Wordt je aangeboden door:

ESET

Gegevensbescherming

voor dummies

- Begrijp het huidige dreigingslandschap
- Vind manieren om je kleine/middelgrote bedrijf te beschermen
- Minimaliseer de impact van een datalek

Speciale ESET-editie

Lawrence Miller

Over ESET

ESET begon als pionier op het gebied van antivirusbescherming door veelgeprezen software voor de detectie van dreigingen te creëren. Nadat we 30 jaar lang IT-beveiliging hebben ontwikkeld die tot de beste in de branche behoort, stellen onze oplossingen bedrijven en consumenten in meer dan 200 landen en regio's in staat het maximale uit hun digitale wereld te halen. Het ambitieuze doel van ESET is ervoor te zorgen dat iedereen kan genieten van de adembenemende kansen die technologie te bieden heeft. "

Gegevens-bescherming

Speciale ESET-editie

door Lawrence Miller

voor dummies®

Gegevensbescherming voor Dummies®, speciale ESET-editie

Gepubliceerd door: **John Wiley & Sons, Ltd.**, The Atrium, Southern Gate Chichester, West Sussex, www.wiley.com

Maatschappelijke zetel

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, Verenigd Koninkrijk

ISBN 978-1-119-54774-7 (pbk); ISBN 978-1-119-54776-1 (ebk)

Gedrukt in Groot-Brittannië

10 9 8 7 6 5 4 3 2 1

Dankwoord van de uitgeverij

Enkele van de mensen die geholpen hebben dit boek op de markt te brengen, zijn:

ESET Nederland: Dave Maasland en Wessel Veltman

De Volksbank: Rick van de Westelaken

Inleiding

"Nee, jouw bedrijf is veel te klein om aan te vallen." Dat heeft geen hacker ooit gezegd. Cybercriminelen zijn opportunistische roofdieren. Ze zullen zich misschien niet specifiek richten op jouw kleine of middelgrote bedrijf. Maar als je bedrijf, om welke reden dan ook, verbonden is met het internet, zullen ze je zeker kunnen vinden. Als de netwerken, servers, applicaties, gegevens, desktops, laptops en mobiele apparaten van je bedrijf niet voldoende worden beschermd, kunnen kwaadwillenden je bedrijf binnendringen. Een datalek zal jouw bedrijf geen 15 beschamende minuten op RTL of NOS opleveren, zoals wel het geval was bij bedrijven als Bupa, CEX, Clarksons, Equifax, Target, Uber of Yahoo! Maar het zal wel ernstige gevolgen hebben, misschien wel zo ernstig dat je uiteindelijk de deur van je bedrijf definitief moet sluiten. Beveiliging is steeds vaker een unique selling point, met name in dit digitale tijdperk, en je moet dit boek dan ook zien als een investering en eerste stap naar beter digitaal zakendoen.

Datalekken en cyberaanvallen zijn niet nieuw, maar veel van de technieken en tactieken die worden gebruikt door moderne cybercriminelen zijn dat wel. Deze zijn bij uitstek geschikt om kwetsbare kleine en middelgrote ondernemingen (het mkb) aan te vallen. 99 procent van alle bedrijven wereldwijd behoort tot het mkb. Het mkb heeft meer dan de helft van de wereldwijde beroepsbevolking in dienst en is goed voor meer dan de helft van het bruto binnenlands product (bbp) van de wereldeconomie. Bij nieuwe aanvalsmethoden moet je onder andere denken aan:

- veelvoorkomende malware-technieken, ransomware en Remote Access Trojans (RAT's)
- Cryptojacking
- Directory Harvest Attacks (DHA's), gerichte spam- en phishing (spearphishing)-campagnes en CEO-fraude via e-mail.
- massieve, geautomatiseerde botnets
- de kaping van domeinnamen (DNS) en DNS-cache poisoning
- gedistribueerde denial-of-service (DDoS)-aanvallen

Veiligheidsdreigingen zijn ernstiger en frequenter dan ooit tevoren en kleine en middelgrote ondernemingen, die over het algemeen kleine IT-operaties hebben met beperkte middelen en personeel, zijn

vaak een gemakkelijk doelwit voor cybercriminelen. Aan de andere kant is het voordeel dat kleine en middelgrote bedrijven kleiner zijn en daarnaast minder met het internet verbonden apparaten hebben dan grote bedrijven, en dus flexibeler zijn wanneer het aankomt op het kiezen en uitvoeren van strategieën voor gegevensbescherming. Als de juiste stappen worden genomen, kunnen kleine en middelgrote bedrijven ervoor zorgen dat ze een aanzienlijk kleiner aanvalsoppervlak hebben.

In dit boek kom je van alles te weten over de beveiligingstechnologieën, hulpmiddelen en processen die je nodig hebt om je bedrijf beter in staat te stellen zijn gegevens en IT-middelen te beschermen en het effect van een datalek effectief tot een minimum te beperken.

Over dit boek

Gegevensbescherming voor Dummies, beperkte ESET-editie, bestaat uit zes korte hoofdstukken waarin wordt ingegaan op:

- Cyberaanvallen en -trends, het regelgevingslandschap en de impact van een lek op een bedrijf (hoofdstuk 1).
- Verschillende technologieën voor gegevensbescherming, toepassingsopties en servicemodellen evalueren (hoofdstuk 2).
- Het risicobeoordelingsproces, je activa identificeren, bedreigingen analyseren en kwetsbaarheden beoordelen (hoofdstuk 3).
- Verschillende technologieën voor gegevensbescherming, zoals versleuteling, endpointbescherming, firewalls en meer (hoofdstuk 4).
- Belangrijke organisatorische en procesmatige controles die noodzakelijk zijn om een effectieve gegevensbescherming te waarborgen (hoofdstuk 5).
- Tien belangrijke punten voor effectieve gegevensbescherming voor kleine en middelgrote ondernemingen (hoofdstuk 6).

We hebben ook een woordenlijst toegevoegd aan het eind van het boek om je te helpen afkortingen en termen die je niet kent, snel te ontcijferen.

Dwaze veronderstellingen

We gaan er voornamelijk van uit dat je een IT-professional bent die voor een klein of middelgroot bedrijf werkt. Misschien ben je de manager van een klein IT-team dat "van alle markten thuis is". Of misschien vorm je het hele IT-team wel in je eentje! Jij en je team (met één of meerdere personen) zijn verantwoordelijk voor zo'n beetje alles: van het verwisselen van printertoners en het opzetten van endpoints voor gebruikers, tot het beheren van het netwerk van je bedrijf en het oplossen van beveiligingsproblemen. Voor je functie moet je dus over kennis en ervaring beschikken op allerlei IT-terreinen. Maar er zijn misschien terreinen - zoals beveiliging en gegevensbescherming - waarvan je vindt dat je kennis en ervaring een beetje tekortschieten.

Als je jezelf herkent in deze veronderstellingen, dan is dit boek voor jou bedoeld! En zo niet, lees dan ook gewoon door. Als je dit boek uit hebt, zal je namelijk een stuk meer weten over gegevensbescherming.

Pictogrammen die in dit boek worden gebruikt

In dit boek gebruiken we af en toe speciale pictogrammen om je te wijzen op belangrijke informatie. Dit is wat je kunt verwachten:

BELANGRIJK OM TE ONTHOUDEN

Dit pictogram wijst op informatie die je moet opslaan in je niet-veranderlijke geheugen, ofwel je grijze massa, samen met verjaardagen en jubilea!

TIP

Tips worden gewaardeerd, maar nooit verwacht. En we hopen zeker dat je deze tips zal kunnen waarderen. Dit pictogram duidt op handige stukjes informatie en bruikbare adviezen.

WAARSCHUWING

Deze meldingen duiden op praktisch advies om potentieel kostbare of frustrerende fouten te vermijden.

Als je nog meer wilt weten

We kunnen in dit korte boek niet alles behandelen. Als je nog meer te weten wilt komen en je afvraagt waar dat kan, ga dan naar `www.eset.nl/mkb`.

De vervolgstappen

Onze excuses aan Lewis Carroll, Alice en de Cheshire Cat:

"Kun je me vertellen welk pad ik moet nemen om hier weg te komen?"

"Dat hangt ervan af waar je heen wilt", zei de kat. Oh nee, we bedoelen natuurlijk de Dummies-lezer.

"Dat maakt me niet zoveel uit …", zei Alice.

"Nou, dan maakt het ook niet uit welk pad je kiest!"

Dat geldt zeker voor *Gegevensbescherming voor Dummies*, een boek dat, net als *Alice in Wonderland*, gedoemd is een tijdloze klassieker te worden!

Als je niet weet waar je heen gaat, zal elk hoofdstuk je op je bestemming krijgen. Maar hoofdstuk 1 is misschien een goede plek om te beginnen! Als je echter een onderwerp ziet dat je aandacht trekt, sla dan vooral een paar bladzijden over en ga rechtstreeks naar dat hoofdstuk. Elk hoofdstuk kan afzonderlijk worden gelezen, dus je kunt zelf kiezen in welke volgorde je dit boek leest (op zijn kop of achterstevoren kunnen we echter niet aanraden).

We beloven je dat je niet zal verdwijnen in een konijnenhol!

IN DIT HOOFDSTUK

- De daadwerkelijke kosten van een datalek meten
- Het actuele panorama van dreigingen analyseren
- Leren van fouten uit het verleden
- Begrijpen waarom naleving van wetgeving belangrijk is

Hoofdstuk 1
Waarom gegevensbescherming een must is

In dit hoofdstuk leer je welke impact een datalek op je bedrijf kan hebben, hoe het actuele panorama van dreigingen zich heeft ontwikkeld, welke impact recente datalekken hebben gehad op andere kleine en middelgrote bedrijven (mkb) en wat de veranderende eisen in de wet- en regelgeving voor jouw bedrijf betekenen.

De zakelijke impact van datalekken begrijpen

99 procent van de bedrijven in de EU en 95 procent van de bedrijven wereldwijd behoort tot de categorie klein of middelgroot (mkb). Het is dan ook geen verrassing dat volgens de International Data Corporation (IDC) de slachtoffers van datalekken in meer dan 70 procent van de gevallen kleine of middelgrote bedrijf zijn. Toch gaan veel bedrijven ervan uit dat zij, omdat ze klein zijn en beperkte middelen hebben, niet het slachtoffer zullen worden van cyberaanvallen. Maar dat is helaas niet het geval.


BELANGRIJK OM TE ONTHOUDEN

Volgens het *Data Breach Investigations Report* (DBIR) van Verizon uit 2017 richten aanvallen (met name aanvallen op points-of-sale) zich steeds meer op restaurants en kleine bedrijven. Bovendien zijn de slachtoffers van de top zes van dreigingen - gestolen inloggegevens, onbekende achterdeuren (in firmware, software of hardware),

spyware, phishing, data-exfiltratie en malware die wordt aangestuurd door command-and-control (C2) software - in driekwart van de gevallen op het web gebaseerde, kleine bedrijven die niet actief zijn in de retailsector.

In het VK meldde verzekeraar Zürich dat vorig jaar 875.000 kleine en middelgrote bedrijven het slachtoffer werden van cyberaanvallen en dat dit meer dan een vijfde van die bedrijven meer dan $ 13.000 kostte en één op de tien zelfs meer dan $ 69.000. Ter vergelijking: uit het *Cost of a Data Breach Study* van het Ponemon Institute uit 2017 bleek dat de gemiddelde kosten van een datalek voor grote bedrijven ongeveer $ 3,62 miljoen bedragen.

Volgens de bevindingen van een studie over de wereldwijde kosten van datalekken, zijn de gemiddelde kosten van datalekken tussen 2014 en 2015 meer dan verdubbeld en stegen de gemiddelde kosten van elke kwijtgeraakte of gestolen record ook licht, naar bijna 150 euro. Hieruit blijkt dat de algehele kosten van een datalek door de jaren heen niet aanzienlijk zijn veranderd. Het is een permanente kostenpost waarop organisaties voorbereid moeten zijn en die zij in hun gegevensbeschermingsstrategieën moeten opnemen.

De kosten van een lek zijn voor het mkb aanzienlijk lager dan voor grote bedrijven, maar kleinere bedrijven hebben vaak niet de - financiële en andersoortige - middelen om te reageren op een groot datalek en zich erna weer te herstellen. Aangezien in regelgeving als de Algemene verordening gegevensbescherming (AVG) van de EU van bedrijven - ongeacht hun omvang - wordt geëist dat zij in het geval van een lek precies kunnen beschrijven wat er is gebeurd en wat de oorzaken waren, zullen de kosten van lekken voor het mkb in de toekomst waarschijnlijk nog verder stijgen.

TIP

Een cyberverzekering is een manier voor het mkb om de kosten van een cyberaanval of datalek binnen de perken te houden. Maar een cyberverzekering beschermt je niet tegen een aanval of lek en is GEEN alternatief voor de toepassing van goede praktijken, beleid, controles en technologieën op het gebied van beveiliging.

Een veiligheidslek leidt onder andere tot de volgende kosten:

- verstoring van de activiteiten van een bedrijf (waardoor onder andere tijd en productiviteit verloren gaan)
- directe kosten (zoals meldingen, klantenservice, kredietmonitoringsdiensten, maatregelen om klanten over te halen om niet weg te gaan, restitutie en vervanging van passen)
- verlies van klanten ("churn rate") en merk- en reputatieschade

- rechtszaken die worden aangespannen door klanten, zakenpartners en beleggers
- overheidsboetes en -sancties
- kosten van herstel en onderzoek naar de oorzaken (deze vertegenwoordigen meestal het grootste deel van de kosten)
- verlies van activa (zoals intellectueel eigendom)

WAARSCHUWING

Volgens de *National Cyber Security Alliance* gaat 60 procent van de kleine bedrijven die te maken krijgen met een cyberaanval, binnen zes maanden failliet. Als je het niet nodig hebt, of je kunt het niet beveiligen, elimineer het dan, want wat je niet hebt kan niet worden gestolen.

Het actuele panorama van dreigingen analyseren

Het aantal, de omvang en de kosten van datalekken zullen in de nabije toekomst alleen maar toenemen. In deze aanvallen zijn enkele trends te zien die een grote dreiging zullen blijven vormen voor bedrijven van alle groottes:

- **Automatische aanvallen op grote schaal** zijn steeds vaker de modus operandi van cybercriminelen die geavanceerde malware en botnets gebruiken om kwetsbare organisaties en netwerken binnen te dringen. Zij richten zich niet per definitie op bepaalde soorten bedrijven. Als je verbinding maakt met het internet, zullen ze je op een bepaald moment vinden. Niemand is het doelwit, maar iedereen kan het slachtoffer worden.
- **Ransomware** zal een steeds grotere dreiging gaan vormen. Volgens een onderzoek van Datto is ongeveer 5 procent van het mkb wereldwijd het afgelopen jaar het slachtoffer geworden van aanvallen met ransomware. Vijfendertig procent van de managed service providers (MSP's) gaf aan dat kleine bedrijven die het slachtoffer worden van deze praktijken, het losgeld betalen. In 15 procent van de gevallen krijgen zij toch hun data niet terug.
- **Crime-as-a-service (CaaS)** zal toenemen aangezien criminele organisaties hun malware steeds geavanceerder maken. Criminele groepen betreden nieuwe markten en bieden hun diensten wereldwijd aan, wat zal leiden tot meer en schadelijkere cyberveiligheidsincidenten dan ooit. De toegangsbarrières

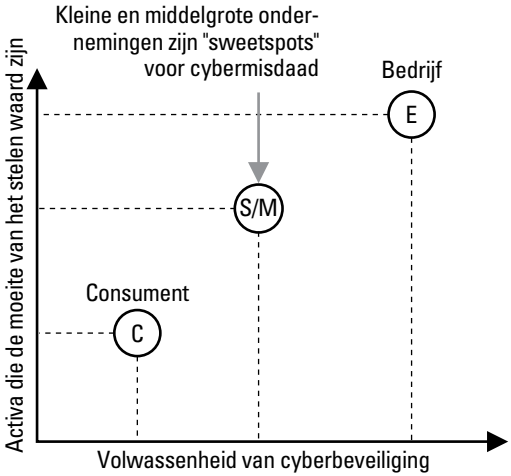
zijn door cyberwapens als "ransomware-as-a-service" en malafide sites ook veel lager, waardoor cybermisdaad veel toegankelijker wordt voor cybercriminelen die minder gespecialiseerd zijn.

- Het **internet der dingen (Internet of Things, IoT)** zal ook meer onbeheerste risico's met zich meebrengen. Organisaties maken gretig gebruik van IoT-apparaten, maar verliezen - in de race naar de markt - vaak uit het oog dat deze apparaten in veel gevallen onveilig zijn ontworpen, waardoor ze allerlei mogelijkheden bieden voor aanvallers. Denk aan CV-ketels, themostaten, televisies, koelkasten, etc.
- **Cloud computing** stelt het mkb in staat te concurreren met de "grote jongens" en kleinere bedrijven hebben nu op grote schaal toegang tot dezelfde krachtige computing-middelen als grote bedrijven, terwijl zij geen grote investeringen doen in IT en dure IT-ondersteuning. Volgens BCSG, een in het VK gevestigd consultancybedrijf dat cloud-oplossingen aanbiedt, gebruikt twee derde van het mkb gemiddeld drie op de cloud gebaseerde software-as-a-service (SaaS)-applicaties. SaaS-applicaties die door het mkb veel worden gebruikt zijn systemen voor customer relationship management (CRM), online samenwerking, gegevensopslag, online marketing, contractbeheer en software voor het beheren van de toeleveringsketen. Deze soorten oplossingen zijn over het algemeen inherent veiliger dan vergelijkbare, lokaal geïnstalleerde varianten. Wel moeten bedrijven nagaan of hun aanbieders van cloud-diensten - met name in kleinere markten of in het geval van zeer exclusieve, kleinschalige SaaS-applicaties - goede praktijken op het gebied van beveiliging toepassen, voldoen aan de relevante regelgeving (zoals de AVG) en acceptabele Service Level Agreements (SLA) aanbieden. Ook in de cloud ligt de uiteindelijke verantwoordelijkheid voor de beveiliging en privacy van gevoelige gegevens en de naleving van regelgeving gewoon bij de kleine en middelgrote bedrijven. Zij moeten daarom zorgen dat ze beschikken over krachtige systemen voor identiteits- en toegangsbeheer, de toegang tot cloud-diensten beveiligen en in de cloud gebaseerde servers op juiste wijze configureren, gebruiken en onderhouden (in het geval van infrastructure-as-a-service of IaaS). Meer informatie over de verschillen tussen SaaS, PaaS en IaaS vind je op pagina 21.
- De **supply chain of leveranciersketen** zal een doelwit blijven en de zwakke plekken van upstream- en downstream-partners, die waardevolle en gevoelige informatie delen, zullen worden

benut om "via de achterdeur" toegang tot bedrijven te krijgen. Vergeet niet dat jouw bedrijf ook deel uitmaakt van de toeleveringsketen van zijn klanten.

- **Wet- en regelgeving** zorgt voor extra complexiteit en bedrijven zullen mogelijk minder aandacht besteden aan en investeren in belangrijke initiatieven op beveiligingsgebied omdat er extra middelen nodig zijn om aan de regelgeving te voldoen (hierop wordt later in dit hoofdstuk ingegaan).

Voor het mkb betekenen deze trends - en het gebrek aan samenhang ertussen - met name slecht nieuws. Omdat kleinere bedrijven over het algemeen niet beschikken over de financiële middelen en informatiebeveiliging van grote bedrijven, vormt het mkb een "sweet spot" voor cybercriminelen (zie figuur 1-1). En het zijn niet alleen cybercriminelen die een ravage aanrichten: veel lekken worden onopzettelijk veroorzaakt door insiders.



FIGUUR 1-1: Kleine en middelgrote bedrijven zijn meestal een waardevoller doelwit dan consumenten en zijn kwetsbaarder dan grote bedrijven.


WAARSCHUWING

Het Information Security Forum (ISF) wijst erop dat de stijging van het aantal datalekken en van de hoeveelheid informatie die met deze lekken is gemoeid, naar verwachting zal leiden tot veel hogere kosten voor alle organisaties, ongeacht hun grootte.

Recente datalekken en -inbreuken

De grootschalige cyberbeveiligingslekken die plaatsvinden bij grote ondernemingen en waarbij gevoelige gegevens in de verkeerde handen komen, krijgen enorm veel aandacht in het nieuws. Maar lekken in het mkb komen niet minder vaak voor en richten zeker zoveel schade aan. Gezien het relatief grote aantal kleine en middelgrote bedrijven en het feit dat zij over veel minder financiële en beveiligingsmiddelen beschikken dan grotere bedrijven, kan de impact van een cyberaanval of datalek voor de klanten van deze bedrijven – en voor het voortbestaan van de bedrijven zelf – veel schadelijker zijn.

BELANGRIJK OM TE ONTHOUDEN

Aan kleine bedrijven (minder dan 50 werknemers) en kleine, vanuit huis gerunde bedrijven wordt in het nieuws nog minder aandacht besteed, maar zij zijn ook zeker niet immuun voor cyberaanvallen en lekken.

Dit zijn een aantal voorbeelden van recente datalekken bij het mkb:

- **Obike:** In december 2017 werd bekend dat Obike, een in Singapore gevestigd bedrijf dat diensten voor het delen van fietsen aanbiedt in verschillende steden in Azië-Pacific, Europa en het VK, in juni 2017 het slachtoffer was geworden van datalekken waarbij gevoelige informatie, waaronder de namen, contactgegevens, profielfoto's en locaties van klanten, in verkeerde handen waren gekomen.
- **TIO Networks USA:** In december 2017 werd gemeld dat TIO Networks USA, een Canadees bedrijf dat betalingen verwerkt en onlangs is overgenomen door PayPal Holding of California, het slachtoffer was geworden van datalekken waardoor persoonlijke en financiële informatie van ongeveer 8.000 klanten van de nutsdiensten van de gemeente Tallahassee (Florida) op straat was komen te liggen.
- **Longs Peak Family Practice:** In november 2017 ontdekte Longs Peak Family Practice, een in Colorado gevestigde medische kliniek, een datalek waardoor de namen, geboortedatums, telefoonnummers, e-mailadressen, socialezekerheidsnummers, rijbewijsnummers, verzekeringsgegevens en andere gevoelige informatie van patiënten mogelijk in verkeerde handen waren gekomen.
- **Royal National Institute of Blind People (RNIB):** In november 2017 werd het Britse RNIB het slachtoffer van een datalek, waarbij gegevens van de credit- en debitcards van 817 klanten

van de online winkel van deze organisatie zonder winstoogmerk werden gestolen.

- **Chilton Medical Center:** In oktober 2017 ontdekte het in New Jersey gevestigde Chilton Medical Center dat een oud-medewerker een harde schijf met de beschermde gezondheidsinformatie van 4.600 patiënten had gestolen.


WAARSCHUWING

Insider threats, oftwel opzettelijk veroorzaakte lekken met informatie, zijn mogelijk een serieuze dreiging voor je onderneming. Volgens het *Data Breach Investigations Report (DBIR)* van Verizon uit 2017 is bij 60 procent van de datalekken sprake geweest van diefstal door insiders.

Omgaan met de veranderende wettelijke en regelgevingskaders

Met de honderden voorschriften die wereldwijd gelden op het gebied van informatiebeveiliging en gegevensbescherming is het voor alle bedrijven, ongeacht hun omvang, een uitdaging om aan alle regels te voldoen. Voorbeelden van deze voorschriften en normen zijn:

- **De Algemene verordening gegevensbescherming van de EU (AVG):** Van toepassing op alle organisaties die zakendoen met EU-burgers. Deze verordening verhoogt de bescherming van de gegevens van EU-burgers en reguleert de export van persoonsgegevens naar landen buiten de EU.
- **Zwitserse Federale wet gegevensbescherming:** Zwitserland heeft zijn Federale wet gegevensbescherming uit 1992 geactualiseerd zodat deze grotendeels in lijn is met de eisen van de AVG. Door deze actualisering wordt de Zwitserse wetgeving inzake gegevensbescherming gemoderniseerd, zodat Zwitserland de door de Europese Commissie toegekende status van toereikendheid kan behouden en gegevens vrij kunnen worden uitgewisseld tussen de EU en Zwitserland. Andere EU-landen actualiseren hun wetgeving inzake gegevensbescherming momenteel ook naar aanleiding van de AVG.
- **Zuid-Afrikaanse Protection of Personal Information (PoPI) Act:** Garandeert dat de Zuid-Afrikaanse instellingen de persoonsgegevens van andere entiteiten op verantwoordelijke wijze verzamelen, verwerken, opslaan en delen en kent personen, als de eigenaars van hun persoonsgegevens, bepaalde rechten met betrekking tot bescherming en controle toe.

- **Amerikaanse Health Insurance Portability and Accountability Act (HIPAA):** Van toepassing op elke organisatie die beschermde gezondheidsinformatie verwerkt of opslaat. Waarborgt de vertrouwelijkheid van patiëntgegevens en gegevensprivacy.
- **Canadese Personal Information Protection and Electronic Documents Act (PIPEDA):** Geldt voor alle organisaties die zakendoen met Canadese burgers. Deze verordening beschermt de privacy en persoonsgegevens van Canadese burgers.
- **27000-serie normen van de Internationale Organisatie voor normalisatie/Internationale Elektrotechnische Commissie (ISO/IEC):** Op internationaal niveau aangenomen normen voor informatiebeveiliging, waaronder: Informatietechnologie – Beveiligingstechnieken – Beheersystemen voor informatiebeveiliging – Vereisten (ISO/IEC 27001), Informatietechnologie – Beveiligingstechnieken – Gedragscode voor het beheer van informatiebeveiliging (ISO/IEC 27002), Informatietechnologie – Beveiligingstechnieken – Gedragscode voor informatiebeveiligingscontroles op basis van ISO/IEC 27002 voor cloud-diensten (ISO/IEC 27017) en Informatietechnologie – Beveiligingstechnieken – Gedragscode voor de bescherming van persoonlijk identificeerbare informatie (PII) in publieke clouds die fungeren als PII-verwerkers (ISO/IEC 27018).
- **Normen van gegevensbescherming voor de betaalkaartenbranche (PCI-DSS):** Van toepassing op alle bedrijven die transacties met passen (zoals creditcards, debetkaarten en betaalkaarten) accepteren, verwerken, en opslaan.

Deze en andere regelgeving is bedoeld om te garanderen dat organisaties die gevoelige gegevens verwerken, passende goede praktijken op het gebied van beveiliging en gegevensbescherming toepassen. De regelgeving is echter vaak erg complex, dubbelzinnig en kostbaar om uit te voeren. Dit heeft onbedoeld tot gevolg dat veel organisaties meer aandacht besteden aan het naleven van de regelgeving dan aan het beschermen van informatie en gegevens.

BELANGRIJK OM TE ONTHOUDEN

Naleving en beveiliging is niet hetzelfde. Een organisatie kan aan de regels voldoen, maar toch niet goed beveiligd zijn. En ook zijn er organisaties die goed beveiligd zijn, maar niet aan de regels voldoen.

VIJF STAPPEN VOOR KLEINE EN MIDDELGROTE ONDERNEMINGEN OM AAN DE AVG TE VOLDOEN

De AVG is ontworpen om de privacy van personen in de EU te beschermen door deze personen meer controle en rechten te geven met betrekking tot hun persoonsgegevens. Personen kunnen bijvoorbeeld:

- van bedrijven eisen dat zij een kopie van hun gegevens verstrekken in een gestructureerd, gebruikelijk en machineleesbaar formaat;
- hun gegevens laten overdragen aan een andere verwerkingsverantwoordelijke (het "recht op gegevensoverdraagbaarheid");
- hun gegevens laten wissen (het "recht om vergeten te worden").

Het AVG bevat veel strengere regels met betrekking tot toestemming, het melden van datalekken, verplichte effectbeoordelingen van de privacy en de vereisten van "privacy door ontwerp" en "privacy door standaardinstellingen".

Als een organisatie de AVG niet naleeft, kan dit resulteren in boetes van tot wel 4 procent van de jaarlijkse wereldwijde omzet van de organisatie of 20 miljoen euro, waarbij de hoogste waarde geldt.

In de AVG wordt ook een aantal technische beveiligingsmaatregelen voorgesteld die kunnen worden toegepast om gegevens te beschermen, zoals:

- de pseudonimisering en versleuteling van persoonsgegevens
- het vermogen om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de systemen en diensten voor de verwerking van persoonsgegeven constant te garanderen
- het vermogen om de beschikbaarheid van en de toegang tot persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident
- een proces voor het regelmatig testen, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen om de beveiliging van de verwerking van persoonsgegevens te garanderen

(vervolgd)

(vervolgd)

Dit zijn vijf stappen die je nu kunt nemen om ervoor te zorgen dat je bedrijf voldoet aan de eisen van de AVG:

- **Stel vast en beoordeel hoe je met data omgaat.** Het is van groot belang dat je volledig begrijpt hoe je organisatie met data omgaat. Onder de oude regels konden alleen verwerkingsverantwoordelijken aansprakelijk worden gehouden voor naleving, maar de verplichtingen uit hoofde van de AVG gelden ook voor gegevensverwerkers. Je moet nagaan of je organisatie een gegevensverwerker of een verwerkingsverantwoordelijke, of beide, is. Het is cruciaal om te weten waar data wordt opgeslagen en hoe die locatie wordt beveiligd. Ook moet worden bepaald welke data wordt gedeeld.
- **Leer van fouten uit het verleden.** Om te beoordelen hoe goed je in staat bent om te reageren op een toekomstige aanval, moet je analyseren wat er bij lekken in het verleden is gebeurd en bepalen of de stappen die toen zijn genomen, voldoen aan de nieuwe eisen van de AVG. Onder de nieuwe regels moeten schendingen binnen 72 uur worden gemeld, in combinatie met informatie over de ernst van de aanval. Als je bedrijf hiertoe niet in staat is, kan dat tot hoge boetes leiden. Het actualiseren (of opstellen) van je responsplan voor incidenten en het regelmatig testen van je capaciteit om op incidenten te reageren en van de effectiviteit waarmee dit gebeurt, is een kritieke stap om te kunnen voldoen aan de eisen van de AVG.
- **Benoem een functionaris voor gegevensbescherming of iemand die formeel verantwoordelijk is voor gegevensbescherming.** Dit is misschien een eenvoudig advies voor een bedrijf met veel geld, maar de kosten die ermee zijn gemoeid kunnen er voor kleinere bedrijven nogal inhakken. Toch is het minder duur dan een boete van 4 procent van je omzet en misschien heb je geen fulltime-medewerker nodig. De functionaris voor gegevensbescherming is onafhankelijk en moet helpen met de uitvoering van de vereisten door te rapporteren aan het hoogste managementniveau. Door hier zo snel mogelijk budget voor beschikbaar te stellen garandeer je niet alleen dat je bedrijf aan de regels voldoet, maar ben je ook beter voorbereid op eventuele datalekken en kun je de kans verkleinen dat je bedrijf een boete krijgt.

- **Zorg ervoor dat je personeel weet welke regels gelden - en jij ook.** Een van de belangrijkste doelen van de AVG is het gemakkelijker te maken voor mensen om te eisen dat zij "worden vergeten" en dat hun gegevens worden gewist. Bedrijven moeten expliciete toestemming krijgen van personen voordat ze hun gegevens mogen verwerken. De regels maken het ook lastiger voor kinderen om hun gegevens te verstrekken. Het is van groot belang te weten hoe deze regels de manier veranderen waarop jouw organisatie omgaat met goedkeuringen en de rechten van personen.
- **Weet welke autoriteit toezicht op je houdt.** Het hangt af van de locatie van je bedrijf, en niet van de locatie van de persoon die de klacht indient, welke autoriteit klachten tegen jouw bedrijf zal afhandelen. Dit kan lastig zijn voor bedrijven die internationaal actief zijn of verschillende locaties in meerdere regio's hebben. Er zijn ook richtlijnen in andere landen die mogelijk verder gaan dan de AVG en waar ook rekening mee moet worden gehouden.

Ga, om meer te weten te komen over de AVG en de beveiligingsmaatregelen die je bedrijf kan nemen om eraan te voldoen, naar `https://encryption.eset.com/int/`.

IN DIT HOOFDSTUK

- **Bekend raken met de grondbeginselen van gegevensbescherming**
- **Technologie toepassen in de cloud en op locatie**
- **De mogelijkheid van managed services en outsourcing**

Hoofdstuk 2
Aan de slag met gegevensbescherming

In dit hoofdstuk kom je te weten wat de grondbeginselen van de technologie voor gegevensbescherming zijn, vergelijken we verschillende opties voor de toepassing van deze technologie in de cloud en op locatie en bespreken we de beveiligingsdiensten die worden aangeboden door "managed service providers" en de mogelijkheid van outsourcing.

De grondbeginselen van gegevensbescherming begrijpen

Het garanderen van de beveiliging en privacy van gevoelige klantinformatie is een belangrijke verantwoordelijkheid van alle bedrijven, ook van het mkb.

Gegevensbescherming (en in meer algemene zin, informatiebeveiliging) behelst alle administratieve, logische en technische controles die noodzakelijk zijn om informatie te beschermen. De V-I-B-driehoek (zie figuur 2-1) wordt vaak gebruikt als leidraad voor de ontwikkeling en invoering van een kader voor het beheren van informatiebeveiliging binnen een organisatie. De V-I-B-driehoek bestaat uit drie fundamentele concepten van informatiebeveiliging:

FIGUUR 2-1: De V-I-B-driehoek.

- **vertrouwelijkheid (en privacy):** het voorkomen dat gegevens zonder toestemming worden geraadpleegd, gebruikt, vrijgegeven, ingezien, geïnspecteerd of opgenomen;
- **integriteit:** het voorkomen dat gegevens zonder toestemming of op onjuiste wijze worden gewijzigd of worden vernietigd.
- **beschikbaarheid:** garanderen dat bevoegde gebruikers betrouwbare en tijdige toegang hebben tot gegevens.

Om de vertrouwelijkheid van gevoelige gegevens te beschermen, wordt over het algemeen in divers beleid op het gebied van arbeid, beveiliging en privacy bepaald wie binnen een organisatie toegang heeft tot bepaalde gegevens en voor welke doeleinden, en wat zij mogen doen met deze gegevens. Voorbeelden van technische controles om de vertrouwelijkheid te garanderen zijn het beheer van identiteit en toegang, versleuteling en oplossingen om het verlies van gegevens te voorkomen.

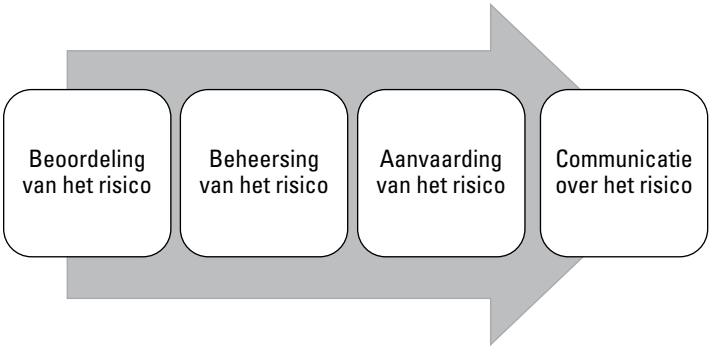
Om de integriteit van gegevens te beschermen, kunnen diverse technische oplossingen worden toegepast, zoals checksums en validatie van de gegevensinvoer in formulieren en databases. Bij digitale handtekeningen en hashing worden versleutelingstechnologieën gebruikt om de authenticiteit van gegevens te verifiëren en na te gaan of de gegevens niet zijn gewijzigd. Ten slotte beschermen anti-malware-oplossingen de integriteit van gegevens (en in veel gevallen ook de vertrouwelijkheid en beschikbaarheid).

Om de beschikbaarheid van gegevens te beschermen en te voorkomen dat ze per ongeluk (bijvoorbeeld door wissen) of met opzet (bijvoorbeeld in een ransomware-aanval) worden vernietigd, worden back-up- en herstelsystemen en back-up- en retentiebeleid ingevoerd. Technologieën voor gegevensbescherming worden in hoofdstuk 4 verder besproken.

Om informatie effectief te beschermen, moeten bedrijven iets doen om de vertrouwelijkheid, integriteit en beschikbaarheid van al hun gevoelige gegevens te garanderen, en ook van de systemen en toepassingen voor het verwerken en opslaan van die gegevens.

Door een op risico gebaseerde aanpak te gebruiken, kunnen organisaties de controles invoeren die nodig zijn om iets te doen aan kwetsbaarheden en een aanvaardbaar risiconiveau bereiken voor hun gegevens met het oog op specifieke dreigingen. Hoe groter het risico dat met de gegevens is gemoeid, hoe meer en vooral beter beschermende maatregelen moeten worden ingevoerd.

Bij de beheersing van beveiligingsrisico's worden vier belangrijke fases doorlopen (zie figuur 2-2):



FIGUUR 2-2: Een basisproces voor het beheersen van risico's.

- **Beoordeling van het risico:** Er zijn diverse methoden om risico's te beoordelen, elk met een eigen kostenplaatje en niveau van complexiteit. Het proces bestaat in grote lijnen uit de volgende stappen:
  - *Identificatie van de activa:* Identificeer alle activa van de organisatie (zowel materiële als immateriële) die moeten worden beschermd en bepaal wat de kwantitatieve waarde

(bijv. kostprijs of bijdrage aan de omzet) en de kwalitatieve waarde (bijv. relatief belang) van elk van die activa is.

- *Analyse van de bedreigingen:* Bepaal welke negatieve door de natuur en/of door de mens veroorzaakte omstandigheden of gebeurtenissen zich kunnen voordoen, wat hiervan de effecten of consequenties kunnen zijn, hoe groot de kans is dat dit gebeurt en hoe regelmatig het zal gebeuren.
- *Beoordeling van kwetsbaarheid:* Bepaal welke waarborgen en/of controlemechanismen voor een bepaald systeem ontbreken of zwak zijn, waardoor een eventuele bedreiging schadelijker, kostbaarder, waarschijnlijker en frequenter kan worden.

- **Beheersing van het risico:** De risicobeoordeling vormt de basis voor beslissingen van het management over wat er gedaan moet worden aan specifieke risico's. Voorbeelden van maatregelen zijn:
  - *het risico afzwakken:* beleid, controles en/of andere maatregelen invoeren om de impact van een bedreiging voor een bepaald systeem te verminderen of de kans dat de situatie zich daadwerkelijk voordoet te verkleinen;
  - *het risico overdragen (of transfereren):* het risico overdragen aan een derde partij, bijvoorbeeld een verzekeringsmaatschappij, een dienstverlener of een andere persoon of instantie die er expliciet mee akkoord gaat het risico te aanvaarden;
  - *het risico voorkomen:* het risico helemaal wegnemen, bijvoorbeeld door het systeem te upgraden of weg te doen of door de activiteit te staken die het risico creëert.
- **Acceptatie van restrisico:** Dit is het moment waarop het management zijn formele goedkeuring geeft voor de maatregelen die zijn getroffen om het risico te beheersen en de eventuele restrisico's (overblijvende risico's) aanvaardt die vanuit praktisch oogpunt niet (verder) kunnen worden beheerst.
- **Communicatie over het risico:** Relevante belanghebbenden moeten worden geïnformeerd over de manieren waarop risico wordt beheerd en/of over beslissingen om bepaalde risico's te aanvaarden. Ook moeten zij weten wat hun individuele rol en verantwoordelijkheden met betrekking tot specifieke risico's zijn.

Implementatie-opties vergelijken: lokaal, in de cloud of hybride

Bedrijven hebben vandaag de dag wat betreft de implementatie van software veel meer mogelijkheden, waaronder lokale implementatie, implementatie in de cloud en een hybride oplossing waarbij sommige middelen op locatie bij het bedrijf en andere in de cloud worden geplaatst.

Niet zo heel lang geleden moest alle technologie nog op locatie bij bedrijven worden geïnstalleerd. Zelfs de kleinste bedrijven zagen zich genoodzaakt een aantal dure servers aan te schaffen, die vaak onder verre van ideale omstandigheden werden geïnstalleerd in een donkere, krappe kast ergens in het gebouw (in sommige gevallen met een sprinklerinstallatie aan het plafond die een groter risico voor de dure IT-investeringen vormde dan een mogelijke brand). Deze servers vereisten constant beheer en onderhoud, waarvoor vaak extra IT-personeel en extern beheer nodig waren. Naast de servers moest er ook netwerkapparatuur zoals routers, switches en netwerkkabels worden geïnstalleerd en beheerd. En er was ten minste een firewall nodig om het "betrouwbare" interne netwerk te beschermen tegen het "onbetrouwbare" internet.

Voor veel bedrijven is een serverruimte of datacenter in het gebouw nog steeds een aantrekkelijke optie. Maar aangezien virtualisatie, netwerkconnectiviteit en technologieën voor cloud computing het afgelopen decennium zoveel robuuster en stabieler zijn geworden, verhuizen veel bedrijven hun IT-middelen nu geheel of gedeeltelijk naar de cloud.

Maar wat is de cloud nu eigenlijk precies? Praktisch elke technologie-aanbieder op de markt biedt wel iets aan dat met de cloud te maken heeft. Maar wat die cloud nu precies inhoudt, is helaas niet altijd even duidelijk. Laten we daarom meer duidelijkheid scheppen in de hele cloud-trend en een paar belangrijke elementen van de cloud definiëren aan de hand van de definities van het Amerikaanse National Institute of Standards and Technology (Nationaal Instituut voor Normen en Technologie, NIST). Volgens het NIST kunnen de servicemodellen voor cloud computing in de volgende drie categorieën worden onderverdeeld:

- **Software as a Service (SaaS):** Klanten krijgen toegang tot een applicatie die zich op infrastructuur in de cloud bevindt. De applicatie is toegankelijk via verschillende apparaten en interfaces van

de klant, maar de klant heeft geen kennis van de onderliggende cloud-infrastructuur en beheert of controleert deze ook niet. De klant zal waarschijnlijk toegang hebben tot beperkte, gebruiker-specifieke applicatie-instellingen en de beveiliging van de gegevens van de klant blijft de verantwoordelijkheid van de klant.

- **Platform as a Service (PaaS):** De klant kan ondersteunde applicaties gebruiken op de cloud-infrastructuur van de aanbieder, maar de klant heeft geen kennis van de onderliggende cloud-infrastructuur en beheert of controleert deze ook niet. De klant heeft controle over de applicaties die worden gebruikt en over een beperkt aantal configuratie-instellingen voor de omgeving waarin de applicaties worden gehost. De klant is de eigenaar van de gebruikte applicaties en gegevens en is daarom verantwoordelijk voor hun beveiliging.
- **Infrastructure as a Service (IaaS):** Klanten kunnen middelen voor het verwerken en opslaan van gegevens, netwerken en andere computing-middelen verschaffen en besturingssystemen en applicaties installeren en gebruiken, maar de klant heeft geen kennis van de onderliggende cloud-infrastructuur en beheert of controleert deze ook niet. De klant heeft controle over het besturingssysteem, de opslag en de gebruikte applicaties en ook over de netwerkcomponenten. De klant is de eigenaar van de gebruikte applicaties en gegevens en is daarom verantwoordelijk voor hun beveiliging.

TIP

De verschillende modaliteiten waarin cloud-diensten worden aangeboden (SaaS, PaaS en IaaS) hebben verschillende implicaties voor klanten wat beveiliging betreft. Zo bieden SaaS-producten als Microsoft 365 en Salesforce infrastructuurbeveiliging via de cloud-aanbieder, maar zijn gegevensbeveiliging en authenticatie de verantwoordelijkheid van de klant. De verantwoordelijkheden van de klant op het gebied van beveiliging nemen progressief toe bij PaaS- en IaaS-modellen. Bij veel cloud-oplossingen verschuift de nadruk van applicaties en infrastructuur naar authenticatie en beveiliging van de gegevensintegriteit.

NIST deelt de implementatiemodellen voor cloud computing in vier groepen in:

- **Openbaar:** Een cloud-infrastructuur die door iedereen kan worden gebruikt. Deze infrastructuur is eigendom van en wordt beheerd en geëxploiteerd door een of meerdere derden en is fysiek aanwezig op de locatie van de cloud-aanbieder.

- **Particulier:** Een cloud-infrastructuur die exclusief wordt gebruikt door één organisatie. Deze infrastructuur kan het eigendom zijn en worden beheerd en geëxploiteerd door de organisatie of een derde partij (of een combinatie van beide) en kan al dan niet op de locatie van de organisatie staan.
- **Hybride:** Een cloud-infrastructuur die bestaat uit twee of meer van de andere implementatiemodellen, samengevoegd door middel van gestandaardiseerde of bedrijfseigen technologie die gegevens- en applicatieoverdracht mogelijk maakt.
- **Gemeenschappelijk (komt niet veel voor):** Een cloud-infrastructuur die exclusief wordt gebruikt door een specifieke groep van organisaties.

Het proces om een cloud op te zetten begint, net zoals bij veel nieuwe initiatieven het geval is, bij applicaties en systemen die niet productiegerelateerd of kritiek zijn, bijvoorbeeld bij de ontwikkelomgeving of de back-up-systemen. Later in het proces beginnen veel bedrijven bestaande applicaties naar de cloud te verplaatsen en passen zij nieuwe applicaties direct in de cloud toe. Ten slotte spannen "cloud first"-organisaties zich in om zo veel mogelijk van hun IT-omgeving in de cloud te zetten en "cloud native" applicaties voor hun klanten te ontwikkelen.

De cloud biedt bedrijven allerlei voordelen, waaronder:

- **Meer flexibiliteit en sneller reageren:** Je kunt applicaties en gegevens in de cloud overal, altijd, vanaf elk apparaat raadplegen.
- **Kortere time-to-market:** Je kunt nieuwe producten en diensten in de cloud sneller ontwikkelen en lanceren met PaaS of gemakkelijk toegankelijke IaaS-middelen.
- **Schaalbaarheid "on demand":** Wanneer dat nodig is, kunnen aanvullende softwarelicenties en/of infrastructuur worden toegevoegd en weer worden verwijderd, wat gunstig is voor bedrijven die snel groeien of zeer seizoensgebonden zijn en die het lastig vinden veranderingen in de markt of de groei nauwkeurig te voorspellen.
- **Meer stabiliteit:** Cloud-infrastructuur wordt meestal geïnstalleerd in robuuste datacenters die door grote teams van gespecialiseerd IT-personeel worden gebouwd om optimale prestaties, stabiliteit en betrouwbaarheid te leveren.
- **Minder investeringen in kapitaal:** Je kunt je hele IT-infrastructuur in de cloud zetten en zo kostbare

kapitaalinvesteringen vermijden. De cloud biedt voorspelbare "pay as you go"-abonnementsdiensten, zodat je de behoeften op IT-gebied kunt begroten als lopende bedrijfskosten en alleen betaalt voor wat je daadwerkelijk gebruikt.

WAARSCHUWING

Als je toepassingen en gegevens naar de cloud verhuist, wil dat niet zeggen dat je niet meer verantwoordelijk bent voor de beveiliging van je applicaties en gegevens. De cloud-aanbieder is verantwoordelijk voor bepaalde aspecten van de omgeving, maar de uiteindelijke verantwoordelijkheid voor de bescherming en beveiliging van applicaties en data ligt bij jou. Aanbieders van cloud-diensten verwijzen vaak naar een "model van gedeelde verantwoordelijkheid", waarin duidelijk wordt aangegeven waarvoor zij in de cloud verantwoordelijk zijn en waarvoor jij verantwoordelijk bent. En in geen enkel model is te zien dat de aanbieder van cloud-diensten verantwoordelijk is voor de beveiliging van jouw gegevens! Let er daarom goed op hoe de verantwoordelijkheden zijn verdeeld zodra je migreert naar de cloud.

De mogelijkheid van managed services voor beveiliging en outsourcing

Het is, nu de risico's en dreigingen steeds groter worden, een steeds grotere last en uitdaging voor bedrijven van alle groottes om hun IT-systemen en applicaties veilig, beschermd en conform de regels te houden. Dit geldt met name voor het mkb, aangezien deze bedrijven minder IT-personeel en beveiligingsmiddelen hebben. Veel kleine en middelgrote bedrijven maken daarom gebruik van managed service providers (MSP). De voordelen en waarde van een MSP voor het mkb zijn onder andere:

- **Meer controle over het IT-budget:** MSP's kunnen een veel breder portfolio van producten en diensten aanbieden dan de producten en diensten waarover kleine en middelgrote bedrijven intern beschikken. Als gebruik wordt gemaakt van de diensten van een MSP, is de financiële flexibiliteit ook groter en kunnen de kosten beter worden voorspeld. Dankzij de flexibele abonnementen kunnen kleine en middelgrote bedrijven hun IT- en beveiligingsbudget ook beter beheersen.
- **Een betrouwbare adviseur met kennis en ervaring:** Het mkb kan profiteren van de grote kennis en brede ervaring van het IT- en beveiligingspersoneel dat door MSP's wordt ingezet.

- **Kennis van de ontwikkelingen op de markt:** MSP's die zich bezighouden met beveiliging hebben meer inzicht in de beveiligingsoplossingen die op de markt verkrijgbaar zijn en kunnen hun klanten op maat gemaakte oplossingen aanbieden.
- **Innovatie:** De gespecialiseerde beveiligingsteams van MSP's kunnen gemakkelijker innovatieve oplossingen ontwikkelen, aannemen en invoeren en klanten helpen de huidige ontwikkelingen op de markt bij te benen.
- **Goed voorbereid op veranderingen:** MSP's bieden klanten de mogelijkheid software en hardware toe te voegen en te verwijderen op basis van hun actuele behoeften, zodat ze daarvoor geen nieuwe hardware en software hoeven aan te schaffen, in te voeren en te onderhouden, een proces dat nogal wat voeten in de aarde heeft.

DE VOLKSBANK

De Volksbank is een Nederlandse, zelfstandige bankholding met vier onderscheidende banken: SNS, ASN Bank, BLG Wonen en RegioBank. Elk van deze labels heeft een eigen positionering en geeft een passende invulling aan de behoeften van zijn klantengroep.

Uitdagingen

De afgelopen jaren gebruikte de Volksbank een securityoplossing van een andere vendor. Deze oplossing verschoof de laatste jaren steeds meer naar een cloud-only dienstverlening – waarbij de Volksbank gedwongen was mee te bewegen. Doordat het binnen de bestaande oplossing niet mogelijk was de infrastructuur naar wens in te richten, volgde de conclusie dat de toenmalige securityoplossingen vervangen moesten worden.

Oplossing

Middels een intern traject heeft de Volksbank haar wensen en behoeften omtrent IT-security in kaart gebracht en hebben zij verschillende aanbieders van securityoplossingen geëvalueerd. Om in contact te komen met aanbieders bezocht de Volksbank verschillende beurzen en events, waaronder de Infosecurity beurs. Hier kwamen zij voor het eerst in contact met ESET. Op de beurs hebben ESET en de Volksbank

(vervolgd)

(vervolgd)

samen een lijst met requirements doorgenomen en gekeken of de oplossingen van ESET voldoen aan de wensen en eisen die de Volksbank stelt aan een securityoplossing.

Resultaten

- De Volksbank is zeer tevreden met de samenwerking. Met name op het gebied van malwaredetectie ziet de Volksbank een positieve verandering. De Volksbank heeft regelmatig te maken met custom malware — deze filtert ESET nu in een eerder stadium zonder extra tools.
- ESET en de Volksbank zijn inmiddels uitgegroeid tot betrouwbare business partners. Doordat ze na de implementatie van de securityoplossingen nauw zijn blijven samenwerken, groeit de Volksbank met ESET mee door continu nieuwe securityoplossingen te testen en te implementeren.

ESET draagt hiervoor constant ideeën aan die een positieve bijdrage leveren voor de Volksbank. Een voorbeeld hiervan is de oplossing ESET Threat Intelligence, die de Volksbank in staat stelt phishing mails beter en sneller te onderzoeken. Ook kunnen zij custom malware via ESET Threat Intelligence doorzetten naar het hoofdkantoor van ESET voor opname in de malware definities.

IN DIT HOOFDSTUK

- **Het proces van risicobeoordeling begrijpen**
- **Gegevensverwerkingsoperaties identificeren**
- **De impact van een datalek bepalen**
- **Pertinente dreigingen op het gebied van gegevensbeveiliging identificeren**
- **Passende gegevensbeschermingscontroles invoeren**

Hoofdstuk 3
Risico's met betrekking tot gegevensbeveiliging beoordelen

In dit hoofdstuk leer je hoe je risicobeheerprocessen (die werden besproken in hoofdstuk 2) kan toepassen op gegevensbeveiliging.

Het proces van risicobeoordeling begrijpen

De beoordeling van de risico's vormt de eerste stap in het proces van risicobeheer (zoals besproken in hoofdstuk 2). Een risicobeoordeling bestaat uit de volgende stappen:

- je activa (zowel de materiële als de immateriële) identificeren
- de dreigingen (waaronder hun impact en waarschijnlijkheid) analyseren
- de kwetsbaarheden beoordelen (ofwel: welke waarborgen of controles ontbreken of zijn ontoereikend voor een bepaald activa?)

Bij de beoordeling van de risico's op het gebied van gegevensbeveiliging worden vergelijkbare fases doorlopen:

- je gegevensverwerkingsoperaties identificeren (om te bepalen hoe en waar jouw bedrijf gebruikmaakt van zijn gegevens)
- de potentiële impact op het bedrijf bepalen (als gegevens in verkeerde handen vallen)
- de potentiële dreigingen bepalen en evalueren hoe waarschijnlijk het is dat deze zich voordoen (en hoe regelmatig)
- het risico evalueren (om te beoordelen welke waarborgen en controles moeten worden ingevoerd om je gegevens te beschermen)

Stap 1: Je gegevensverwerkingsoperaties identificeren

De gegevens binnen je organisatie hebben verschillende risicoprofielen. Deze profielen zijn niet alleen afhankelijk van de inhoud van de gegevens, maar ook van de manier waarop ze worden gebruikt binnen de organisatie. Het is daarom belangrijk om bij aanvang van het risicobeoordelingsproces te weten hoe gegevens binnen je bedrijf worden verwerkt. De meeste kleine en middelgrote ondernemingen voeren gegevensverwerkingsoperaties uit op enkele of alle van de volgende gebieden:

- **personeelszaken** zoals salarisadministratie, werving en selectie, opleidingsdossiers, disciplinaire maatregelen en functioneringsgesprekken;
- **klantenbeheer, marketing en leveranciers** zoals klantinformatie, aankoop- en verkooporders, facturen, e-maillijsten, gegevens voor marketing- en reclamedoeleinden en contracten met leveranciers;
- **(fysieke) veiligheid van personen** zoals logboeken waarin de aanwezigheid van medewerkers wordt geregistreerd voor beveiligingsdoeleinden, bezoekerslijsten en videobewaking.

Beantwoord voor elke gegevensverwerkingsoperatie de volgende vragen:

- Welke persoonsgegevens worden verwerkt?
- Wat is het doeleinde van het proces?
- Waar vindt de verwerking plaats?
- Wie is verantwoordelijk voor het proces?
- Wie heeft toegang tot de gegevens?

BELANGRIJK OM TE ONTHOUDEN

Het *least privilege*-beginsel wordt beschouwd als een goede werkwijze op het gebied van informatiebeveiliging en houdt in dat alleen rechten worden toegekend die strikt noodzakelijk zijn voor de uitvoering van een specifieke functie.

Stap 2: De potentiële impact op het bedrijf bepalen

Vervolgens moet je bepalen wat de potentiële impact is van een datalek of -inbreuk. Een inbreuk of lek kan afbreuk doen aan de vertrouwelijkheid van gegevens (in het geval van bijv. onbevoegde toegang), de integriteit van gegevens (bijvoorbeeld bij onbevoegde wijziging) of de beschikbaarheid van gegevens (bijvoorbeeld bij een ransomware-aanval).

BELANGRIJK OM TE ONTHOUDEN

Organisaties moeten de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens waarborgen. In de informatiebeveiliging wordt dit de V-I-B-driehoek genoemd.

Bij een typische risicobeoordeling wordt de potentiële impact van een bepaald risico meestal uitgedrukt in termen van schade voor de organisatie, bijvoorbeeld het verlies of de vernietiging van materiële activa (zoals servers, kopieerapparaten of voertuigen).

De impact die een gegevensbeveiligingsrisico heeft op een bedrijf is vergelijkbaar met de impact van andere soorten risico's, met als verschil dat deze impact ook indirect kan zijn. In het geval van gevoelige persoonsgegevens is het directe slachtoffer de persoon van wie de gegevens zijn gelekt of in de verkeerde handen terecht zijn gekomen. In die gevallen kan de identiteit of een financieel actief van de persoon zijn gestolen of kan zijn of haar privacy zijn geschonden. De impact op het bedrijf is minder direct, maar kan toch grote kosten met zich meebrengen in de vorm van (onder andere):

- verlies van klanten en inkomsten
- merk- en reputatieschade en negatieve publiciteit
- overheidsboetes en rechtszaken
- meldingen van lekken en kredietmonitoringsdiensten
- onderzoek naar de oorzaken en herstel

TIP

De impact op het bedrijf kan worden aangemerkt als laag, gemiddeld of hoog. Elk bedrijf zal deze impactniveaus echter op unieke wijze definiëren, waarbij zowel objectieve (kwantitatieve) als subjectieve (kwalitatieve) maatstaven in acht moeten worden genomen.

Stap 3: Mogelijke dreigingen identificeren en hun waarschijnlijkheid evalueren

Dreigingen zijn gebeurtenissen of omstandigheden, door de natuur of door de mens veroorzaakt, die negatieve gevolgen kunnen hebben voor de betrouwbaarheid, integriteit of beschikbaarheid van persoonsgegevens of gevoelige gegevens. Je kunt hierbij onder andere denken aan cyberaanvallen, accidenteel verlies of accidentele vrijgave, dreigingen van binnenuit, brand en overstromingen, aardbevingen en tsunami's, extreme weersomstandigheden (zoals orkanen of tornado's), civiele onrust, arbeidsgeschillen enz. Bedrijven moeten bepalen wat de potentiële dreigingen zijn voor hun gegevensverwerkingsoperaties en evalueren hoe waarschijnlijk het is dat elke dreiging zich voordoet (en hoe regelmatig). Zorg ervoor dat je geen dreigingen vergeet op belangrijke gebieden, bijvoorbeeld degene die verband houden met de netwerk- en technische middelen (software/hardware) die worden gebruikt voor de verwerking van gegevens, verwante processen en procedures, personele middelen en de schaal van de verwerking.


TIP

Voor elke geïdentificeerde dreiging kan je de waarschijnlijkheid indelen in dezelfde categorieën die je hebt gebruikt voor de impact op het bedrijf: laag, gemiddeld of hoog. Houd bij het evalueren van de waarschijnlijkheid van een dreiging rekening met twee aspecten: de waarschijnlijkheid dat de dreiging zich voordoet en de frequentie waarmee de dreiging zich waarschijnlijk zal voordoen in een bepaalde periode (bijvoorbeeld in een jaar).

Stap 4: Risico evalueren

Zodra je al je gegevensverwerkingsoperaties (en de gegevens die worden verwerkt) hebt geïdentificeerd, de potentiële impact hebt bepaald van een datalek of -inbreuk en de mogelijke dreigingen en hun waarschijnlijkheid en frequentie hebt vastgesteld, kun je het risico evalueren dat gemoeid is met elke operatie en bepalen welke technologische controles (deze worden besproken in hoofdstuk 4) en organisatorische processen je moet invoeren om je gegevens te beschermen. Naar aanleiding van de risicoevaluatie moeten organisatorische en procesmatige controles (deze worden besproken in hoofdstuk 5) worden ingevoerd om je gegevens en gegevensverwerkingsoperaties naar behoren te beveiligen aan de hand van een op risico's gebaseerde benadering.

In figuur 3-1 is een sjabloon voor de beoordeling van gegevens opgenomen als voorbeeld van een beoordeling van gegevensverwerkingsoperaties.

Risicobeoordelingsmatrix voor gegevensverwerkingsoperaties				Impactniveau			
				Evalueer voor specifieke gegevensverwerkingsoperaties de mogelijke impact op de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens (V-I-B-driehoek). De hoogste impact van de drie bepaalt het uiteindelijke impactniveau			
				Laag	**Gemiddeld**	**Hoog**	**Zeer hoog**
				kleine ongemakken die probleemloos kunnen worden verholpen	aanzienlijke ongemakken die met enige moeite kunnen worden verholpen	aanzienlijke consequenties die het bedrijf te boven kan komen, maar wat grote moeite zal kosten	aanzienlijke of zelfs onomkeerbare consequenties die het bedrijf mogelijk niet te boven zal komen
Waarschijnlijkheid van de dreiging	Loop voor specifieke gegevensverwerkingsoperaties een lijst met mogelijke dreigingen door en evalueer/beoordeel de waarschijnlijkheid van de dreigingen. De uiteindelijke waarschijnlijkheid moet zijn gebaseerd op de som van de score van alle dreigingen in de lijst.	**Laag**	het is onwaarschijnlijk dat de dreiging zich daadwerkelijk voordoet	de gegevensverwerkingsoperatie vertoont een **Laag risico**	de gegevensverwerkingsoperatie vertoont een **Laag risico**	de gegevensverwerkingsoperatie vertoont een **Hoog risico**	
		Gemiddeld	het is redelijk waarschijnlijk dat de dreiging zich daadwerkelijk voordoet				
		Hoog	het is waarschijnlijk dat de dreiging zich daadwerkelijk voordoet	**Laag risico**			

FIGUUR 3-1: Matrix voor risicobeoordeling.

				Impactniveau			
Voorbeeld **Gegevensverwerkingsoperatie: Marketing/reclame** **Verwerkte gegevens:** Contactinformatie (bijv. naam, postadres, telefoonnummer, e-mail) **Gegevensclassificatie:** Persoonsgegevens **Doeleinde van de verwerking:** Promotie van goederen en speciale aanbiedingen aan potentiële klanten **Datasubjecten:** Klanten en potentiële klanten				Impactbeoordeling vertrouwelijkheid: laag, integriteit: laag, beschikbaarheid: laag. **Uiteindelijk impactniveau: Laag**			
				Laag	**Gemiddeld**	**Hoog**	**Zeer hoog**
				kleine ongemakken die probleemloos kunnen worden verholpen	aanzienlijke ongemakken die met enige moeite kunnen worden verholpen	aanzienlijke consequenties die het bedrijf te boven kan komen, maar wat grote moeite zal kosten	aanzienlijke of zelfs onomkeerbare consequenties die het bedrijf mogelijk niet te boven zal komen
Waarschijnlijkheid van de dreiging	Dreigingen voor netwerken en technische middelen: Gemiddeld dreigingen met betrekking tot processen en procedures: Laag dreigingen op het gebied van personeelszaken: Gemiddeld Dreigingen met betrekking tot branche en schaal van verwerking: Gemiddeld **Uiteindelijke waarschijnlijkheid: Gemiddeld**	**Laag**	het is onwaarschijnlijk dat de dreiging zich daadwerkelijk voordoet				
		Gemiddeld	het is redelijk waarschijnlijk dat de dreiging zich daadwerkelijk voordoet	**X – Laag risico** verwerking van marketing-/ reclamegegevens vormt een laag risico - Er moeten technische en organisatorische maatregelen worden ingevoerd die adequaat zijn voor dit risico.			
		Hoog	het is waarschijnlijk dat de dreiging zich daadwerkelijk voordoet				

FIGUUR 3-1: *(continued)*.

IN DIT HOOFDSTUK

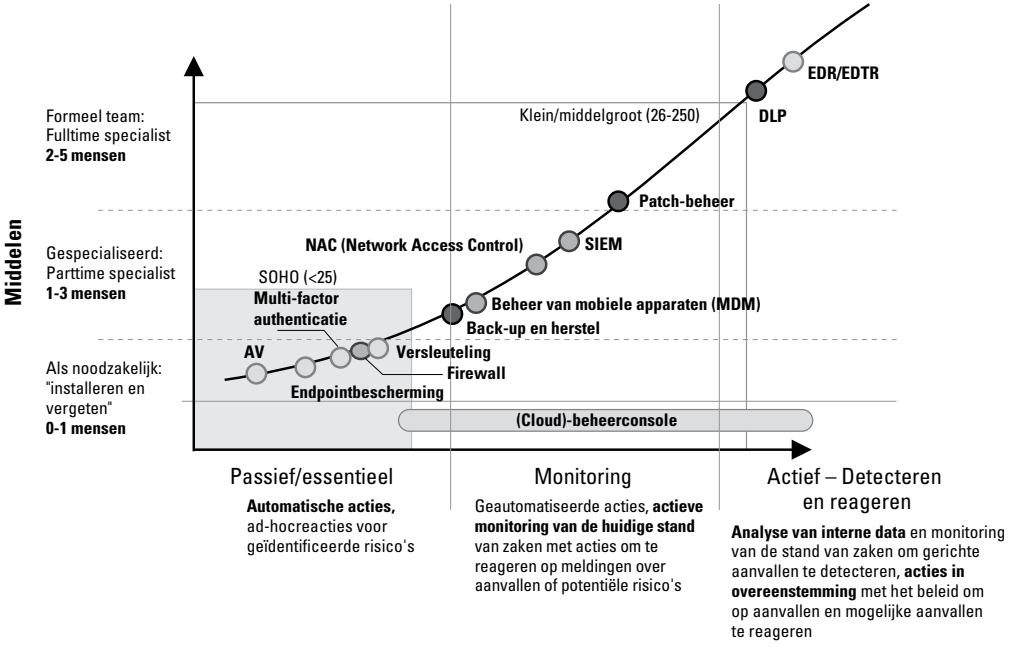
- **Oplossingen voor gegevensbescherming evalueren**
- **Het netwerk beveiligen**
- **Het aantal fouten verminderen en de efficiëntie verhogen door middel van orkestratie**

Hoofdstuk 4
Technologie voor gegevensbescherming begrijpen

In dit hoofdstuk kom je meer te weten over de verschillende technologieën voor informatiebeveiliging en gegevensbescherming die je kunt overwegen te implementeren in jouw bedrijf, van het endpoint tot het netwerk en verder.

Gegevens beschermen, overal

Gegevens zijn een kritieke activa van je bedrijf, maar kunnen ook een enorm risico vormen. Er zijn heel veel beveiligingstechnologieën die je kunt gebruiken om de gegevens in je werkruimtes (zoals computers en mobiele apparaten), op je netwerk en aan de back-end (bijvoorbeeld in de lokale serverruimte of je datacenter in de cloud) te beveiligen. In figuur 4-1 worden verschillende beveiligingstechnologieën weergegeven die je kunt overwegen toe te passen in jouw bedrijf als ze aansluiten op het risiconiveau en de beschikbare middelen (hieronder worden deze technologieën besproken).



FIGUUR 4-1: Beveiligingstechnologieën

Naast antivirussoftware (AV-software) moeten kleine en middelgrote bedrijven de volgende beveiliging overwegen:

- **Endpoint security:** Endpoint security gaat verder dan antivirussoftware en is een meerlaagse technologie die infecties met malware (waaronder virussen, wormen, ransomware, spyware, Trojans en remote access Trojans en rootkits/bootkits), misbruik van zwakke plekken, netwerkaanvallen, botnet-infiltratie enz. voorkomt (zie in de marge "Endpoint security kiezen").
- **Multifactorauthenticatie (MFA):** MFA vormt een verbetering ten opzichte van gewone authenticatie (op basis van bijvoorbeeld een gebruikersnaam en een wachtwoord) door een aanvullende factor te eisen bij het inloggen in een systeem of applicatie. Dit is meestal een eenmalige code die wordt verstuurd naar een van tevoren ingesteld, afzonderlijk e-mailadres, smartphone app of via een tekstbericht naar een smartphone. De code kan alleen worden gebruikt om gedurende een beperkte periode (bijvoorbeeld 60 seconden) één enkele sessie van de gebruiker te authenticeren, waardoor de kans kleiner wordt dat iemand de code kan onderscheppen om deze vervolgens te gebruiken voor een andere sessie. Met de nieuwste vorm van challenge-response-MFA (die wordt ondersteund door ESET Secure Authentication) kan de gebruiker de authenticatie eenvoudigweg bevestigen op een gekoppelde smartphone, waardoor de eenmalige code niet opnieuw hoeft te worden ingevoerd.
- **Firewalls** (hier gaan we later in het hoofdstuk op in).
- **Versleuteling:** Door versleuteling worden gegevens onleesbaar voor iemand die niet beschikt over de juiste decryptiesleutel. Versleuteling (encryptie) en decodering (decryptie) kunnen worden uitgevoerd in hardware (sneller) of software (minder duur). Als schijven en verwijderbare media worden versleuteld, zijn de gegevens op servers, desktopcomputers, laptops en mobiele apparaten beschermd indien een endpoint kwijtraakt of gestolen wordt, of in het geval van een datalek. Als bestanden, mappen en e-mails worden versleuteld, kunnen werkgroepen en teams volledig beveiligd samenwerken, waarbij het beveiligingsbeleid op alle endpoints wordt gehandhaafd door middel van centraal beheer op afstand (ESET Endpoint Encryption ondersteunt deze aanpak).
- **Back-up en herstel.** Back-up- en herstelsystemen omvatten back-up-software en -media, zoals tapes of schijven, die zich op de locatie of in de cloud kunnen bevinden. Back-ups moeten regelmatig worden getest om na te gaan of ze kunnen worden gebruikt voor herstel en of alle noodzakelijke systemen en gegevens regelmatig

genoeg en op juiste wijze worden weggeschreven om tegemoet te kunnen komen aan de behoeften van het bedrijf. Back-ups beschermen bedrijven tegen het accidenteel of opzettelijk vernietigen, wissen of wijzigen van gegevens (onder meer door middel van aanvallen met ransomware) en helpen de continuïteit van het bedrijf te garanderen na een calamiteit.

- **Beheer van mobiele apparaten (mobile device management, MDM).** Veel organisaties, in het bijzonder kleine en middelgrote bedrijven, staan medewerkers toe hun eigen mobiele apparaten te gebruiken voor werkgerelateerde doeleinden. Deze populaire trend wordt ook wel "bring your own device" (BYOD, neem je eigen apparaat mee) genoemd. Bedrijven moeten er echter wel voor zorgen dat deze apparaten veilig worden gebruikt om te garanderen dat gevoelige bedrijfsinformatie of klantgegevens niet in verkeerde handen komen als het apparaat kwijtraakt, gestolen wordt of op andere wijze wordt gecompromitteerd. MDM-software (zoals ESET MDM) biedt functies als beleidshandhaving (bijvoorbeeld door een wachtwoord te eisen), versleuteling, het plaatsen van apps/gegevens in "containers" (zodat zakelijke apps/gegevens en persoonlijke apps/gegevens van elkaar worden gescheiden) en wissen/vergrendelen op afstand.
- **Preventie van gegevensverlies (data loss prevention, DLP).** DLP-software voorkomt de accidentele (of opzettelijke) vrijgave van bepaalde gegevens, zoals socialezekerheidsnummers, beschermde gezondheidsinformatie en financiële gegevens, door e-mails en documenten te scannen op bepaalde trefwoorden en patronen van gegevenscombinaties.

WAARSCHUWING

Om DLP effectief toe te kunnen passen, moeten aanvullende middelen worden ingezet om beleid te wijzigen, incidenten (zowel interne als externe) te evalueren en correcties toe te passen. Als DLP wordt ingevoerd zonder deze aanvullende inspanningen, zal de effectiviteit ervan beperkt zijn.

ENDPOINT SECURITY KIEZEN

Endpoint security op je desktop-pc's, mobiele apparaten en servers vormt je eerste verdedigingslinie tegen cyberaanvallen, aangezien aanvallers zich meestal zullen richten op de "zwakste schakel" als ze je netwerk willen kraken.

Geavanceerde endpoint security bevat meerdere geraffineerde technologieën, zoals machine learning, vroegtijdige detectie en sandboxing, in een multidimensionale oplossing. Veel van de producten voor endpoint security van de "nextgen" die momenteel op de markt verkrijgbaar zijn, beweren de beste optie te zijn in de strijd tegen malware. Maar om te worden aangemerkt als product van "de volgende generatie" hoeven deze oplossingen maar één enkel aspect van endpoint security, bijvoorbeeld machine learning, aan te bieden. En daar blijft het dan ook vaak bij. Ga, wanneer je opties voor endpoint security voor je bedrijf evalueert, op zoek naar oplossingen die al deze technologieën bevatten: machine learning, vroegtijdige detectie, sandboxing en andere toonaangevende technologieën, evenals traditionele, op definities gebaseerde malware-detectie die in realtime wordt geactualiseerd met informatie uit de cloud over actuele dreigingen.

Om effectief te kunnen zijn moet endpoint security de volgende kenmerken hebben:

- **Een kleine installatie-grootte.** Anti-malwaresoftware die veel schijfruimte, geheugen en processorcapaciteit opeist, kan de apparatuur vertragen en zal vaak door gebruikers worden omzeild (uitgezet).
- **Robuuste update-mogelijkheden.** Anti-malwaresoftware moet realtime toegang hebben tot informatie over dreigingen, zonder zwakke plekken (single points of failure) of knelpunten (zoals een updateserver op je netwerk). De cloud wordt steeds meer benut om updates en informatie over dreigingen aan endpoints te leveren.
- **Veerkracht.** Anti-malwaresoftware moet effectief zijn, zelfs wanneer het niet met het netwerk is verbonden, en de veerkracht hebben die nodig is om zich te beschermen tegen malware die zich specifiek op anti-malware richt.
- **Productstabiliteit.** De producten die worden vrijgegeven, moeten bewezen veilig, stabiel en bug-vrij zijn.
- **Centraal beheer.** Bedrijven moeten niet alleen endpoint security installeren, maar ook controleren of de software juist is geïnstalleerd, goed werkt en regelmatig wordt geüpdatet. Je moet problemen met endpoint security op afstand kunnen oplossen en kunnen aantonen dat je endpoint security werkt (bijvoorbeeld aan de hand van audits en compliance-controles).

Het netwerk beveiligen

Het is de afgelopen jaren een stuk moeilijker geworden om netwerken van bedrijven te beschermen, nu er steeds meer gebruik wordt gemaakt van mobiele apparaten en cloud computing steeds belangrijk wordt. Maar het is nog steeds van groot belang om informatie te kunnen beveiligen en gegevens te kunnen beschermen. Voorbeelden van technologieën voor gegevensbescherming voor netwerken zijn:

- **Firewalls:** Netwerk-firewalls blijven de hoeksteen van netwerkbeveiliging en vormen misschien wel de belangrijkste investering die een bedrijf kan doen op het gebied van netwerkbeveiliging. Eenvoudige firewalls bieden pakketfiltering en stateful inspection van het netwerkverkeer. Een next-generation firewall (NGFW) biedt geavanceerde functies voor netwerkbeveiliging, waaronder bescherming tegen malware, content-filtering, inbraakdetectie- en preventie en informatie over dreigingen. Een web application firewall (WAF) is een soort firewall die speciaal is ontworpen om websites van bedrijven en applicaties die in verbinding staan met het internet te beschermen.
- **Inbraakdetectie- en preventiesystemen (IDS/IPS):** IDS en IPS detecteren malafide netwerkverkeer op basis van vooraf ingestelde definities en regels. Een IDS is een passief systeem dat het IT-team op de hoogte brengt van een mogelijke inbraak en verder niets doet. Een IPS is een actief systeem dat bepaalde acties kan uitvoeren, zoals het droppen of blokkeren van malafide verkeer.
- **Software as a Service (SaaS):** SaaS-toepassingen worden tegenwoordig ontzettend veel gebruikt: gebruikers vinden overal gebruiksvriendelijke software die hen helpt hun dagelijkse werkzaamheden uit te voeren en installeren deze massaal. Voorbeelden van populaire SaaS-toepassingen zijn Box, Dropbox, Google Docs en OneDrive. Bedrijven moeten de SaaS-toepassingen die op hun netwerk worden gebruikt actief identificeren en het gebruik van specifieke SaaS-apps beperken én erover voorlichten. Andere toepassingen moeten geheel worden geblokkeerd.
- **VLAN-segmentatie:** Bij de segmentatie van virtual local area networks (VLAN) wordt een netwerk gesegmenteerd volgens een bepaalde logica, bijvoorbeeld op afdeling (zoals Financiën, Personeelszaken en Operationeel) om onbevoegde toegang tot bepaalde gegevens te vermijden en buitensporig netwerkverkeer dat apparaten en verbindingen vertraagt (bijv. massale broadcasts) te voorkomen.

- **Virtueel privé-netwerk (VPN):** Een VPN-apparaat of -software stelt gebruikers in staat op afstand via internet verbinding te maken met het netwerk van het bedrijf. Deze verbinding loopt via een versleutelde tunnel. Een VPN kan ook worden gebruikt om verbinding te maken met de netwerken van partners- en/of providers, bijvoorbeeld een leverancier in je toeleveringsketen of een aanbieder van cloud-diensten.
- **Netwerktoegangsbeheer (Network Access Control, NAC):** NAC is een uniforme oplossing voor beveiligingsbeheer die het beveiligingsbeleid handhaaft op basis van gebruikers- of systeemauthenticatie, waarbij een systeem of gebruiker toegang krijgt tot bepaalde delen van het netwerk op basis van de mate waarin wordt voldaan aan de beveiligingsvoorschriften (zijn de beveiligingspatches en antivirusdefinities bijvoorbeeld actueel, is de netwerkverbinding versleuteld met een VPN enz.).
- **Beheer van beveiligingsinformatie en beveiligingsevents (security information and event management, SIEM):** SIEM-oplossingen verzamelen en analyseren log-informatie uit verschillende gegevensbronnen als firewalls, IDS/IPS, WAF's, servers en endpoints om zo inzicht te krijgen in de huidige beveiligingsstatus van het netwerk en afwijkingen te kunnen detecteren en tijdig mitigeren.
- **Patch-beheer:** Het patchen van de bekende zwakke plekken in de beveiliging van servers en endpoints is een kritieke beveiligingsfunctie voor alle organisaties. Naarmate je organisatie groter wordt, zal het steeds moeilijker worden om handmatige software-patches te installeren op honderden servers en endpoints die zich mogelijk op verschillende, ver uit elkaar gelegen locaties bevinden. Oplossingen voor patch-beheer helpen organisaties hun patch-beheerfuncties te automatiseren en beheren.
- **Wachtwoordmanagers:** Ze zijn eenvoudig maar zeer nuttig. Dit stelt gebruikers in staat met meer gemak verschillende, sterke wachtwoorden te genereren & beheren. Het is zeker de moeite waard om binnen je bedrijf een wachtwoordmanager in te voeren gezien het rendement van deze oplossing.
- **Bescherming van domeinnaamsystemen (DNS):** DNS is opnieuw een populaire vector voor aanvallen, met name denial-of-service (DoS)-aanvallen. Er moeten daarom verbeteringen in de beveiliging van het DNS-protocol worden ingevoerd, zoals DNS Security Extensions (DNSSEC) en best practices voor beveiliging in de serverconfiguratie (zoals het uitschakelen van recursieve lookups). Andere opties voor DNS-beveiliging zijn de installatie van

speciale (en extra beveiligde) DNS-apparatuur of het gebruik van een externe DNS-service.

- **Filteren van web content:** Door content te filteren kan, aan de hand van het website-adres (IP-adres of URL) of de daadwerkelijke inhoud, worden voorkomen dat gebruikers niet-geautoriseerde en potentieel schadelijke of malafide websites bezoeken.

Begrijpen hoe belangrijk orkestratie is

Naarmate je bedrijf groeit, wordt de behoefte aan automatisering en orkestratie van je IT-processen steeds groter, met name als je een klein IT-team hebt met beperkte middelen. Het handmatig installeren en configureren van endpoints - desktop-pc's, mobiele apparaten en servers - is niet haalbaar als een bedrijf begint te groeien en zeker niet als er verschillende locaties zijn die ver van elkaar zijn verwijderd.

Naast de inefficiënties die zijn gemoeid met het "aanraken" van elk endpoint, neemt door handmatige processen de kans op fouten toe. Denk hierbij aan inconsequente of verkeerde instellingen.

Door middel van automatisering en orkestratie kan je IT-team efficiënter werken, neemt jouw productiviteit en die van je eindgebruikers toe (omdat apparatuur en verbindingen minder vaak buiten bedrijf zijn) en kunnen de kosten van fouten in de configuratie worden teruggedrongen. Beheerplatforms maken het gemakkelijker om handmatige processen te automatiseren en standaardvoorschriften vast te stellen.


TIP

Sommige kleine en middelgrote bedrijven beschikken over onvoldoende middelen om een beheerplatform op locatie te installeren. In die gevallen kan gebruik worden gemaakt van een oplossing in de cloud of kan een managed service provider (MSP) de automatiserings- en orkestratiediensten verzorgen die nodig zijn om de snelle groei en de steeds complexere IT-omgeving te ondersteunen.


TIP

Veel kleine en middelgrote bedrijven gebruiken ESET Security Management Center (ESMC) en ESET Cloud Administrator (ECA) om hun externe middelen en middelen in de cloud op eenvoudige en veilige wijze te beheren, zonder dat er kostbare en complexe hardware op locatie hoeft te worden geïnstalleerd.

FONQ

SAMENVATTING

In het kader van de GDPR was fonQ op zoek naar een encryptieoplossing voor alle laptops die medewerkers dagelijks gebruiken. Na een uitgebreide testfase is de keuze gevallen op de encryptieoplossingen van ESET. De doorslaggevende factor was de mogelijkheid om alles vanuit één centraal managementplatform te beheren. Dit zorgt niet alleen voor beveiligde laptops, maar ook voor een efficiëntere IT-afdeling.

GEEF JE HUIS WAT FONQ

FonQ is een online warenhuis met ruim 65.000 producten op het gebied van wonen, koken en lifestyle. Het webwarenhuis is uitgeroepen tot beste webwinkel in de categorie 'Wonen & Tuin' tijdens de Thuiswinkel Awards 2016. Ook tijdens de ABN AMRO Webshop Awards 2016-2017 en 2017-2018 is fonQ verkozen tot beste webshop in wonen. Fonq is in 2003 opgericht en sinds enkele jaren internationaal actief in onder andere België, Duitsland en Frankrijk. Het hoofdkantoor is gevestigd in Utrecht en met ruim 250 werknemers wordt het gehele ordertraject in-house gedaan: van logistiek, klantenservice en fulfillment tot inkoop, marketing en visual design.

DE UITDAGING VAN FONQ

Bij fonQ werkt ongeveer de helft van de medewerkers met een laptop. Deze laptops worden uiteraard overal mee naartoe genomen. Met de invoering van de GDPR wetgeving, mei 2018, zocht fonQ naar een encryptie oplossing om de harde schijven van al deze laptops te versleutelen. Met 125 laptops was een eenvoudig te beheren oplossing cruciaal.

DE OPLOSSING VOOR FONQ

In de zoektocht naar een geschikte oplossing heeft fonQ onderzoek gedaan naar de verschillende oplossingen op het gebied van encryptie. Hierbij heeft fonQ vooral gelet op prijs/kwaliteit en het gebruiksgemak voor hun IT-afdeling. fonQ heeft bij ESET een demo aangevraagd, uitgebreid getest en vergeleken met andere oplossingen. In deze uitgebreide testfase heeft ESET, fonQ uitgebreid ondersteund met technische vragen en heeft ESET een technische demo verzorgd (op afstand).

(vervolgd)

(vervolgd)

fonQ heeft gedurende dit traject voornamelijk gekeken naar de gebruiksvriendelijkheid. Is de oplossing gemakkelijk te implementeren in de organisatie? Hoe is de indruk bij de eindgebruikers?

Na vergelijkingen met andere oplossingen heeft fonQ ervoor gekozen om ESET Secure Authentication en ESET Endpoint Encryption powered by DESlock te implementeren in de organisatie. Doorslaggevende factor voor fonQ in de keuze voor ESET waren de uitgebreide functionaliteiten van ESET Endpoint Encryption powered by DESlock, de lokale aanwezigheid, Nederlandse support en dat ze al bekend waren met de endpoint securityoplossing van ESET. Daarnaast is het een pluspunt dat de IT-securityoplossingen op de verschillende endpoints eenvoudig te beheren zijn via één centraal managementplatform.

Hiermee maakt ESET het mogelijk dat de IT-afdeling standaard meer inzicht heeft. fonQ kan alles monitoren en op afstand aanpassingen doorvoeren of instellingen wijzigen. Ook de gebruiksvriendelijkheid van ESET speelde een rol in de uiteindelijke beslissing. De laptops worden voornamelijk gebruikt door marketeers en verkopers; zij willen zo min mogelijk te maken hebben met de technische implicaties in de interface.

Daarnaast is er het vooruitzicht dat alle oplossingen van ESET vanuit één centraal punt kunnen worden beheerd. Dit door middel van de ESET Security Management Center die binnenkort wordt gelanceerd. Momenteel heeft fonQ een apart beheerprogramma voor endpoint security en encryptie, dus het voordeel hiervan is aanzienlijk.

DE RESULTATEN

fonQ was heel gericht op zoek naar een oplossing naar aanleiding van de GDPR. Het implementeren van encryptiesoftware was daarom de hoogste prioriteit voor de IT-afdeling van fonQ. Door gebruik te maken van de tweefactorauthenticatie- en encryptieoplossingen van ESET heeft fonQ zekerheid dat de harde schijf van een laptop is vergrendeld wanneer deze ergens wordt achtergelaten of gestolen.

Naast de zekerheid dat de laptops goed zijn beveiligd heeft fonQ ook een slag geslagen op het gebied van efficiency. Voor de IT-afdeling van fonQ is dit enorm belangrijk omdat het een helse klus is om 125 laptops per stuk te beheren via de supportdesk. Dit doen ze nu gemakkelijk vanuit 1 beheerportaal. Een hele hoop acties zetten ze nu centraal uit, wat aanzienlijk veel tijd bespaart.

IN DIT HOOFDSTUK

- **Technische controles aanvullen met organisatorische controles**
- **Begrijpen waarom procesmatige controles belangrijk zijn**

Hoofdstuk 5
Bekend raken met organisatorische en procesmatige controles

In dit hoofdstuk leer je hoe organisatorische en procesmatige controles er samen met technische controles voor zorgen dat de gegevens van je bedrijf beschermd worden.

Organisatorische controles invoeren

Voor effectieve gegevensbescherming is meer nodig dan alleen technische oplossingen. Je moet ook administratieve en organisatorische controles vaststellen om te garanderen dat technische controles naar behoren kunnen worden geïnstalleerd, geconfigureerd en gebruikt in het kader van een samenhangende strategie voor beveiligingsbeheer.

Dit zijn een paar voorbeelden van organisatorische controles:

- **Privé- en gevoelige persoonsgegevens:** Technische controles, zoals versleuteling en software voor de preventie van gegevensverlies (DLP), moeten voorzichtig worden gebruikt met het oog op hun kosten (zowel financiële als performance-gerelateerd). Voor versleuteling en decodering zijn aanvullende processen nodig en DLP-oplossingen moeten scans kunnen uitvoeren aan de hand

van trefwoorden en patronen om privé- en gevoelige gegevens, zoals creditcardnummers, gezondheidsinformatie en socialezekerheidsnummers, te identificeren. Als je een schema voor gegevensclassificatie opstelt, is het gemakkelijker te begrijpen welke gegevens moeten worden beschermd en hoe.

- **Documenteren en inspecteren van gegevens:** Bedrijven die gevoelige gegevens verzamelen, verwerken en/of opslaan, moeten documenteren waarom zij die gegevens verzamelen, hoe ze worden verzameld (uit welke bronnen), hoe ze worden gebruikt en hoe ze worden beschermd. Als je het beleid voor gegevensbeveiliging en -privacy op papier zet, is het gemakkelijker om deze vragen te beantwoorden en te voldoen aan audit-eisen, met name in het kader van regelgeving als de Health Insurance Portability and Accountability Act (HIPAA) in de VS en de Algemene verordening gegevensbescherming (AVG) in de EU.
- **Beveiligingsbeleid:** Beleid hoeft niet te bestaan uit enorme boekwerken. In veel gevallen is een paar paragrafen genoeg. In het beveiligingsbeleid moeten de individuele rollen en verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens duidelijk worden gedefinieerd. Voorbeelden van belangrijke beveiligingsaspecten die in het beleid van elk bedrijf aan bod moeten komen, zijn:
  - internet en beleid inzake aanvaardbaar gebruik
  - beleid voor het meenemen van eigen apparaten
  - beleid voor toegang op afstand
  - beleid met betrekking tot geautoriseerde software
- **Personeelszaken:** Het gaat hierbij om beleid en procedures om te garanderen dat de persoonsgegevens (zoals sollicitatieformulieren en gegevens over loonadministratie, opleiding en disciplinaire maatregelen) die worden verzameld, bewaard en verwerkt door de afdeling Personeelszaken, naar behoren worden beschermd. Hieronder vallen ook processen als screening voor aanvang van het dienstverband, drugstesten en functieroulering.
- **Een volwassenheidsmodel voor beveiliging gebruiken:** Aan de hand van een volwassenheidsmodel voor beveiliging kan je bepalen welke beveiligingscapaciteiten je bedrijf heeft op bepaalde terreinen en de hiaten identificeren tussen waar je nu bent en waar je zou moeten zijn. Wat je wilt bereiken hangt uiteraard af van een aantal factoren, zoals:

- wat je moet beschermen: bijvoorbeeld gevoelige gegevens, financiële informatie, intellectueel eigendom, medische apparatuur of kritieke infrastructuur;
- je branche, bijvoorbeeld medisch, financieel, retail, defensieopdrachten of nutsvoorzieningen;
- de regelgeving waar je aan moet voldoen, bijvoorbeeld de Health Insurance Portability and Accountability Act (HIPAA) in de VS, de Algemene verordening gegevensbescherming (AVG) in de EU, de Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, de normen van gegevensbescherming voor de betaalkaartenbranche (PCI-DSS) enz.;
- je risicoprofiel: ben je gevestigd in een vijandige of instabiele geografische regio, een stad met veel misdaad of een gevaarlijk of industrieel gebied?

» **Je medewerkers opleiden en testen:** Al je medewerkers moeten security awareness trainingen volgen zodat zij de 'first line of defense zijn' als het aankomt op de bescherming van gegevens binnen je organisatie. Je gaat bij deze cursussen in op onderwerpen als de veiligheid van wachtwoorden, spam en phishing, bescherming tegen malware, eisen voor de naleving van regelgeving en gegevensbescherming (zoals gegevensclassificatie, soorten gevoelige gegevens en technologieën om gegevens te beschermen). De testen kunnen verschillende vormen aannemen en het is belangrijk dat de trainingen boeiend zijn en de opgedane kennis gedurende het jaar wordt herhaald.

» **Gegevensbeschermings-effectbeoordelingen uitvoeren:** Gegevensbeschermings-effectbeoordelingen worden in de AVG verplicht gesteld voor gegevensverwerkingsoperaties die "waarschijnlijk gepaard gaan met hoge risico's in verband met de rechten en vrijheden van natuurlijke personen". Een gegevensbeschermings-effectbeoordeling is vergelijkbaar met het gewone proces voor risicobeheer (dat wordt besproken in hoofdstuk 2), maar bevat een aantal aanvullende parameters die verband houden met de verwerking van persoonsgegevens.

» **Implementeren van gegevensbescherming door ontwerp en door standaardinstellingen:** De AVG vereist dat gegevens worden beschermd door ontwerp en door standaardinstellingen, hetgeen betekent dat organisaties technische en organisatorische maatregelen moeten invoeren om zo weinig mogelijk persoonsgegevens te verzamelen, verwerken en op te slaan.

GEGEVENS BESCHERMEN: EEN STAPPENPLAN

De volgende systematische benadering van cyberbeveiliging zal je helpen de waardevolle gegevens in je bedrijf te beschermen. Het is eigenlijk heel eenvoudig.

Bepaal wat je activa, risico's en middelen zijn

Maak een lijst van alle computersystemen en -diensten die je bedrijf gebruikt. Als je niet weet wat je hebt, kun je het immers ook niet beschermen. Vergeet de mobiele apparaten niet, zoals eventuele smartphones en tablets die worden gebruikt om informatie van het bedrijf of van klanten te raadplegen. Dit is buitengewoon belangrijk, want het Ponemon Institute schat dat 60 procent van de medewerkers de beveiligingsfuncties op mobiele apparaten omzeilt en dat 48 procent van hen de beveiligingsinstellingen uitschakelt die de werkgever vereist. En vergeet cloud-diensten als Box, Dropbox, iCloud, Google Docs, Office365, OneDrive en SalesForce niet.

Neem de lijst door en analyseer welk risico is gemoeid met elk item en of je het systeem, de software of de dienst nog nodig hebt. Wie of wat vormt het risico? Een andere goede vraag om jezelf te stellen is: "Wat zou er mis kunnen gaan?" Bij sommige risico's is de kans dat ze voorvallen groter. Schrijf eerst alle risico's op en rangschik ze vervolgens op basis van de schade die ze kunnen aanrichten en de kans dat ze zich daadwerkelijk voordoen.

Misschien heb je hulp van buiten nodig voor dit proces. Daarom heb je nog een lijst nodig: de middelen die je kunt inzetten om problemen op het gebied van cyberveiligheid op te lossen. Denk hierbij aan een personeelslid dat veel weet over beveiliging, of een partner of leverancier. Brancheverenigingen en lokale organisaties van ondernemers hebben vaak ook hulpmiddelen en kunnen nuttig advies geven. Partijen zoals de National Cyber Security Alliance en European Union Agency for Network and Information Security bieden gratis voorlichtingsmateriaal en overzichten met handige tips aan. Neem ook eens contact op met de lokale wethandhavingsinstantie (je moet in ieder geval een contactpersoon en nummer hebben voor het geval je het slachtoffer wordt van een cybermisdaad).

Formuleer beleid

Een degelijk beveiligingsprogramma begint bij beveiligingsbeleid dat wordt gesteund door het management. Als je de baas bent, moet je aan iedereen duidelijk maken dat je beveiliging serieus neemt en dat je

bedrijf er alles aan doet om de privacy en beveiliging van alle gegevens die het verwerkt te garanderen. Vervolgens moet je de voorschriften bepalen die je wilt invoeren, bijvoorbeeld dat er geen sprake mag zijn van onbevoegde toegang tot de systemen en gegevens van het bedrijf en dat medewerkers de beveiligingsinstellingen op hun mobiele apparaten niet mogen uitschakelen.

Kies je controles

Controles dienen om het beleid in de praktijk te handhaven. Als het beleid bijvoorbeeld is dat niemand onbevoegd toegang mag hebben tot systemen en gegevens van het bedrijf, dan kan je ervoor kiezen alle toegang tot systemen van het bedrijf te beschermen met een unieke combinatie van gebruikersnaam, wachtwoord en token.

Als je wilt beheersen welke programma's worden gebruikt op de computers van je bedrijf, kun je ervoor kiezen medewerkers geen beheerdersrechten te geven. Om datalekken te voorkomen die het gevolg zijn van kwijtgeraakte of gestolen mobiele apparaten, kun je van medewerkers eisen dat zij dergelijke incidenten dezelfde dag nog melden en aangeven dat dit soort apparaten op afstand zullen worden vergrendeld en gewist.

Je hebt ten minste drie elementaire beveiligingstechnologieën nodig:

- **anti-malwaresoftware** om te voorkomen dat schadelijke code (zoals virussen en ransomware) op je apparaten wordt gedownload;
- **versleuteling** om ervoor te zorgen dat gegevens op kwijtgeraakte of gestolen apparaten niet toegankelijk zijn;
- **multifactorauthenticatie** zodat er meer nodig is dan alleen een gebruikersnaam en wachtwoord (bijvoorbeeld een eenmalige code die naar een geregistreerde mobiele telefoon wordt verzonden) om toegang te kunnen krijgen tot systemen en data.

Voer controles in

Als je controles invoert, moet je nagaan of ze ook werken. Als je beleid bijvoorbeeld is dat er geen niet-geautoriseerde software op systemen van het bedrijf mag staan, kan één van je controles bestaan uit anti-malwaresoftware die scans uitvoert om schadelijke code te identificeren. Je moet deze software installeren en testen om te zien of de normale zakelijke operaties er niet of minimaal door worden beïnvloed en de procedures documenteren die moeten worden gevolgd als er malware wordt gedetecteerd. Het geniet wel de voorkeur om gebruikers geen rechten te geven om niet-geautoriseerde software te kunnen installeren.

(vervolgd)

(vervolgd)

Medewerkers, partners en leveranciers voorlichten

Je medewerkers moeten van meer op de hoogte zijn dan alleen het beleid en de procedures van je bedrijf. Ze moeten ook begrijpen *waarom* deze noodzakelijk zijn. Dit betekent dat je moet investeren in bewustwording en voorlichting omtrent beveiliging. Dit is vaak de meest effectieve beveiligingsmaatregel die je kunt treffen.

Door met je personeel samen te werken, kun je de aandacht vestigen op problemen als phishing-e-mails. Uit een recent *Data Breach Investigations Report (DBIR)* van Verizon werd duidelijk dat 23 procent van de phishing-e-mails die naar medewerkers worden gestuurd, wordt geopend en dat 11 procent van de ontvangers ook de bijlage opent. Dit vergroot de kans op een datalek en informatiediefstal aanzienlijk.

Zorg ervoor dat iedereen die gebruikmaakt van je systemen, waaronder managers, leveranciers en partners, van informatie wordt voorzien. En onthoud dat schendingen van het beveiligingsbeleid consequenties moeten hebben. *Als je de naleving van het beleid niet afdwingt, worden al je beveiligingsinspanningen ondermijnd.*

Blijf beoordelen, controleren en testen

Cyberveiligheid is voor elk bedrijf, groot of klein, een constant proces en geen eenmalig project. Plan periodieke herbeoordelingen van je beveiliging in, ten minste eenmaal per jaar. Blijf op de hoogte van nieuwe dreigingen door regelmatig nieuws over beveiliging te lezen op websites als WeLiveSecurity.com, KrebsOnSecurity.com en `DarkReading.com`.

Mogelijk moet je het beveiligingsbeleid en de controles meer dan eens per jaar actualiseren als er veranderingen plaatsvinden binnen het bedrijf, bijvoorbeeld als je met nieuwe leveranciers begint te werken, nieuwe projecten start, nieuwe mensen aanneemt of er personeel weggaat (als iemand het bedrijf verlaat, moeten bijvoorbeeld alle toegangsrechten worden ingetrokken). Overweeg een externe consultant in de arm te nemen om een penetratietest en beveiligingsaudit uit te voeren om te kijken waar de zwakke plekken zitten en hier iets aan te doen.

Procesmatige controles invoeren

Procesmatige controles helpen je bedrijf de impact van een datalek of dataverlies tot een minimum te beperken. Uit een recent onderzoek van Ponemon Institute kwam bijvoorbeeld naar voren dat bedrijven de gemiddelde kosten van een gegevenslek per record kunnen verlagen van $ 141 naar $ 122 door een effectief proces te implementeren voor de reactie op incidenten, waardoor zij minder tijd nodig hebben

om een datalek op te merken en te beheersen. Je calamiteitenteam kan uit interne medewerkers bestaan of deze functie kan worden uitbesteed aan een derde partij. Daarnaast is een combinatie van beide mogelijk. Voor een inbreuk op slechts 10.000 records zorgt dit al voor besparingen van $ 190.000. Deze investering is dus zeker de moeite waard.

Bij het opzetten van processen moeten bedrijven:

- **mensen betrekken:** Dit mag geen initiatief zijn dat door het management van bovenaf wordt opgelegd. Als je de mensen betrekt die daadwerkelijk met de verschillende processen en technologieën werken, kan je garanderen dat de controles nuttig zijn en effectief kunnen worden geïmplementeerd;
- **verantwoordelijkheden bepalen:** De individuele verantwoordelijkheden moeten duidelijk worden gedefinieerd en begrepen: iedereen moet weten wat zijn rol is;
- **toelichten waarom procesmatige controles nodig zijn:** Beveiligingsmaatregelen worden vaak gezien als lastig of hinderlijk. Ze zullen worden genegeerd of omzeild als de medewerker niet begrijpt waarom ze nodig zijn en waarom ze belangrijk zijn voor het bedrijf.

BELANGRIJK OM TE ONTHOUDEN

Volgens het Ponemon Institute worden datalekken gemiddeld na 191 dagen ontdekt en duurt het gemiddeld 66 dagen om ze te beheersen. De tijd die nodig is om een datalek op te merken en te beheersen heeft directe consequenties voor de omvang en de kosten ervan.

Bedrijven kunnen de kosten van een datalek of -verlies ook terugdringen door middel van processen voor beveiligde gegevensoverdracht. Versleuteling vermindert de gemiddelde kosten per record volgens het Ponemon Institute bijvoorbeeld met $ 16. Als gegevens worden versleuteld (en kan worden aangetoond dat dit naar behoren is gebeurd) zullen in het kader van veel regelgeving op het gebied van gegevensprivacy de "EU-US Privacy Shield"-bepalingen gelden. In deze gevallen hoeven bedrijven vaak geen melding te doen van het lek, waardoor de kosten aanzienlijk lager zijn - zowel wat directe (zoals meldingen, kredietmonitoringsdiensten en rechtszaken) als indirecte kosten (zoals imagoschade en verlies van klanten) betreft. Wederom: versleuteling kan bij een inbreuk waarbij 10.000 records zijn betrokken de totale kosten met ongeveer $ 160.000 verminderen.

Belangrijke procesmatige controles zijn:

- **Beleid voor toegangscontrole:** In dit beleid wordt bepaald wie toegang heeft tot welke systemen, toepassingen en gegevens en voor welke doeleinden.
- **Beheer van middelen/activa:** Het is belangrijk dat je weet wat je beschermt en waarom (de waarde of het risico ervan voor de organisatie). Bedrijven moeten niet alleen een nauwkeurige inventaris bijhouden van alle computers en gegevensactiva/-middelen, maar ook zorgen voor een gepaste "beveiligingshygiëne". Dit wil zeggen dat systemen en toepassingen de laatste beveiligingspatches moeten bevatten en dat gevoelige gegevens die niet langer nodig zijn tijdig worden vernietigd, in overeenstemming met het geldende beleid voor het bewaren, archiveren en vernietigen van gegevens.
- **Veranderingsmanagement:** Met veranderingsmanagement wordt gegarandeerd dat systemen en applicaties worden gedocumenteerd, getest en goedgekeurd zodat de impact van een verandering en de gevolgen voor de algehele beveiligingsstrategie van het bedrijf duidelijk zijn.
- **Reageren op incidenten:** Wanneer een beveiligingsincident (zoals een lek of aanval) plaatsvindt, moeten bedrijven precies weten en begrijpen hoe op het incident moet worden gereageerd. Zo kan er snel en effectief worden ingegrepen, zodat schade kan worden beperkt, het herstel kan worden ingezet, bewijsmateriaal kan worden beschermd, intern en extern kan worden gecommuniceerd en de onderliggende oorzaken kunnen worden geanalyseerd.
- **Zakelijke continuïteit:** Een plan voor zakelijke continuïteit minimaliseert de impact van een incident of calamiteit op het bedrijf en zorgt ervoor dat het bedrijf redelijk blijft functioneren totdat de normale werkzaamheden weer kunnen worden hervat.

Ten slotte kunnen bedrijven gebruikmaken van professionele beveiligingsdiensten om hun interne capaciteit aan te vullen. Het gaat hierbij onder meer om dagelijkse monitoring en informatie over dreigingen, evenals detectie, escalatie en de reactie op incidenten. Dit is buitengewoon belangrijk voor forensische en onderzoeksactiviteiten, beoordelings- en auditdiensten, crisisteam-management en communicatie.

BELANGRIJK OM TE ONTHOUDEN

De organisatorische en procesmatige controles die worden ingevoerd, moeten worden afgestemd op het risiconiveau.

IN DIT HOOFDSTUK

- **Aan de slag met administratieve controles**
- **Weet wat je moet beschermen en hoe je dat kunt doen**
- **Technische controles invoeren**
- **Back-ups en herstel garanderen, reageren op incidenten en herstel na een calamiteit**
- **Samenwerken met gebruikers en andere beveiligingsexperts**

Hoofdstuk 6
Tien belangrijke punten voor effectieve gegevensbescherming

In dit hoofdstuk bespreken we tien goede werkwijzen om je te helpen de gegevens van je bedrijf effectief te beschermen.

- **Formuleer beveiligingsbeleid:** Veel bedrijven kennen niet veel prioriteit toe aan schriftelijk beleid en beginnen gelijk met de invoering van technische controles. Technische controles (zoals firewalls, endpointbescherming enz.) die worden ingevoerd zonder administratieve controles (ofwel beleid en procedures) worden bijna altijd reactief geïmplementeerd, zonder een goed doordachte, samenhangende en integrale beveiligingsstrategie of een beheerkader voor beveiliging (die je aan de hand van het beleid en je informatiebeveiligingsanalyse kunt vaststellen). Dit leidt er onvermijdelijk toe dat je te veel tijd besteedt aan technische oplossingen die niet effectief (of correct) worden toegepast en onvolledige of ontoereikende bescherming bieden.
- **Identificeer je activa:** Je moet weten wat je gaat beschermen, dus houd vooral een nauwkeurige inventaris bij van al je IT-hardware en -software. Zonder een volledige inventaris ben je mogelijk niet op de hoogte van kwetsbare systemen in je netwerk die

het risico op een aanval groter maken. Bij het datalek bij Target in 2013 verkregen de aanvallers op afstand toegang tot een onderhoudssysteem voor de verwarming, ventilatie en airconditioning om vervolgens de creditcard- en debetkaartgegevens en/of persoonsgegevens van meer dan 110 miljoen klanten te stelen. Er zijn diverse vrij toegankelijke hulpmiddelen die je kunt gebruiken om je netwerk en endpoints te scannen en een begin te maken. Commerciële oplossingen kunnen je helpen constant een nauwkeurige inventaris van je activa bij te houden en vele bieden ook beheermogelijkheden op afstand aan, zodat je software kunt installeren, verwijderen en actualiseren. Je moet de kwetsbare punten van alle apparaten die met het internet zijn verbonden (waaronder persoonlijke mobiele apparaten) zo veel mogelijk dichten door gepaste beveiliging te installeren en te handhaven.

- **Weet waar je staat wat beveiliging betreft:** Dit is heel simpel: je creëert een roadmap of volwassenheidsmodel om te evalueren waar je bedrijf zich momenteel bevindt (de huidige stand van zaken). Vervolgens pas je een op risico's gebaseerde benadering toe om relevante dreigingen te identificeren voor de activa in je omgeving (zie de vorige tip) en te bepalen welke maatregelen op het gebied van cyberbeveiliging en gegevensbescherming je moet treffen. Ten slotte kun je een gap-analyse uitvoeren en bepalen welke stappen je moet nemen en waar je je middelen in moet investeren. Raadpleeg hoofdstuk 3 voor meer informatie over de beoordeling van beveiligingsrisico's.
- **Classificeer al je gegevens:** Voor veel bedrijven vormen gevoelige klantgegevens en andere bedrijfseigen informatie hun "kroonjuwelen". Maar het is niet haalbaar of wenselijk om voor al je gegevens dezelfde bescherming en controlemechanismen in te voeren. Denk in plaats daarvan eens na over de vraag welke gegevens je uit je slaap zouden houden, als ze worden gestolen of als je ze kwijtraakt. Wat zou de impact van een datalek op het imago van je merk, de loyaliteit van je klanten en zelfs de levensvatbaarheid van je bedrijf zijn? Formuleer (en documenteer) een intuïtief beleid voor gegevensclassificatie voor jouw organisatie met categorieën (bijvoorbeeld "Alleen voor intern gebruik", "Gevoelige gegevens" en "Goedgekeurd voor openbaarmaking"), waarin wordt aangegeven hoe verschillende niveaus van informatie moeten worden beschermd (bijvoorbeeld door middel van versleuteling, back-ups, goedkeuring voor vrijgave en vernietiging).

TIP

De Algemene verordening gegevensbescherming (AVG) eist van organisaties dat zij persoonsgegevens wissen als het datasubject (bijvoorbeeld een persoon) hierom vraagt. Ontwerp, om het gemakkelijker te maken om te voldoen aan de eisen van de AVG, een strategie voor gegevensclassificatie waarmee je persoonsgegevens die in de toekomst moeten worden verwijderd of anderszins moeten worden gewijzigd, kunt identificeren of markeren (onder meer aan de hand van back-ups).

- **Versleutel je gevoelige gegevens:** Bij de versleuteling van gegevens wordt platte tekst omgezet in een niet-leesbaar formaat ("ciphertext" genoemd), waardoor de tekst onbruikbaar is voor niet-bevoegde partijen die niet beschikken over de encryptie-/decryptiesleutels. Voor effectieve versleuteling is het dus van groot belang dat de sleutels goed beveiligd worden. Je moet op zijn minst je ongebruikte (opgeslagen) gegevens versleutelen. Je kunt aanvullende versleuteling gebruiken voor gegevens die "in beweging" (of "onderweg") zijn door middel van Transport Layer Security (TLS)-versleuteling. Verder moet je voor gegevens die in gebruik zijn, gebruik maken van versleuteling binnen de applicatie, als deze beschikbaar is. Versleuteling kan zowel op hardware als op software zijn gebaseerd.

TIP

Veel regelgeving op het gebied van datalekken bevat "EU-US Privacy Shield"-bepalingen voor versleutelde gegevens, hetgeen de kosten en impact van een datalek aanzienlijk kan verminderen.

- **Maak back-ups en herstel je waardevolle gegevens (en voer testen uit):** Regelmatig betrouwbare back-ups maken van je systemen en data is een elementaire, maar cruciale best practice op het gebied van beveiliging. Als je goede back-ups hebt gemaakt, kun je de gegevens van een bestand dat per ongeluk is gewist of een harde schijf die beschadigd is geraakt, weer terugkrijgen. Het wordt steeds goedkoper om back-ups te maken op schijven en back-up-oplossingen in de cloud zijn zeer kosteneffectief en gebruiksvriendelijk. Er is dus geen excuus om niet te back-uppen. De laatste jaren komen aanvallen met ransomware steeds vaker voor en back-ups zijn de enige manier om te garanderen dat je je gegevens terugkrijgt na zo'n aanval. En de bonus is dat je het losgeld niet hoeft te betalen.

BELANGRIJK OM TE ONTHOUDEN

Je moet regelmatig testen hoe goed je bedrijf in staat is kritieke systemen en gegevens te herstellen met behulp van back-ups. Niet alleen om na te gaan of de back-ups niet beschadigd zijn, maar ook om te garanderen dat jij en je personeel bekend zijn met het herstelproces.

- **Investeer in endpointbescherming:** Met "investeren" bedoelen we niet dat je een gratis antivirussoftware downloadt van het internet. We bedoelen dat je al je endpoints - desktop-pc's, mobiele apparaten en servers - beschermt met een robuuste, commerciële oplossing voor endpoints. Vandaag de dag is overal informatie te vinden en het endpoint is waar alles bij elkaar komt. Nu meer dan ooit. Het is dus zonder meer de moeite waard erin te investeren.
- **Plan en bereid je voor:** Elk bedrijf moet plannen hebben om te reageren op incidenten, de zakelijke continuïteit te waarborgen en de activiteiten na een calamiteit te hervatten. Je calamiteitenteam moet worden getraind in elementaire forensische procedures om te garanderen dat elk beveiligingsincident wordt behandeld als een potentiële rechtszaak en dat mogelijke bewijsmaterialen worden bewaakt. Plannen voor zakelijke continuïteit en herstel na calamiteiten maken het voor je bedrijf gemakkelijker om de normale werkzaamheden zo snel mogelijk weer te hervatten na een ingrijpende gebeurtenis of calamiteit. Nauwkeurige en tijdige communicatie, zowel intern als extern, vormt een cruciaal onderdeel van de plannen voor zakelijke continuïteit en herstel na calamiteiten.
- **Train je gebruikers:** De zwakste schakel in de beveiliging van organisaties zijn altijd de eindgebruikers. Maar dat wil niet zeggen dat het hun schuld is. Waarschijnlijk zal niet iedereen binnen je bedrijf aangenomen zijn omdat ze experts zijn op het gebied van beveiliging. Aanvallers weten dit en gebruiken social engineering-technieken om nietsvermoedende gebruikers onder meer te verleiden om op malafide links in spam- en phishing-e-mails te klikken, hun wachtwoord te onthullen (zie de tekst in de marge "Hoe kan ik een goed wachtwoord kiezen?") en malafide websites te bezoeken. Organiseer regelmatig boeiende, relevante en *korte* trainingsoefeningen om de aandacht op beveiliging te vestigen, zodat gebruikers zichzelf - en jou - kunnen helpen!
- **Probeer het niet alleen op te lossen:** Cybercriminelen werken niet alleen. Ze werken samen met andere dubieuze personen om hun slachtoffers aan te vallen, recyclen malafide code op

het "dark web" en maken misbruik van de endpoints van niets-vermoedende gebruikers om deze in te zetten om andere apparaten aan te vallen. Maar de "good guys" zijn gelukkig ook niet alleen. Benut de kennis van de grote gemeenschap van beveiligingsexperts. Ze zijn te vinden bij wethandhavingsinstanties, brancheorganisaties, outsourcing-bedrijven en managed service providers in de beveiligingssector. Ook is er realtime informatie over dreigingen te vinden in de cloud.

HOE KAN IK EEN GOED WACHTWOORD KIEZEN?

Voor bijna alles wat we online doen, hebben we inloggegevens nodig. Bij het inloggen wordt op een bepaalde manier gecontroleerd of we zijn wie we zeggen dat we zijn. Je wachtwoord moet eigenlijk even uniek (en complex) zijn als jij! Hier heb je een paar tips:

- **DOEN: lange wachtwoorden en -zinnen gebruiken.** Wachtwoorden moeten ten minste 12 tekens bevatten maar ook weer niet zo lang zijn dat je ze niet kunt onthouden (zie de tip hieronder). Controleer of je wachtwoord betrokken is geweest bij een datalek op `https://haveibeenpwned.com/Passwords`. Nog beter is het gebruik maken van een wachtwoordkluis. Daarmee maak je elk wachtwoord uniek zonder deze te hoeven onthouden.
- **DOEN: unieke zinnen en bijzondere tekens gebruiken.** Een korte zin van 30 of meer tekens (eventueel met een paar nummers, hoofdletters en leestekens) die je kan onthouden is veel beter dan een woord van 12 letters met codes die iedereen toepast (bijvoorbeeld een "3" voor de letter "e").
- **DOEN: een (gratis of betaald) programma gebruiken om je wachtwoorden te beheren.** Een wachtwoordbeheerprogramma kan nuttig zijn voor het aanmaken, opslaan, beheren en onthouden van unieke, sterke wachtwoorden voor je verschillende apparaten, systemen en applicaties. Je hoeft je wachtwoorden dan ook niet meer op te schrijven in documenten of op post-its, iets dat veel mensen doen.
- **DOEN: Gebruikmaken van multi-factor-authenticatie (MFA).** Indien dat mogelijk is, moet je in plaats van of in aanvulling op je wachtwoorden MFA inschakelen op je accounts. MFA maakt gebruik

(vervolgd)

(vervolgd)

van twee of meer authenticatiefactoren ("iets dat je weet", zoals je gebruikersnaam en/of wachtwoord, en "iets dat je hebt", zoals een hardware- of softwaretoken of een smartphone). Als je inlogt op een MFA-account, wordt er een eenmalige code op je token gegenereerd of via een sms naar je smartphone gestuurd. Deze code kan maar één keer worden gebruikt en moet binnen een bepaalde tijd worden gebruikt (meestal binnen één tot vijf minuten). Zo wordt het buitengewoon moeilijk voor een hacker om je code te onderscheppen en te gebruiken om in te loggen op je account zonder dat jij dat weet en voordat de code verloopt.

- **Gebruik NIET twee keer hetzelfde wachtwoord, hoe goed het ook is.** Als je wachtwoord op één plek wordt gehackt (bijvoorbeeld je persoonlijke Yahoo!-account) zullen cybercriminelen proberen dezelfde inloggegevens te gebruiken op andere plekken (bijv. voor je internetbankieren).
- **Deel je wachtwoord NIET met anderen.** Nooit! Je wachtwoord is nog persoonlijker dan je tandenborstel (die je misschien nog wel eens deelt met je partner of - wie weet - je hond).
- **Gebruik GEEN gebruikelijke woorden die in het woordenboek staan.** Programma's die wachtwoorden automatisch kraken, hebben woordenboeken zo gescand. Woorden in andere talen en medische, juridische of technische termen zijn dus geen veilige optie. Vermijd ook het herhalen van tekens (bijvoorbeeld "aaaa"), opeenvolgende tekens (bijvoorbeeld "1234") en herkenbare patronen (bijvoorbeeld "qwerty").
- **Gebruik GEEN persoonlijke gegevens in je wachtwoorden.** Dankzij sociale media is het voor cybercriminelen gemakkelijker dan ooit om persoonlijke dingen over je te weten te komen. Denk hierbij bijvoorbeeld aan je doopnaam, geboortedatum, adres, school, de naam van je echtgenoot of kind en wat je afgelopen zomer hebt gedaan!

Woordenlijst

adware: Programma's voor pop-up-reclame die meestal worden geïnstalleerd met freeware of shareware en in sommige gevallen kunnen worden aangemerkt als malware. *Zie ook* malware.

Algemene verordening gegevensbescherming (AVG): Van toepassing op alle organisaties die zakendoen met EU-burgers. Verhoogt de bescherming van de gegevens van EU-burgers en reguleert de export van persoonsgegevens naar landen buiten de EU.

backdoor: Malware die een aanvaller in staat stelt de normale authenticatie te omzeilen om toegang te krijgen tot een gecompromitteerd systeem. *Zie ook* malware.

beschermde gezondheidsinformatie: Informatie over de gezondheid, verstrekking van gezondheidszorg of betaling voor gezondheidszorg die wordt aangemaakt of verzameld door een organisatie, bijvoorbeeld een zorgaanbieder, verzekeringsmaatschappij of andere entiteit, en kan worden gekoppeld aan een specifiek persoon.

bootkit: Een malware-variant van een rootkit op kernelniveau, veel gebruikt om computers aan te vallen waarvan de volledige harde schijf is beschermd door middel van versleuteling. *Zie ook* malware *en* rootkit.

bot: Een doelwitcomputer die is besmet met malware en deel uitmaakt van een botnet. *Zie ook* botnet *en* malware.

botnet: Een breed netwerk van met malware besmette bots die samenwerken en worden aangestuurd door een aanvaller via command-and-control (C2)-servers. *Zie ook* bot *en* malware.

Bring Your Own Device (BYOD): Een beleid dat medewerkers toestaat hun eigen mobiele apparaten, zoals smartphones en tablets, mee te nemen naar het werk voor zowel werkgerelateerde als persoonlijke doeleinden.

ciphertext: Een bericht met klare tekst dat is versleuteld in een gecodeerd bericht dat onleesbaar is zonder de juiste decryptiesleutel. *Zie ook* decodering, versleuteling *en* klare tekst.

cryptovaluta: Een digitale activa dat cryptografie gebruikt om transacties te beveiligen, de aanmaak van aanvullende eenheden te beheersen en de overdracht van activa te verifiëren. Bitcoin is een populair voorbeeld van een cryptovaluta.

decodering/decryptie: Het proces om ciphertext om te zetten in klare tekst. *Zie ook* ciphertext *en* klare tekst.

directory harvest attack (DHA): Een "brute force"-techniek die wordt gebruikt door spammers in een poging om geldige e-mailadressen te vinden in een domein.

distributed denial-of-service (DDoS): Een aanval op grote schaal waarbij meestal bots in een botnet worden gebruikt om het netwerk of de server die het doelwit is te vernietigen. *Zie ook* bot *en* botnet.

DNS cache poisoning: Een soort aanval, ook wel DNS spoofing genoemd, waarbij de zwakke plekken van een DNS worden benut om internetverkeer weg te leiden van de bestemmingsservers naar valse servers. *Zie ook* domeinnaamsysteem (DNS).

DNS-kaping: Een aanvalstechniek die wordt gebruikt om DNS-verzoeken weg te leiden van legitieme DNS-servers. *Zie ook* domeinnaamsysteem (DNS).

domeinnaamsysteem (DNS): Een gedecentraliseerde, hiërarchische database voor computers, diensten en andere middelen die zijn verbonden met een netwerk of het internet die numerieke IP-adressen, evenals andere informatie, indeelt in domeinnamen. *Zie ook* internetprotocol (IP).

drive-by-download: Software, vaak malware, die op een computer wordt gedownload vanaf het internet zonder kennis of toestemming van de gebruiker. *Zie ook* malware.

endpoint: Een computer van een eindgebruiker, bijvoorbeeld een desktop, laptop, tablet of smartphone.

exploit: Software en code die, door misbruik te maken van de zwakke plekken van een besturingssysteem (OS) of toepassing, ongewenst gedrag veroorzaakt in de OS of in de toepassing, zoals het escaleren van privileges, besturing op afstand of een denial-of-service.

Health Insurance Portability and Accountability Act (HIPAA): Van toepassing op elke organisatie die beschermde gezondheidsinformatie verwerkt of opslaat. Waarborgt de vertrouwelijkheid van patiëntgegevens en gegevensprivacy.

Internationale Organisatie voor normalisatie (ISO): Internationaal orgaan voor de ontwikkeling van normen. ISO wordt afgeleid van het Griekse woord "isos", wat "gelijk" betekent.

internetprotocol (IP): Het belangrijkste communicatieprotocol in de TCP/IP-communicatiereeks voor routing buiten de grenzen van netwerken (routers) en het internet. *Zie ook* Transmission Control Protocol (TCP).

klare tekst: Een bericht in het oorspronkelijke, leesbare formaat of een ciphertext-bericht dat naar behoren is gedecodeerd om het oorspronkelijke, leesbare bericht te produceren. *Zie ook* ciphertext *en* decodering/decryptie.

kwetsbaarheid, zwakke plek: Een bug of tekortkoming in de software die leidt tot een beveiligingsrisico dat kan worden benut door een aanvaller. *Zie ook* exploit.

logic bomb: Een malware-programma, of een deel daarvan, dat is ontworpen om schade aan te richten wanneer een vooraf bepaalde situatie zich voordoet. *Zie ook* malware.

malware: Malafide software of code die een computersysteem meestal schaadt, uitschakelt, de controle erover overneemt of er informatie uit steelt. Onder malware vallen onder meer virussen, wormen, Trojaanse paarden, logic bombs, ransomware, rootkits, bootkits, backdoors, spyware en adware.

metamorfisme: Een techniek die wordt gebruikt om malwarecode telkens te herschrijven, zodat elke nieuwe versie anders is dan de voorgaande. *Zie ook* malware *en* polymetamorfisme.

next-generation firewall (NGFW): Een platform voor netwerkbeveiliging dat traditionele firewalls en functies om netwerkinbraken te voorkomen combineert met andere geavanceerde beveiligingsfuncties die deep packet inspection (DPI) mogelijk maken voor volledige zichtbaarheid, een nauwkeurige identificatie van toepassingen, content en gebruikers en granulaire controle op basis van beleid. *Zie ook* systeem voor de preventie van inbraken (IPS).

normen van gegevensbescherming voor de betaalkaartenbranche (PCI-DSS): Van toepassing op alle bedrijven die transacties met passen (zoals creditcards, debetkaarten en betaalkaarten) accepteren, verwerken en opslaan.

Personal Information Protection and Electronic Documents Act (PIPEDA): Geldt voor alle organisaties die zakendoen met Canadese burgers. Beschermt de privacy en persoonsgegevens van Canadese burgers.

phishing: Een sociale engineering-techniek waarbij met een e-mail die van een legitiem bedrijf (bijvoorbeeld een financiële instelling) afkomstig lijkt te zijn, wordt geprobeerd de ontvanger over te halen te klikken op een ingebedde link in de e-mail of een bijlage te openen waarin malware of een exploit zit. De ingebedde link leidt de browser van de ontvanger naar een malafide website om daar gevoelige persoonsgegevens (bijvoorbeeld rekeninginformatie) in te vullen. Ook kan de malafide website op de achtergrond via de browser malware of een exploit plaatsen op het endpoint van de gebruiker. *Zie ook* drive-by-download, endpoint, exploit, *en* malware.

polymorfisme: Een techniek die wordt gebruikt om een deel van malwarecode telkens te herschrijven, zodat elke nieuwe versie net iets anders is dan de voorgaande. *Zie ook* malware *en* metamorfisme.

port hopping: Een techniek die door toepassingen wordt gebruikt om de toegankelijkheid te verbeteren, maar ook in cyberaanvallen om dynamisch te schakelen tussen TCP-poorten om detectie te voorkomen. *Zie ook* Transmission Control Protocol (TCP).

ransomware: Malafide software die de gegevens van een slachtoffer versleutelt en een bepaald bedrag aan losgeld (meestal in cryptovaluta) eist om de gegevens te decoderen (al garandeert de betaling van het losgeld niet dat de gegevens van het slachtoffer ook daadwerkelijk zullen worden gedecodeerd). *Zie ook* cryptovaluta *en* malware.

remote access Trojan (RAT): Een malware-programma dat een backdoor bevat om het beheer van een doelwitcomputer over te nemen.

rootkit: Malware die toegang verschaft tot een computer met privileges (op root-niveau). *Zie ook* malware.

Transport Layer Security (TLS): wordt voornamelijk gebruikt in situaties waarin het nodig is te verifiëren of men inderdaad verbonden is met de gewenste server. Met name in bancaire toepassingen

(internetbankieren) of communicatie met de overheid is dit van groot belang, aangezien vaak financiële belangen in het spel zijn, of persoonlijke of anderszins vertrouwelijke informatie wordt uitgewisseld.

social engineering: Een technisch eenvoudige aanvalsmethode waarbij technieken als shoulder surfing (over de schouder meekijken) en dumpster diving (zoeken in de vuilnisbak) worden toegepast om gevoelige informatie, zoals wachtwoorden, van een gebruiker te achterhalen.

spam: Massaal ongevraagd verzonden e-mails die vaak worden gebruikt om malware te verspreiden via malafide links of bijlagen. *Zie ook* malware.

spearphishing: Een gerichte phishing-poging die geloofwaardiger lijkt voor slachtoffers en daarom een grotere kans heeft om te slagen. Een spearphishing-e-mail kan bijvoorbeeld de indruk wekken afkomstig te zijn van een organisatie of persoon die de ontvanger kent. *Zie ook* phishing.

spyware: Malware waarmee informatie wordt verzameld over een persoon of organisatie zonder zijn of haar kennis of toestemming. *Zie ook* malware.

SSL-verhulling: Een techniek waarbij gebruik wordt gemaakt van SSL (Secure Sockets Layer)-versleuteling om de inhoud van netwerkverkeer te verhullen, bijvoorbeeld om detectie door netwerkbeveiliging te voorkomen bij het stelen van gevoelige gegevens (ook wel gegevensexfiltratie genoemd).

systeem voor de detectie van inbraken (IDS): Een hardware- of softwaretoepassing die verdachte inbraken op netwerken of hosts detecteert.

systeem voor de preventie van inbraken (IPS): Een hardware- of softwaretoepassing die verdachte inbraken op netwerken of hosts detecteert en blokkeert.

Transmission Control Protocol (TCP): Een van de belangrijkste protocollen uit de Internet Protocol-reeks. TCP is een van de twee oorspronkelijke componenten van de reeks en vormt een aanvulling op het internetprotocol (IP). Daarom wordt naar de gehele reeks vaak verwezen als TCP/IP-reeks. TCP maakt de betrouwbare, geordende aflevering mogelijk van een stroom bytes van een programma op een computer naar een ander programma op een andere computer.

TCP is het protocol waarop belangrijke internettoepassingen, zoals het World Wide Web, e-mail, beheer op afstand en bestandsoverdracht zijn gebaseerd. *Zie ook* internetprotocol (IP).

Trojaans paard: Een malware-programma dat doet alsof het een bepaalde functie uitvoert, maar in plaats daarvan iets anders (meestal schadelijks) doet. *Zie ook* malware.

unified threat management (UTM): Een beveiligingstoepassing die op één platform verschillende beveiligingsfuncties combineert, zoals een firewall, anti-malware en preventie van inbraken.

Uniform Resource Locator (URL): Een webadres.

versleuteling (encryptie): Het proces om klare tekst om te zetten in ciphertext. *Zie ook* ciphertext *en* klare tekst.

virtual local area network (VLAN): Een broadcast-domein binnen een lokaal netwerk dat is gesegmenteerd en geïsoleerd.

virtueel privé-netwerk (VPN): Een privé-netwerk dat wordt gebruikt om privé te communiceren via publieke netwerken. VPN's maken gebruik van versleuteling en inkapseling om verbindingen te beschermen en vereenvoudigen.

virus: Een reeks computerinstructies die als doel heeft zich in te bedden in een ander computerprogramma om zichzelf te vermenigvuldigen. *Zie ook* malware.

web application firewall (WAF): Een firewall die is ontworpen om toepassingen en servers op het web te beschermen.

worm: Malware die meestal het vermogen heeft zich van de ene computer naar de andere te vermenigvuldigen zonder dat hiervoor menselijk handelen nodig is. *Zie ook* malware.

JE BEDRIJF WORDT GEVORMD DOOR JE GEGEVENS

ZORG ERVOOR DAT JE BEDRIJF BEVEILIGD IS TEGEN DATA-INBREUKEN OF -LEKKEN.
GEBRUIK DE KRACHTIGE, GEMAKKELIJK TOE TE PASSEN VERSLEUTELING VOOR EINDPUNTEN VAN ESET EN

- versleutel harde schijven, verwijderbare media, bestanden en e-mails veilig.
- Geef je informatiebeveiliging een boost en zorg ervoor dat je voldoet aan de Algemene verordening gegevensbescherming van de EU.
- Voeg een extra beveiligingslaag toe met ESET Secure Authentication.

BEZOEK DE WEBSITE VAN ESET VOOR ALLE OPLOSSINGEN.

eset ENJOY SAFER TECHNOLOGY™

WWW.ESET.COM

Houd de gegevens van je bedrijf veilig en zorg dat ze kunnen worden hersteld

Recente datalekken en aanvallen hebben laten zien dat betrouwbare gegevensbescherming voor kleine bedrijven net zo belangrijk is als voor grote ondernemingen. Gegevensbescherming *voor Dummies* is je essentiële handleiding om de juiste technologie voor gegevensbescherming en organisatorische maatregelen te kiezen voor jouw bedrijf, of je nu een eenmanszaak bent of er 250 mensen bij je in dienst zijn. Lees het boek en kom van alles te weten over de beveiligingstechnologieën, hulpmiddelen en processen die je nodig hebt om je bedrijf beter in staat te stellen zijn gegevens en IT-middelen te beschermen en het effect van een datalek effectief tot een minimum te beperken.

Binnenin ...

- Begrijp alle consequenties van een cyberaanval
- Evalueer verschillende IT-beveiligingstechnologieën, toepassingsopties en servicemodellen voor kleine en middelgrote bedrijven
- Ontdek hoe effectieve gegevensbescherming je bedrijf helpt aan de regels te voldoen
- Ontdek wat de waarde van effectieve gegevensbescherming voor je bedrijf is

Ga naar Dummies.com®
voor video's, stapsgewijze instructies aan de hand van foto's, artikelen met uitleg of om producten aan te schaffen!

ISBN: 978-1-119-54774-7
Niet voor wederverkoop

voor dummies®

Ook beschikbaar als e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.