.
- Vraag werknemers om 'wissen op afstand' toe te staan (kosteloos beschikbaar voor Android, iPhone en Windows Phone; met abonnement voor BlackBerry) zodat in het geval van verlies gevoelige bedrijfs- en privégegevens kunnen worden gewist.
- Vraag werknemers om apparaatversleuteling toe te staan op hun smartphones om gegevens te beschermen (dit staat standaard op nieuwe iOS- en Android-telefoons).

Bron: [22] 2016 Cyberthreat Defense Report, CyberEdge [23] ibid [24] ibid

4 Fouten werknemers

Hoe u uw personeel helpt

- Leid uw personeel op in best practices voor cyberbeveiliging en verstrek regelmatig trainingen om de nieuwste dreigingen voor te zijn.
- Ontwikkel een beveiligings-protocol dat op maat gemaakt is voor uw bedrijf en de soorten gegevens die het verwerkt.
- Stel een team samen voor het communiceren van uw cyberbeveiligingsbeleid aan zowel medewerkers als klanten en zakenpartners.

De belangrijkste grondregel van cyber-beveiliging is een goed wachtwoordbeleid. Toch was 31% van de zwaarste beveiligings-inbreuken in 2015 het gevolg van een personeelgerelateerd incident.

Van het hacken van zwakke wachtwoorden tot het stelen van documenten die worden ge-e-maild via een onbeveiligde verbinding, of een phishing e-mail gericht op een specifieke werknemer, aanvallers profiteren vaak van menselijke fouten.

5 Voorbereiden op het internet der dingen

Onderzoek van bedrijfs-IDC voorspelt dat in 2020 30 miljard apparaten verbonden zullen zijn met internet. Dit aantal wordt nu geschat op 13 miljard.[25]

Terwijl kantoorcomputers ten minste beveiligd zijn met wachtwoorden en idealiter met beveiligingssoftware, zijn printwachtrijen en printopdrachten vaak niet beschermd met gelijkwaardige beveiligingsprotocollen.

Dergelijke onbeveiligde printers, en andere hardware op het netwerk, kunnen een prooi zijn voor 'sniffing programs' die printopdrachten, netwerkverkeer, gebruikersnamen en wachtwoordgegevens kunnen loggen en terugsturen naar een voor cybercriminaliteit bedoelde server.

Het is van belang hier op te merken dat de veelgepubliceerde Dyn-inbreuk volgens de berichten verbonden was met een netwerk van webgestuurde CCTV-camera's, vervaardigd door één bedrijf, XiongMai Technologies. Volgens beveiligingsfirma Flashpoint.

Dit illustreert dat ieder apparaat op uw netwerk een eindpunt is en uw netwerk is slechts zo sterk als uw minst beveiligde apparaat. Zo'n 97 procent van organisaties heeft beveiligingsbeleid voor bureaucomputers en laptops, 77 procent voor mobiele apparaten en 57 procent heeft beveiligingsbeleid vastgesteld voor printers.[26] De enige manier voor alle bedrijven om beveiligd te blijven is beveiligingsbeleid vast te stellen voor ieder eindpuntapparaat.

Hoe u zich voorbereidt op het internet der dingen

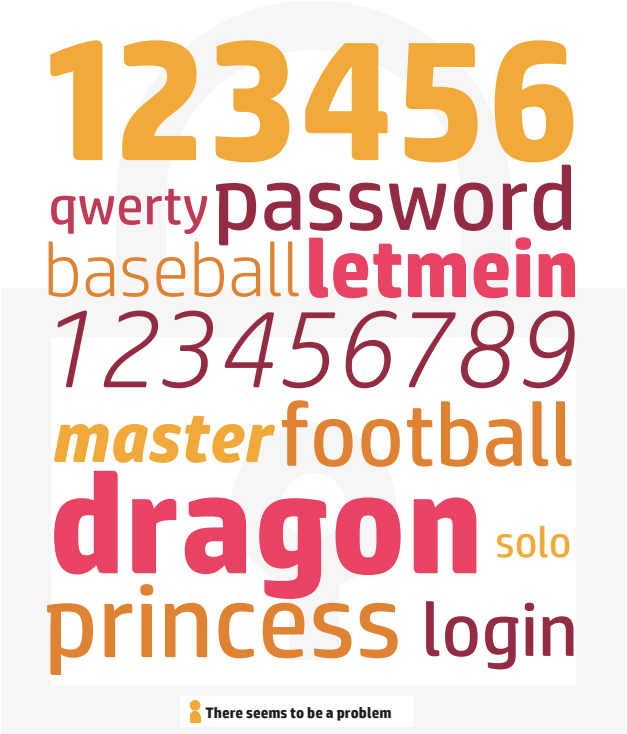
- Zorg voor verwijdering of uitschakeling van onnodige functionaliteit op hardware, want meer functies creëren meer toegangen voor aanvallers om binnen te komen.

Bronnen: [25] PwC: The Global State of Information Security Survey 2016 [26] HPI Printer Security Research, Spiceworks 2016

Wachtwoorden en ransomware

De meest voorkomende wachtwoorden

Begin 2013 kraakte een Ars Technica journalist, die nooit een cybercrimineel was geweest en ook geen ervaring had met het inbreken in met wachtwoord beschermde systemen, 8000 van meer dan 16.000 versleutelde wachtwoorden in één dag*. Dus wat voor kans hebben deze zeer veel gebruikte wachtwoorden tegen een vastbesloten kraker?



Wat is ransomware?

Cybercriminelen hebben zich steeds meer gewend tot ransomware, een vorm van malware die systemen kidnapt die vervolgens alleen kunnen worden gedeblokkeerd met de levering van een afkoopsom in bitcoin. Duizenden werden het slachtoffer in een uitbraak in 2013 van een Trojaans paard genaamd Cryptolocker die de aandacht trok van de National Crime Agency van het Verenigd Koninkrijk en diens National Cyber Crime Unit. Hier ziet u van dichterbij hoe dit soort aanvallen werkt.

	1. Installatie	Een kwaadaardige code werkt zichzelf uw computer binnen na een onbedoelde download via een e-mail of kwaadaardige website.
	2. Alarmeert zijn hoofdkwartieren	Ransomware verbindt met zijn home-server om een encryptie tot stand te brengen.
	3. Versleutelt uw bestanden	Ransomware scant de bestanden op uw netwerk en versleutelt ze, waardoor ze niet toegankelijk zijn.
	4. Afpersing	Meestal verschijnt een bericht op de computer van de gebruiker met een tijdslimiet en het te betalen bedrag om de bestanden te ontsleutelen voordat ze worden verwijderd.
	5. Betalen	Bedrijfseigenaar kan digitale valuta zoals bitcoin kopen om over te boeken naar de aanvaller, die hopelijk de bestanden zal ontsleutelen.

* Splashdata

6 Netwerk gateways

Als hackers een netwerk binnen willen gaan kunnen ze een DDoS-aanval loslaten: duizenden met malware geïnfecteerde machines worden met elkaar verbonden om zoveel junkverkeer te genereren dat het netwerk plat gaat onder het gewicht van de aanval.

Vaak willen DDoS-aanvallers sitebeheerders afleiden met een bevroren systeem, terwijl ze gegevens stelen of malware installeren voor toekomstige gegevensroof. Sommige DDoS-aanvallen zijn het resultaat van 'script kiddies', beginnende hackers die gewoonweg een website omlaag willen halen omdat ze het kunnen. Zelfs enkele uren verstoring van een website kan verwoestend zijn voor de omzet en reputatie van een bedrijf.

TIP:
Investeer in hardware die ingebouwde bescherming biedt zoals geavanceerde authenticatie en tools voor encryptie.

Hoe u uw netwerk beveiligt

- Bouw systemen die het verkeer controleren dat uw netwerk binnenkomt en verlaat. Een plotselinge stroomontlading kan wijzen op een aanval, terwijl constante maar niet te verklaren activiteit kan wijzen op een Trojaans paard dat gegevens verstuurt naar zijn moederschip.
- Filter al het verkeer, zodat alleen verkeer dat vereist is om uw bedrijf te ondersteunen op uw netwerk eindigt.
- Zorg dat iedere router, schakelaar of ander netwerkapparaat werkt met dezelfde basissoftware en -functionaliteit en download voortdurend software-updates.

De toekomst van bedrijfscyberbeveiliging

Met bedrijven die zo afhankelijk zijn van het internet is het steeds crucialer om solide cyberbeveiligingsverdediging op te bouwen.

Vandaag de dag nemen werknemers hun eigen apparaten mee naar het werk. Bedrijven huren cloud computing platforms in en maken gebruik van externe belangrijke technische diensten. En meer mensen werken nu op afstand. Cyberbeveiliging wordt moeilijk als u geen controle hebt over het apparaat, noch over de infrastructuur, noch over de werkruimte.

Tegelijkertijd hebben smartphones ons geleerd dat zaken overal en op ieder moment kunnen worden gedaan. Een café is net zo'n goede werkplaats als een kantoor. We gebruiken publieke wifi-netwerken om uitgebreide hoeveelheden zakelijke en privégegevens te verwerken, vaak over smartphones die zwak beveiligd zijn. Criminelen merken de verschuiving uiteraard op. Beveiliging heeft te lijden als we geen aandacht schenken aan de werkomstandigheden.

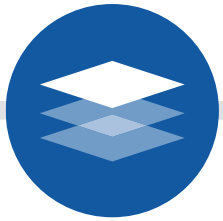
Voor de komende jaren betekent dat veel meer dan het toevoegen van antivirussoftware op onze apparatuur of het bijwerken van wachtwoorden ieder half jaar. In plaats daarvan moeten bedrijven verbeterde beveiligingsmaatregelen omarmen die net zo goed op afstand werken als op een kantoor, beheerd door een IT-beheerder

Voor de wijdverspreide organisaties van morgen hangt cyberbeveiliging af van verfijnde analyses die ongewoon gedrag isoleren en van gelaagde beveiliging die alle toegangspunten beschermt.

De toekomst van bedrijfscyberbeveiliging

Analyses: de cyberbeveiligingsdetective

Zelfs als uw site geen zwaar verkeer te verwerken heeft, zijn er toch patronen. Met gebruikmaking van analyse-tools die activiteiten meten en loggen is gemakkelijker een diagnose te maken als er iets niet in orde is. Deze tools werken door allereerst normaal gedrag te volgen en te documenteren zodat ze vervolgens onregelmatigheden kunnen opsporen. Eenmaal opgespoord kunnen beheerders de strijd aangaan en aanvallen verwijderen voordat ze de kans krijgen cyberchaos los te laten.



Lagen aanbrengen: blijf aanvallers een stap voor

Soms 'diepteverdediging' genoemd, beschermt gelaagde beveiliging ieder toegangspunt op meervoudige manieren. Veelvoorkomende benaderingen omvatten validatie van SSL-certificaten die het vervalsen van inloggegevens om een beveiligd netwerk binnen te gaan bemoeilijken. Het kan ook nuttig zijn daar meerzijdige authenticatie aan toe te voegen waardoor indringers meer dan alleen een wachtwoord moeten kraken.

Los van de specifieke technologie die wordt gebruikt is het principe van gelaagdheid het op enige manier vergrendelen van ieder gevoelig gebied in uw bedrijfsnetwerk. Uw gebruikers en partners zijn dan misschien meer tijd en inspanning kwijt om toegang te krijgen tot cruciale gegevens, maar dat ongemak wordt ruimschoots vergoed door gemoedsrust voor uw bedrijf.

Onderneem nu actie

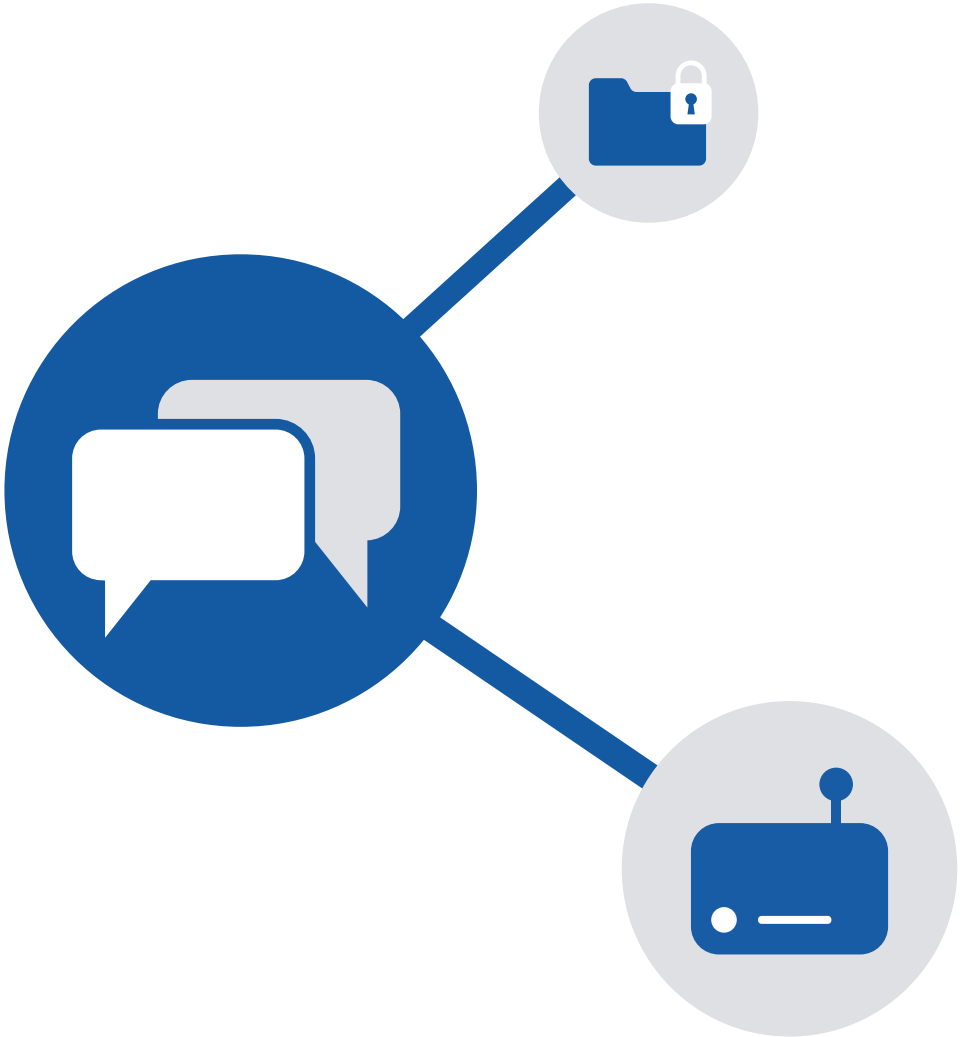
Investeren in cyberbeveiligingssoftware en -training is de beste vorm van verdediging. Begin met een audit van uw systemen en infrastructuur. Doet u genoeg? Wat zou u beter kunnen doen?

Ten slotte kunt u ook onze deskundigen hier bij Hewlett Packard Inc bellen. Onze collectieve kennisbasis is erop gefocust om niet alleen te reageren op dreigingen, maar om ze voor te zijn. Bezoek ons voor meer informatie op HP.com.

TIP:
Eerst normaal gedrag volgen en documenteren om vervolgens onregelmatigheden op te sporen.

Overwegingen voor eindpuntapparatuurbeveiliging

Beveiligen van ieder apparaat op uw netwerk



Beveiligingsresearch uitgevoerd door Spiceworks[27] bracht naar voren dat de hoofdoorzaken van beveiligingsdreigingen voor bedrijven waren:

- Laptops en bureaucomputers: 81% extern en 80% intern
- Mobiele apparaten 36% extern en 38% intern
- Printers 16% extern en 16% intern

Welke van deze dreigingen heeft het dringendst beveiliging nodig? Allemaal, is het heel eenvoudige antwoord. Dit mag dan overduidelijk lijken, toch is een alarmerend aantal organisaties nog steeds heel zuinig met welke apparaten er moeten worden beveiligd.

Het HP perspectief is dat ieder apparaat, dat verbonden wordt met uw netwerk, beveiligd moet zijn. Eenvoudig gezegd: uw netwerk is slechts zo veilig als uw minst beveiligde apparaat.

Intuïtieve logica zegt u wellicht dat het beveiligen van een verbonden printer niet zo belangrijk is als het beveiligen van uw vloot laptops. Maar het gevaar is hetzelfde. Hackers staan erom bekend zich te richten op dingen als printers, of welk smart-apparaat dan ook dat in verbinding staat met uw netwerk. Ze weten dat deze apparaten gewoonlijk niet erg goed beveiligd zijn, terwijl ze hetzelfde toegangsniveau hebben voor toegang tot uw netwerk.

Bron: [27] HP Printer Security Research 2016, Spiceworks

HP: Richting geven in een nieuw landschap

Cyberbeveiliging is aan het veranderen. We hebben de tools om bij te dragen aan uw verdediging.

Er zijn geen snelle reparaties in cyberbeveiliging. Een solide verdediging vereist een meerzijdige aanpak voor netwerken, apparaten en mensen gezamenlijk. Kiezen van de juiste technologie is een sterk begin.

Bij HP staat veiligheid bovenaan. De apparaten uit de HP Premium Elite-reeks hebben marktleidende beveiligingskenmerken die nergens anders verkrijgbaar zijn, zoals HP SureStart, 's werelds eerste zelfhelende BIOS.

HP voorzien hun apparatuur van:

- **Bluetooth-slot:** Met gebruik van Bluetooth vergrendelt de machine automatisch als u wegloopt en ontgrendelt als u terugkomt.
- **Biometrische beveiliging:** Gezichts- en vingerafdrukherkenning staan alleen toegang toe aan biometrisch geauthenticeerde gebruikers.
- **HP SureView schermen*:** De verduisterde monitor voorkomt dat mensen die langslopen uw scherm kunnen zien, waardoor vertrouwelijk materiaal wordt beschermd als u onderweg werkt.
- **HP SureStart zelfhelende BIOS:** Iedere HP Elite monitort zijn BIOS iedere 15 minuten. Bij ontdekking van een onregelmatigheid wordt de pc gereset naar zijn oorspronkelijke staat, waardoor binnendringers naar buiten worden geworpen.

Een HP Elite beschermt uw bedrijf niet in zijn eentje. Maar bouwt wel een sterke frontlinie. Ga naar www8.hp.com om meer aan de weet te komen over de volledige HP Elite-reeks.

* Geselecteerde modellen

HP: Toonaangevend in een nieuw printlandschap

Beveilig uw netwerk met de veiligste printers ter wereld*

"Dankzij jarenlange investeringen in printerbeveiliging heeft HP het breedste aanbod beveiligingsoplossingen en diensten op de markt."

– Quocirca, jan 2017**

HP apparaten beschikken over:

- **Runtime inbraakpreventie:** HP runtime inbraakdetectie beschermt printers wanneer de meeste aanvallen plaatsvinden: als ze gebruikt worden en verbonden zijn met het netwerk.
- **Jet Advantage Security Manager:** Dit biedt IT-managers een gestroomlijnde benadering voor onderzoek en, indien nodig, het aanpassen van beveiligingsinstellingen op apparaten, in het gehele printerpark, om te kunnen voldoen aan vooraf vastgestelde bedrijfsregels voor beveiliging.
- **HP SureStart zelfherstellend BIOS:** Tijdens het opstarten controleert HP Sure Start op kwaadaardige code, voorkomt dat deze wordt uitgevoerd en herstelt het BIOS. Er wordt een ingebouwde 'gouden kopie' van het BIOS geladen.
- **Whitelisting:** Dit zorgt ervoor dat alleen authentieke, bekende HP code in het geheugen wordt geladen. Wanneer een afwijking wordt gevonden, start het apparaat op in een veilige offlinemodus en ontvangt het IT-team een melding.

Bronnen: *5 Claim over 'De veiligste printers' is gebaseerd op een evaluatie door HP van in 2016 gepubliceerde beveiligingskenmerken in concurrerende printers uit dezelfde klasse. Alleen HP biedt een combinatie van beveiligingskenmerken die kan bewaken om aanvallen te detecteren, deze automatisch te stoppen en daarna bij het opnieuw opstarten de software-integriteit te valideren. **Quocirca, "Print security: An imperative in the IoT era," quocirca.com/content/print-security-imperative-iot-era, januari 2017.

Woordenlijst en verder leesmateriaal

Toegang beheertools

Botnet:
Verwijst meestal naar een soort geautomatiseerd programma dat ontworpen is voor toegang tot en beheer van met het internet verbonden computers zonder dat de eigenaar op de hoogte is. De computers zijn vaak geïnfecteerd met malware. Hackers gebruiken botnets om een **Denial of Service-aanval** op een website los te laten.

Tools ter preventie van gegevensverlies:
Een brede categorie van software met als doel gevoelige gegevens te monitoren en pogingen van onbevoegd personeel om toegang te krijgen en kopieën te maken te blokkeren. Verschillende aanpakken maken bescherming mogelijk bij het toegangspunt (bijv. het eindpunt), terwijl een netwerk of bestandssysteem doorlopen wordt. Gartner zorgde voor een groei in deze markt **met 25 procent** in 2013.

Versleutelingstechnologieën:
Tools die ervoor zorgen dat **de gegevens zelf onleesbaar zijn** zonder een soort decoder. De UK Information Commissioner heeft zich sterk uitgesproken **voor** verschillende soorten van encryptie de afgelopen jaren. Meer recentelijk werd de regering gedwongen **haar positie betreffende versleutelingstechnologie te herzien** na hevige kritiek.

Firewall-technologieën:
Een andere brede term die een apparaatstijl omschrijft die gebruikmaakt van algoritmes en andere technieken om onbevoegd(e) verkeer en gebruikers die een netwerk binnen willen gaan te blokkeren. **Nieuwe-generatie-versies** van deze apparaten hebben potentie doordat ze functies samenvoegen die voorheen werden uitgevoerd door separate apparaten. Intrusiedetectie bijvoorbeeld. Ze zijn ook vaak applicatiebewust en kennen het verschil tussen webverkeer vanaf een salesforce.com en vanaf een Facebook-pagina.

GRC-tools:
Bedoeld voor brede en gecoördineerde initiatieven binnen een bedrijf, gericht op het beheren en sturen van activiteiten op een wijze die in naleving is met regelgeving en die resulteren in risicoverlaging.

Malware:
Een brede categorie software die schade kan veroorzaken aan andere systemen of ze zelfs onklaar kan maken. Virussen, wormen en Trojaanse paarden zijn voorbeelden van malware. Verder wordt malware ten behoeve van de Ponemon-studie die overal in dit eBook wordt aangehaald beschouwd als verschillend van virussen die “zich bevinden in het eindpunt en nog niet een netwerk hebben geïnfiltreerd”.

Perimetercontroles:
Een algemene categorie die cyberverdediging omschrijft op het punt waar het openbare internet of een ander openbaar netwerk in contact komt met een privénetwerk dat in plaatselijk bezit en beheer is. **Meervoudige lagen en soorten apparaten** maken daar gewoonlijk deel van uit.

Phishing:
Gewoonlijk uitgevoerd via e-mail, waarbij een aanvaller vraagt om identificatie-informatie in een dialoogvak dat er legitiem uitziet.

Tools voor beleidsbeheer:
Ruim gedefinieerd stellen tools voor beleidsbeheer de norm voor wat bepaalde gebruikers wel en niet kunnen zien en leggen dan dat beleid op door het gehele netwerk. Consistentie (in ieder geval theoretisch) zorgt voor beveiliging.

Woordenlijst en verder leesmateriaal

Beveiligingsintelligentiesystemen:
Een brede variëteit van beveiligingsintelligentie kan bijdragen aan het verzamelen en samenvoegen van informatie betreffende dreigingen. Systemen variëren van logmanagers tot systemen om netwerkonregelmatigheden op te sporen.

Social engineering:
Waarbij een aanvaller een bevoegde gebruiker dwingt gegevens los te laten die hij niet mag vrijgeven, waardoor een aanvaller toegang krijgt.

Trojaans paard:
Met de impact van een virus of worm, moeten Trojaanse paarden worden geïnstalleerd door de gebruiker en zijn derhalve slim gecamoufleerd. De gevolgen variëren van wijziging in computerinstellingen tot het verwijderen van bestanden en het maken van een 'achterdeur' waar de hacker later gebruik van maakt.

Virussen:
Kwaadaardige code die in staat is tot vermenigvuldiging en spreiding over een geheel netwerk.

Op het web gebaseerde aanvallen:
Meestal betreft een op het web gebaseerde aanval het omleiden van een browser naar een kwaadaardige site.

Wormen:
In tegenstelling tot virussen die zich verspreiden bij het delen van een gastbestand kunnen wormen zich onafhankelijk van een gastbestand zoals een Word document of Excel spreadsheet vermenigvuldigen en hebben daarom verder geen menselijke interactie nodig om verwoesting aan te richten. Instant messaging-systemen staan erom bekend wormen te hebben verspreid; Skype onderging die inbreuk in 2012.

4AA7-1085NLE