INFOZINE OVER DE BESCHERMING VAN DIGITALE GEGEVENS

CYBER- EN DATARISICO'S

AANGEBODEN DOOR

Froonacker Van de Witte
assurantiën - risicobeheer

Van der Veen & Kromhout
registeraccountants • belastingadviseurs

CYBER- EN DATARISICO'S

COLOFON

Het magazine Cyber- en Datarisico's
is een eenmalige uitgave
van Froonacker Van de Witte
Assurantiën en Van der Veen &
Kromhout Registeraccountants en
Belastingadviseurs

Froonacker Van de Witte Assurantiën
0517 399 999
info@frovdw.nl

Van der Veen & Kromhout
Registeraccountants en
Belastingadviseurs
Drachten: 0512 584 800
drachten@kromhout.com

Gorredijk: 0513 468 468
gorredijk@kromhout.com

Joure: 0513 480 480
joure@kromhout.com

Redactie,
vormgeving & productie
VRHL Content en Creatie
Alphen aan den Rijn

Fotografie
Marco Hamoen

Drukwerk
Okay Color Graphics,
Alphen aan den Rijn

Met dank aan
Anne Bergsma, Jan Verheul, Marco Beentjes, Manon Louwers, Nart Wielaard, Douwe Bergsma, Rolf Rudolphy, Reynold Bontes, Carine Harting, Ronald Bruins, Aleid Wolfsen (Autoriteit Persoonsgegevens), Bernard Goede en Gaby de Wijs (Chubb European Group Limited), Enrico Bianchi en Stefan Zwager (AIG Europe, Netherlands), Loek Hermans, Betty Hoogsteen en Enno Wiertsema (Adfiz)

Copyright/disclaimer © 2017
Zet- en drukfouten voorbehouden. Niets uit deze uitgave mag zonder voorafgaande schriftelijke toestemming van de uitgevers verveelvoudigd of openbaar worden gemaakt. Bij het samenstellen van dit magazine is de grootste zorg besteed aan de juistheid van de hierin opgenomen informatie. De uitgevers zijn niet verantwoordelijk voor enige onjuist verstrekte informatie in dit magazine

INHOUD

VOORWOORD

In mei 2018 treedt de Algemene verordening gegevensbescherming (AVG) in werking en dat heeft grote gevolgen, ook voor u. Alle bestuurders van bedrijven en instellingen zullen zich nóg bewuster moeten zijn van de gegevens die zij bezitten. De makers van dit magazine willen daarbij ondersteunen, allereerst door informatie te verstrekken over de veranderingen die u kunt verwachten. Froonacker Van de Witte Assurantiën en Van der Veen & Kromhout Registeraccountants en Belastingadviseurs hebben samengewerkt om het onderwerp cyber- en datarisico's vanuit verschillende perspectieven te belichten. Daarnaast leest u in dit magazine verhalen van slachtoffers van cybercriminelen, een interview met de voorzitter van de Autoriteit Persoonsgegevens en een interessant betoog over data.

“Update, update, update & IT-audits!”

Inbraak en diefstal zijn van alle tijden. Alleen de wijze waarop dit gebeurt en het soort personen dat achter deze - vaak ingrijpende - inbreuk op de privacy zit, zijn in de loop van de eeuwen aan veranderingen onderhevig.

DUIDELIJKE TAAL

Drs. Douwe Bergsma RA is privacy officer en directeur van Van der Veen & Kromhout Registeraccountants en Belastingadviseurs. "Vanuit vestigingen in Gorredijk, Drachten en Joure werkt Van der Veen & Kromhout met enthousiaste professionals die houden van duidelijke taal en scherpe analyses. Met een nuchtere aanpak en nauwe betrokkenheid helpen onze vakmensen u graag verder. Want wij snappen best dat u zich bezig wilt houden met wat u het allerliefst doet: ondernemen. U onderneemt, onze adviseurs doen de rest."

Neem contact op met Douwe Bergsma via dbergsma@kromhout.com of 0513 480 480.

www.kromhout.com

Van der Veen & Kromhout
registeraccountants • belastingadviseurs

Bedrijven hebben hun productiviteit en efficiency binnen met name de administratieve processen in de afgelopen jaren flink verhoogd, door steeds verdergaande automatisering en daarmee samenhangende digitalisering. Veel data kan simpel worden vastgelegd en gedeeld, zowel in 'interne' als 'externe' clouds. Door de digitalisering van bedrijfsprocessen in de achterliggende periode zijn de mogelijkheden van inbraak en diefstal in korte tijd zeer snel en ingrijpend gewijzigd. Ten opzichte van het analoge tijdperk is althans een geheel nieuwe wijze van inbraak en diefstal mogelijk geworden.

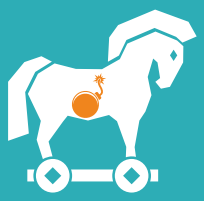
BESCHERMING DATA STEEDS BELANGRIJKER

Deze cybercriminaliteit vormt thans, maar zeker ook de komende jaren, een groot probleem voor vele bedrijven en instellingen. Maar ook particulieren zullen hieraan niet ontkomen. Met de invoering van de General Data Protection Regulation (GDPR) heeft de Europese Unie privacy-verhogende regelgeving ingevoerd (per 25 mei 2018 van kracht), met als doel (persoons)gegevens en andere privacygevoelige informatie te beschermen. De Nederlandse vertaling luidt Algemene verordening gegevensbescherming (AVG). Eerder is reeds de Wet meldplicht datalekken ingevoerd (1 januari 2016). Een zeer zorgvuldige en adequate bescherming van persoonsgegevens is derhalve een must.

PREVENTIEVE MAATREGELEN

De noodzaak voor instellingen en bedrijven is niet alleen om aan de huidige en toekomstige wet- en regelgeving te kunnen voldoen en daarmee eventueel hoge boetes te voorkomen; de imago- en reputatie-

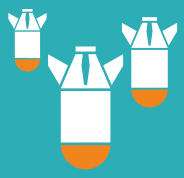
"Ransom- en andere malware maken vaak gebruik van lekken in verouderde software"



TROJAN
Is vermomd als een nuttig programma. Bevat voor hackers een toegangspoort om gegevens te bewerken, kopiëren of zelfs verwijderen.

RANSOMWARE
Kaapt hardware door data te blokkeren. Het slachtoffer moet een geldbedrag betalen om van de blokkade af te komen.

PHISHING
Hengelen naar vertrouwelijke informatie via e-mail en via de telefoon, ogenschijnlijk vanuit betrouwbare organisaties.



DDoS-AANVAL
Distributed Denial of Service. Maakt een website of internetdienst onbruikbaar door overbelasting van de server.

SPYWARE
Vergaart informatie over een computergebruiker en stuurt deze door naar een externe partij.

MALWARE
Alle software met een opzettelijk kwaadaardige werking. Ook vaak virus genoemd.

schade kunnen wel eens tot nog veel grotere financiële gevolgschade leiden voor hen die onzorgvuldig met persoonsgegevens omgaan. En in het ergste geval zelfs tot een continuïteitsprobleem leiden.

"Een zeer belangrijke - en in de basis ook redelijk simpel uit te voeren - maatregel om datalekken te voorkomen betreft het up-to-date houden van de in gebruik zijnde software(applicaties)", vertelt drs. Douwe Bergsma, privacy officer en directeur van Van der Veen & Kromhout Registeraccountants en Belastingadviseurs. "Procedures binnen een organisatie om tijdig updates uit te voeren, en dit te bewaken, zijn daarbij essentieel. Ransom- en andere malware maken veel gebruik van lekken in verouderde software, dus middels structurele vernieuwing kan veel ellende worden voorkomen. Bij deze procedures zijn ook instructies voor sterke wachtwoorden zeer aan te bevelen."

PERIODIEK BEOORDELEN

Daarnaast adviseert hij bedrijven en instellingen om regelmatig een IT-audit uit te voeren; een vakgebied dat zich bezighoudt met het beoordelen van de automatisering van de organisatie en de organisatie van de automatisering. "IT-auditing is een specialisme binnen het auditing-vakgebied, en wordt meer en meer gevraagd bij de uitvoering van accountantscontroles. Door middel van het laten uitvoeren van een IT-audit kan zekerheid (assurance) worden verkregen in welke mate de IT-omgeving voldoet aan de daaraan te stellen eisen, zowel qua continuïteit en kwaliteit van vitale bedrijfsprocessen, als ten aanzien van de eisen die tegenwoordig worden gesteld aan IT-governance (goed ondernemingsbestuur) en compliance (voldoen aan wet- en regelgeving)."

"Voorkomen is beter dan genezen!"

Tot slot is het zorgdragen van adequate back-up procedures uiteraard een must voor elke organisatie. Het voorkomen van dataverlies dient zowel vanuit privacy als bedrijfseconomisch oogpunt een zeer hoge prioriteit te krijgen. Teneinde de financiële schade zoveel mogelijk te beperken is het uiteraard van groot belang dat men snel over een juiste en volledige back-up van verloren en of gehackte gegevens kan beschikken.

https://www.kromhout.com/diensten/automatiseringsadvies

Voorkomen is beter dan genezen: is uw organisatie al cyberproof?

Handig is het wel, alles digitaal. Het maakt veel werkzaamheden een stuk makkelijker en bespaart ondernemingen veel tijd en geld. Maar de digitalisering brengt ook de nodige cyberrisico's met zich mee. Virussen en cyberaanvallen kunnen uw onderneming letterlijk gijzelen. De gevolgen van zo'n aanval zijn vaak aangrijpend en de oplossing is tijdrovend. Onder het motto 'voorkomen is beter dan genezen' willen wij bij Van der Veen en Kromhout onze klanten wapenen tegen cyberaanvallen. Met onze IT-audits helpen we u met het identificeren en reduceren deze risico's.

Onderschat de cyberrisico's niet! Is uw organisatie al cyber-proof?

Wij adviseren u graag!

Bekijk ook onze overige diensten!
Ga naar www.kromhout.com

Van der Veen & Kromhout
registeraccountants • belastingadviseurs

Reynold Bontes (adviseur zakelijk risicobeheer en verzekeringen) en Anne Bergsma (directeur en Registermakelaar in Assurantiën) van Froonacker Van de Witte

LEK

Bestuurders van bedrijven en instellingen: actie is vereist voor verantwoord risicobeheer

Data is geld waard. Veel geld. Niet voor niets maakte BMW afgelopen juni als eerste autofabrikant bekend hun 'car-data' actief te gaan vermarkten. Maar er is ook een keerzijde. Kwaadwillende hackers verdienen aan de schemerzijde van het internet kapitalen door vertrouwelijke informatie te verkopen op de zwarte markt. Of door fraude te plegen met gestolen BSN-nummers. De gevolgschade voor gehackte bedrijven is groot en kan al gauw oplopen tot enkele tonnen of meer. Het gaat bovendien niet alleen om cybercrime; de schade van een datalek door onzorgvuldigheid kan even groot zijn. Experts roepen op tot een actieve houding en verantwoord risicobeheer.

SPECIALIST IN CYBER- & DATARISICO'S

Een goede adviseur zal – rekening houdend met het risicogebied van de organisatie – een passende Cyber & Data Risks verzekering aanbieden. Froonacker Van de Witte neemt cyberrisico's inhoudelijk nadrukkelijk mee tijdens haar reguliere gesprekken met zakelijke klanten.
Het assurantiebedrijf organiseert tevens bijeenkomsten, waarbij dieper wordt ingegaan op de cyberrisico's en bescherming voor het mkb. Daarnaast organiseert Froonacker Van de Witte 'cybergames' en -lezingen om ondernemers en medewerkers spelenderwijs bewust te maken van hetgeen er op hen afkomt in geval van een datalek of cyberaanval.

0517 399 999
r.bontes@frovdw.nl

www.frovdw.nl

Froonacker Van de Witte
assurantiën - risicobeheer

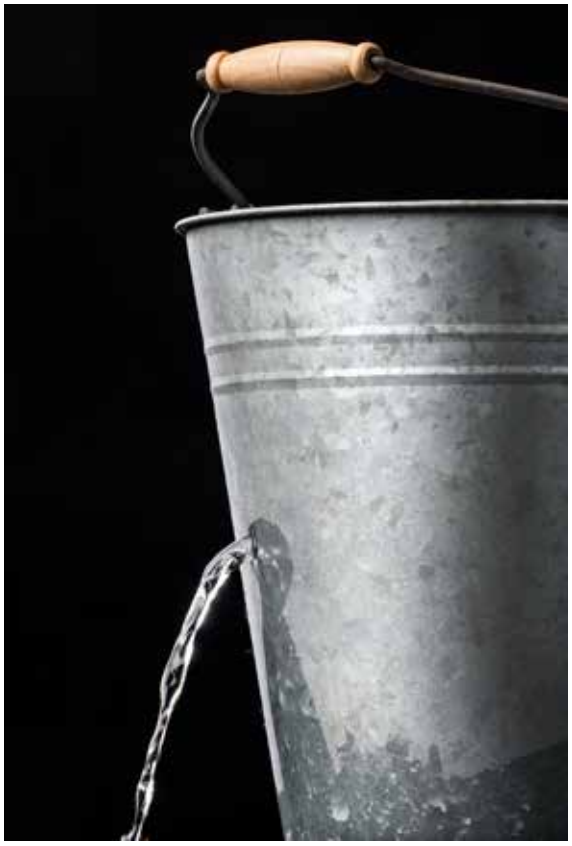
Het bleek al in 2015 na onderzoek in opdracht van Ernst & Young: alleen een actieve houding van het bedrijfsleven kan de toenemende internetcriminaliteit voldoende weerstand bieden. Inmiddels experimenteert TNO in het recent geopende Cyber Threat Intelligence Lab met nieuwe technologieën. Aansluitend heeft de overheid de regelgeving verscherpt om u – als potentieel doelwit – te motiveren ook zelf technische en organisatorische maatregelen te nemen.

"Dat betekent niet dat ondernemers wakker hoeven te liggen van mogelijke aansprakelijkheidsclaims in geval van een datalek, of van het bedrag dat door criminelen wordt geëist in geval van ransomware", stelt Reynold Bontes, adviseur zakelijk risicobeheer en verzekeringen van Froonacker Van de Witte. "Wat ondernemers zich moeten realiseren is dat er een ongelofelijke hoeveelheid verplichtingen op hen af komt wanneer zij slachtoffer worden van datalekkage of cybercriminaliteit. Wanneer namelijk blijkt dat zij onvoldoende voorbereid waren, worden ze een prooi van de Autoriteit Persoonsgegevens met kans op hoge boetes. Maar wanneer zij via een protocol hebben vastgelegd wat te doen in die gevallen, wordt de schade zoveel mogelijk beperkt."

HET PROTOCOL

Een kijkje in het handboek van gespecialiseerde adviseurs geeft helderheid in wat ondernemers bij een datalek te doen staat. Bedrijven en instellingen moeten - samen met hun adviseur - een protocol opstellen waarmee iedereen binnen hun organisatie weet wat er van hem of haar wordt verwacht. Wanneer er een datalek of hack heeft plaatsgevonden, dan komt er nogal wat bij kijken. Allereerst moet u identificeren wat er precies is gebeurd. Mogelijk moet u specialisten inhuren

"Door een protocol klaar te hebben wordt de schade zoveel mogelijk beperkt"



"Risico's die je niet kunt dragen moet je verzekeren"

om te helpen problemen te ontcijferen en systemen weer bruikbaar te maken. Vervolgens moet worden uitgezocht wiens privacygevoelige informatie is gelekt: deze personen moeten worden geïnformeerd. Reputatie is hierin ook belangrijk: partijen zullen naar u wijzen wanneer door u gelekte informatie op verkeerde plekken opduikt. Een goed communicatiebureau kan dat managen. In geval van ransomware ligt de overweging voor de hand om de criminelen dan maar te betalen, maar Reynold Bontes adviseert ondernemers om hier vanaf te zien. "De kans is groot dat je binnen afzienbare tijd opnieuw aan de beurt bent en de privacywetgeving is daar niet van gediend. Het is beter om een nieuw computersysteem in werking te stellen en via back-ups te proberen om informatie terug te krijgen."

VERANTWOORD RISICOBEHEER

Een netwerk van financiële, juridische en technische specialisten kan de impact voor uw bedrijf verkleinen. Het grootste deel van de te maken kosten ligt bij een datalek of een hack aan de kant van de dienstverlening van alle partijen die u moet inschakelen om de schade te beheersen. Naast deze kosten kunnen de kosten van bedrijfsstilstand ook fors oplopen. Wanneer een week lang alle medewerkers niet declarabel zijn, dan gaat het om forse bedragen. En dan is het nog maar hopen dat alle dossiers weer helemaal hersteld kunnen worden. Tot slot loopt u nog het risico dat een Autoriteit Persoonsgegevens een boete oplegt of dat een benadeelde, wiens gegevens gelekt zijn, u aansprakelijk stelt.

Een goede verzekering dekt veel kosten. Het dekt niet de buikpijn, de onzekerheid en stress in de organisatie en voorkomt niet dat er waarschijnlijk een litteken zichtbaar blijft. Het voorkomt wel dat de schade groter wordt dan die al was en voorkomt een groot financieel verlies.

Met de vier V's van verantwoord risicobeheer kan een goede verzekeringsadviseur ondernemers helpen om deze digitale risico's op de juiste wijze te beoordelen:

1. Sommige problemen kun je Voorkomen
2. Je kunt de kans Verlagen, dan wel de impact verminderen
3. Sommige zaken kan je Verdragen, bijvoorbeeld in de vorm van een eigen risico
4. Risico's die je niet kunt dragen moet je Verzekeren

Volgens de verzekeringsspecialist draait het allemaal om bewuste keuzes maken. Welke risico's kan ik vermijden, welke accepteer ik en welke houd ik buiten mijn bedrijf door ze te verzekeren? "Ik begrijp dat een ondernemer of bestuurder vaak andere interesses heeft", aldus Reynold Bontes. "Zolang je je maar door experts laat voorlichten om daar vervolgens zelf een bewuste keuze in te maken. Dan ben je voldoende actief om effectief cyberrisico's of de gevolgen daarvan uit je organisatie te weren."

Sjoerd en Arjan. Typisch ondernemers met een nine-to-five mentaliteit.

van BOEKHOUT KROMHOUT

Nieuw! Slim boekhouden met een betrouwbare online totaaloplossing

Da's lekker... tijd overhouden voor een potje tennis met je vrienden. Hoe doe je dat? Met Boekhout van Kromhout. Deze slimme online oplossing van Van der Veen & Kromhout geeft 24/7 inzicht in de prestaties van uw bedrijf. U bent altijd in control en de tijdrovende administratie behoort tot het verleden. Zo kunt u de kostbare uren na vijven besteden zoals u zelf wilt: aan uw relatie, uw kinderen, uw hobby, uw sport of om nieuwe ondernemingsplannen uit te werken.

- Het gemak van een grotendeels geautomatiseerde administratie
- Overal en altijd inzicht in actuele cijfers
- Betrouwbare sturingsinformatie in één muisklik
- Altijd het advies van uw accountant bij de hand
- Tijd overhouden voor zaken die er écht toe doen

Ontdek hoeveel tijd u kunt besparen!
Ga naar www.boekhoutvankromhout.com

Van der Veen & Kromhout
registeraccountants • belastingadviseurs

ALGEMENE VERORDENING GEGEVENSBESCHERMING:

ÓÓK VOOR HET MKB!

Autoriteit Persoonsgegevens helpt bedrijven op weg

In 1995 waren de eerste veranderingen in het mediagebruik al merkbaar. Vijf jaar daarvoor was het World Wide Web geïntroduceerd en inmiddels deden ook de eerste webwinkels en zoekmachines hun intrede. Bovendien nam de internationale handel toe. (Persoons)gegevens werden gedeeld tussen internationale bedrijven, reisorganisaties en andere organisaties die wereldwijd opereerden. Op dat punt ontstond de behoefte om de privacy van personen beter te waarborgen. 1995 was daarom het jaar dat de Europese privacyrichtlijn werd geïntroduceerd. Vanaf dat moment zouden alle Europese landen hun privacywetgeving in grote lijnen op dezelfde manier geregeld hebben.

In Nederland resulteerde dat in 2001 in de intrede van de Wet bescherming persoonsgegevens (Wbp). Het College Bescherming Persoonsgegevens (CBP) zag er sindsdien op toe dat de wet werd nageleefd. Maar de digitalisering zette door, waardoor bedrijven en overheden steeds meer persoonsgegevens tot hun beschikking kregen. De angst ontstond dat daarmee ook hun macht groeide. Viviane Reding, destijds Europees Commissaris, stelde voor dat de Europese Privacyrichtlijn niet langer een richtlijn zou zijn, maar een verordening met directe werking voor alle lidstaten. In het voorjaar van 2016 bereikte de Europese Commissie een akkoord: de Algemene verordening gegevensbescherming (AVG) is een feit en treedt op 25 mei 2018 in werking. De Autoriteit Persoonsgegevens (AP), voorheen het CBP, ziet in Nederland toe op de naleving van de AVG. Aleid Wolfsen is de voorzitter. Hij vertelt over de concrete veranderingen, over de rol van de AP en over wat het mkb te wachten staat.

"We zijn niet uit op zo veel mogelijk boetes"

AUTORITEIT PERSOONSGEGEVENS

Aleid Wolfsen is sinds 1 augustus 2016 voorzitter van de Autoriteit Persoonsgegevens. Daarvoor was hij onder meer rechter in Amsterdam, vice-president van de rechtbank Haarlem, Tweede Kamerlid voor de PvdA en burgemeester van Utrecht.

"Welkom123 als wachtwoord, het ontbreken van encryptie, USB-sticks die rondslingeren, ontgrendelde computers terwijl een klant meekijkt en e-mails met gevoelige informatie die in de cc in plaats van de bcc naar een hele ontvangersgroep worden verstuurd. Slordigheid en onwetendheid vormen in de meeste gevallen de oorzaak van een datalek", vertelt de voorzitter van de AP Aleid Wolfsen. "Dat betekent niet dat iedere USB-stick in een kluis moet worden opgeborgen. Maar het betekent wel dat iedere organisatie zeker vanaf nu kritisch moet kijken naar de gegevens die hij in huis heeft."

PRIVACYVRIENDELIJK

De veranderingen in de wetgeving eisen van organisaties dat zij inzichtelijk maken welke gegevens zij verwerken en dat zij beoordelen hoe gevoelig die informatie is. Afhankelijk van de gevoeligheid, moeten ondernemers technische en organisatorische maatregelen treffen. Hoe gevoeliger de gegevens, hoe hoger

"Slordigheid en onwetendheid vormen meestal de oorzaak van een datalek"

de beveiligingseisen. Aleid Wolfsen: "Ik snap de vraag of dit ook voor mkb'ers geldt. Zij verwerken toch maar weinig gegevens? En hun klanten, waar ze vaak een goede relatie mee hebben, zullen heus geen melding maken als een datalek zich voordoet, zijn veelgehoorde argumenten. Maar de AVG geldt niet alleen voor grote multinationals. Want mkb'ers die bijvoorbeeld in de zorg werken, verwerken vaak (zeer) gevoelige gegevens. En ook kleinere bedrijven die apps beschikbaar stellen waarvoor gebruikers persoonlijke gegevens moeten achterlaten, moeten voorzichtig zijn. Je kunt niet zomaar van iedereen zijn gegevens vragen. En voor de persoonsgegevens die je vraagt en wellicht ook wel mág vragen, geldt dat in de algemene voorwaarden glashelder te lezen moet zijn waarvoor de gegevens worden gebruikt. Vervolgens moeten die gegevens worden beveiligd. Bovendien moet de software zelf privacyvriendelijk zijn, dus te allen tijden rekening houden met de privacyrechten van de gebruiker. De standaardinstellingen moeten privacyvriendelijk zijn ingericht. Wanneer je de gebruiker om toestemming vraagt, mag het hokje voor de zin 'Ja, ik geef toestemming' niet bij voorbaat al zijn aangevinkt. Het zijn allerlei zaken waar ook de mkb'er rekening mee moet houden."

VERSCHUIVING RECHTEN EN PLICHTEN

En eigenlijk moet dat nu ook al, vastleggen waarvoor je gegevens gebruikt en maatregelen treffen om een datalek te voorkomen. Op 1 januari 2016 voerde de Nederlandse overheid, anticiperend op de AVG, de Meldplicht datalekken in. Boetes kunnen nu al worden opgelegd. Maar vaak gaat een waarschuwing daaraan vooraf, mits er geen opzet in het spel is. Als je daarna je privacyzaken nog niet op orde hebt, krijg je pas een boete. Vanaf mei 2018 kun je die boete meteen krijgen en is die boete ook nog eens hoger: maximaal 20 miljoen euro of 4% van de wereldwijde omzet. Daarmee worden de bevoegdheden van de Europese privacyautoriteiten groter. Tegelijkertijd nemen de rechten van burgers toe. Voor hen wordt het straks bijvoorbeeld makkelijker om toestemming die zij hebben gegeven voor het gebruik van hun gegevens, ook weer in te trekken. Aan de andere kant wordt de verantwoordelijkheid van bedrijven juist groter; zij moeten actiever kunnen aantonen dat zij volgens de privacywetgeving werken.

AP ALS WAAKHOND

De AP bewaakt straks de naleving van de AVG. "Onze organisatie wordt groter en krijgt meer onderzoekmogelijkheden", verklaart Aleid Wolfsen. "We gaan niet alleen af op meldingen die we binnenkrijgen, maar gaan zelf ook actief op zoek naar organisaties die slordig omgaan met persoonsgegevens. Tegelijkertijd laten we bedrijven niet spartelen. We zijn niet uit op zo veel mogelijk boetes; het gaat ons erom dat zoveel mogelijk bedrijven de privacywet naleven. We hebben er dan ook alle belang bij om bedrijven op weg te helpen. Wat we nu al doen - adviseren over de nieuwe verordening - blijven we doen. Mijn advies aan mkb'ers is om u goed te laten informeren. Op de website van de AP (autoriteitpersoonsgegevens.nl) staan veel praktische tips. Klop ook aan bij uw brancheverenigingen, want met hen hebben we veel contact zodat ook zij het juiste advies kunnen geven."

"Actief op jacht naar organisaties die slordig omgaan met persoonsgegevens"

“30.000 EURO LOSGELD

of de data ligt op straat”

Bij een zorginstelling in het oosten van het land houden medewerkers zich dagelijks bezig met patiënten en de financiële administratie. De instelling heeft de beveiliging van het netwerk redelijk op orde en alle patiënt- en organisatorische gegevens goed afgeschermd. Tot die ene dag...

Toch geen ransomware?!
"Jawel, één muisklik was genoeg. Een medewerker ontving een e-mail met een link van een postbedrijf waarmee we veel werken. Tenminste, zo leek het. Want na een klik op de link verscheen direct de melding dat zekere bestanden waren versleuteld. Alleen de betaling van € 30.000 losgeld zou ons weer toegang geven tot onze bestanden. Betaalden we dit niet, dan lag de data op straat."

Wat deed u na deze melding?
"We zijn voor cybercriminaliteit verzekerd, dus we belden natuurlijk onmiddellijk het noodnummer. Een incident response manager bracht de situatie snel in kaart en schakelde vervolgens de juiste experts in, zoals forensisch onderzoekers en juridisch adviseurs. Die stellen onder meer vast wat er precies is gebeurd, om welk type data het gaat en wat de impact zou zijn als de gegevens worden verspreid. Het lijkt me duidelijk dat de persoonsgegevens van 10.000 patiënten niet op straat horen."

Moest u de deuren sluiten?
"Nee, gelukkig niet. Terwijl wij op de achtergrond met man en macht werkten om dit tot een goed einde te brengen, draaiden onze medewerkers gewoon door. Bepaalde informatie konden ze tijdelijk niet benaderen, maar dat heeft ons weinig tot geen schade opgeleverd."

Waarom niet gewoon het losgeld betalen?
"Dat heb ik ook voorgesteld. Laten we betalen, dan voorkomen we reputatieschade en zijn we ermee klaar. Maar de experts overtuigden mij ervan dat betalen geen garantie was voor het vrijgeven van de data. Ook bleef het alsnog verspreiden van de data door de hackers een reële optie. Daarbij komt dat de kern van het probleem de ransomware zelf is. Als het virus achterblijft, kan het eenvoudig weer worden geactiveerd."

Hoe is dit afgerond?
"We hebben een goed back-up systeem, dus de forensisch onderzoekers adviseerden om die data terug te zetten. Helaas bleef het risico op verspreiding bestaan. Hierop anticiperend is melding gemaakt bij de Autoriteit Persoonsgegevens (AP). Ook zijn alle betrokken patiënten geïnformeerd over dit incident. Het lijkt vreemd, omdat er op dat moment nog geen data waren gelekt. Toch kun je het beter melden. Stel dat een patiënt in de toekomst wordt geconfronteerd met identiteitsfraude en wij hebben het niet gemeld bij de AP... Dan kun je de tent wel sluiten! De hele gebeurtenis is een wijze les geweest. Onze medewerkers waren onvoldoende op de hoogte van mogelijke bedreigingen en hoe te handelen in geval van een calamiteit. Daarom hebben we geïnvesteerd in opleidingen. Ook het netwerk is nu extra beveiligd. We voeren regelmatig audits uit en scherpen de beveiliging aan als de actualiteit erom vraagt."

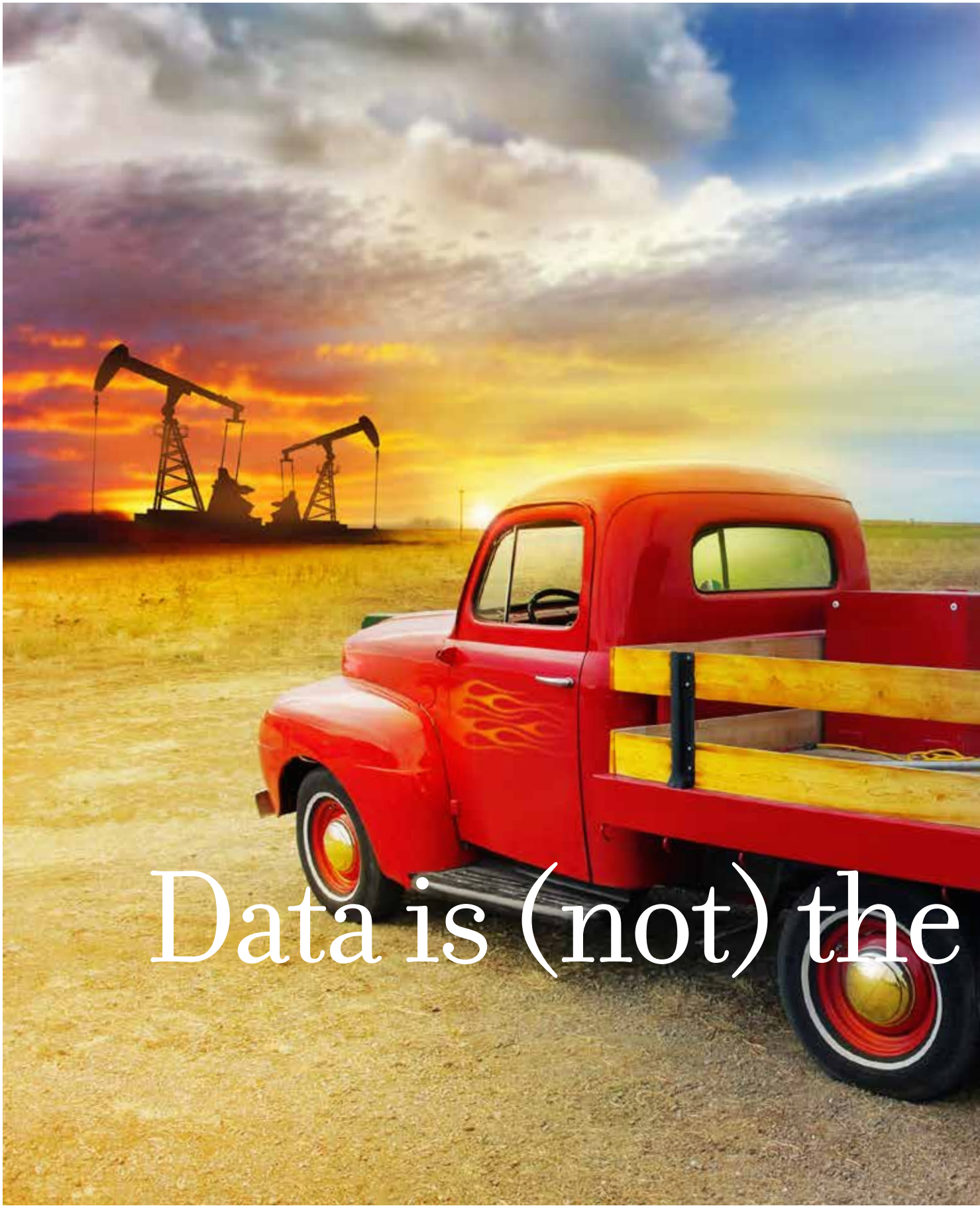
CHUBB EUROPEAN GROUP LIMITED

De zorginstelling was weliswaar bekend met de risico's van cybercriminaliteit, maar investeerde onvoldoende in IT-audits, beveiligingsprotocollen en opleiding van de medewerkers. Naast het hebben van een goed back-up systeem is het evenzo belangrijk om aandacht te besteden aan de veiligheidsrisico's op het gebied van personeel, beleid en procedures. De totale kosten voor dit incident bedroegen € 260.000 en zijn gedekt door de verzekering.

Chubb biedt een uitgebreide cyberverzekering met dekking van onder meer:

- Bedrijfsschade als gevolg van falende netwerkbeveiliging of een cyberaanval, menselijke fouten of programmeerfouten
- Dekking voor crisismanagementkosten, inclusief forensisch onderzoek, melding, fraudeherstel, kosten voor juridische hulp en communicatie
- Aansprakelijkheid met betrekking tot het lekken van vertrouwelijke data
- Aansprakelijkheid door onbevoegd gebruik van een netwerk
- Cyberafpersing

CHUBB®



Data is (not) the

new oil

Een hacker is een prima wekker: veel managers en ondernemers schroeven investeringen in beveiliging op omdat ze wakker worden geschud door incidenten. Een onverstandige aanpak.

ESSAY

Nart Wielaard is strategisch scherpdenker op het snijvlak van maatschappij, technologie en bedrijfsleven. Hij brengt complexe ontwikkelingen terug tot begrijpelijke verhalen als gespreksleider, adviseur en schrijver. Hiervoor was hij registeraccountant, wereldreiziger en journalist. Zijn kennis ligt vooral op het gebied van big data, sustainability, ondernemerschap en nieuwe media. Naast een veelheid aan projecten voor opdrachtgevers schreef hij in 2014 een boek over de maatschappelijke impact van big data.

In 2014 maakte ik een rondreis door Texas. Met mijn modale camper voelde ik me vaak nogal nietig naast de uit hun krachten gegroeide kampeerbussen en pick-up trucks. Een aantal van hen voerde vol trots een vlag met daarop een afbeelding van een mitrailleur en de woorden 'we don't dial 911'.

Wat heeft dat te maken met de risico's van data? Meer dan u denkt. De vrijbuitersgeest van de Texanen is geworteld in de beginjaren van het olietijdperk. Het Wilde Westen werd geregeerd door outlaws en malafide zakenlui die het niet al te nauw namen met de wet. Iets dergelijks speelde ook bij het begin van de digitalisering van onze samenleving. Wetgeving over wat er wel en niet mag met data was er aanvankelijk nauwelijks of was lachwekkend ouderwets - de wet op het briefgeheim moest bijvoorbeeld ook decennialang de inhoud van een e-mail beschermen.

ONDERGRONDSE ECONOMIE

Het was dan ook niet verwonderlijk dat de nieuwe digitale kansen als een magneet werkten op ondernemers van allerlei pluimage. Zij hadden vaak niet veel oog voor zaken als privacy. Ook criminelen roken hun kans. In eerste instantie ging het vooral om hackers die hun skills aan de wereld wilden tonen. Inmiddels is er sprake van goed georganiseerde misdaad en vallen ook landen elkaar digitaal aan. Sterker nog: er is een nieuwe ondergrondse economie ontstaan met een goed geoliede dienstverlening. Net zoals veel ondernemers software in de cloud gebruiken en er verder niet naar om hoeven te kijken - onder de noemer 'software as a service' - is er inmiddels ook sprake van 'crime as a service'. Wie criminele plannen heeft, kan simpelweg de wensen - spionage, afpersing, platleggen - duidelijk maken en het wordt geregeld.

Data is the new oil, zo vertellen experts ons regelmatig. Die vergelijking loopt in tal van opzichten nogal mank - olie raakt bijvoorbeeld per definitie op; de hoeveelheid data blijft juist exponentieel groeien - maar klopt dus wel waar het gaat om de gevaren van malafide lui.

"Cybersecurity biedt ook kansen"

"Cybercrime is een thema dat op dezelfde wijze aandacht verdient als het risico op brand, fraude of diefstal"

Wat moet een ondernemer met die wetenschap?
Vast staat dat het hier om een domein gaat waar ze vaak weinig kennis van hebben. Ze worden in de media echter wel gebombardeerd met alarmerend nieuws - privacygevoelige informatie die op straat ligt, hoge boetes voor een datalek, bedrijfsspionage via USB-sticks, gijzelsoftware die organisaties totaal verlamt - en besluiten op basis daarvan te investeren in allerhande beveiligingstools.

EXTREEM HOGE VERWACHTINGEN

Is dat wel zo verstandig? Vaak niet. Laat er geen misverstand over bestaan: natuurlijk is goede beveiliging essentieel. De continuïteit van vrijwel iedere organisatie is immers tegenwoordig afhankelijk van informatietechnologie. Dit voorjaar bleek bijvoorbeeld dat Britse ziekenhuizen na een aanval met gijzelsoftware (Wannacry) niet in staat waren op handmatige wijze hun operatieprocessen te doen. Dat is nauwelijks anders voor een willekeurige tandarts, aannemer of transportbedrijf. Bovendien leven we in een tijdperk met extreme verwachtingen van klanten. “Onmogelijkheden worden door ons direct gedaan, voor wonderen hanteren we een levertijd van twee weken”, was vroeger op een tegeltje te lezen in de werkplaats van mijn vader. Dertig jaar later is dat eigenlijk geen grap meer: klanten hebben extreem hoge verwachtingen die worden opgestuwd door de mogelijkheden die nieuwe technologie biedt. Als de dienstverlening korte tijd hapert kan dat ingrijpende gevolgen hebben.

De dreigingen zijn dus groot. De gevolgen ook. Toch is het niet verstandig alles dicht te spijkeren uit angst voor wat er mis kan gaan.

Verstandiger is om cybercrime te beschouwen als ‘business as usual’. Als een thema dat op dezelfde wijze aandacht verdient als bijvoorbeeld het risico op brand, fraude of diefstal. Neem bijvoorbeeld eens in gedachten hoe een juwelier naar diefstalrisico’s kijkt. Deze laat zich niet gek maken door leveranciers van beveiligingsmiddelen maar maakt zelf een bewuste keuze over wat nodig is, stemt de beveiliging vooral af op zijn eigen situatie en pas secundair op basis van wat criminelen aan nieuwe technieken ontwikkelen, schiet niet in de paniek als er iets (bijna) fout gaat bij de buren maar wil er vooral lering uit trekken over hoe het beter kan, en traint zijn medewerkers op wat te doen en laat beveiliging niet over aan een gespecialiseerde afdeling. Dit alles staat vaak in schril contrast met hoe we omgaan met cybercrime.

MENS BLIJFT ZWAKSTE SCHAKEL

In die wereld zetten we vaak hoog in op technologische tools als wapen tegen cybercriminelen. Die tools zouden echter niet het startpunt moeten zijn van een goed beleid, maar eerder de laatste stap. De mens is en blijft vaak de zwakste schakel in het beveiligingsbeleid en investeren in de allerbeste tools is dan ook alleen maar zinvol als mensen hun verantwoordelijkheden nemen. Social engineering - waarbij hackers het vertrouwen winnen van medewerkers door slim sociaal gedrag en daardoor toegangsrechten weten te krijgen tot systemen - blijft een van de belangrijkste risico’s. Een juwelier weet dat overigens ook als geen ander. A fool with a tool is still a fool.

Gelukkig maar dat de Texanen over het algemeen geen fools zijn en hun wapentuig niet te pas en te onpas in het rond zwaaien. Je kunt veel van de rednecks zeggen maar ze laten in elk geval niet met zich sollen en gaan niet in een slachtofferrol zitten. Dat mogen we ook van ondernemers verwachten waar het gaat om cybercrime.

Tot slot: cybersecurity biedt ook kansen. De juiste benadering van de risico’s kan immers zelfs een concurrentievoordeel opleveren. Want klanten lezen ook de krant, worden zich ook bewust van wat er mis kan gaan met hun data en verwachten dat bedrijven daar goed op anticiperen. Wie dat beter doet dan de concurrent heeft daarmee een nieuw concurrentiewapen in handen. Wie met die bril kijkt naar security ziet heel andere perspectieven opdoemen. Probeer het eens.

“Er is een ondergrondse economie ontstaan met een goed geoliede dienstverlening”

Een grote ICT-dienstverlener biedt internationale klanten een uitgebreid pakket aan diensten aan, waaronder beheer van infrastructuur en data (datacenter), systeemintegratie, applicatieontwikkeling en onderhoud. Deze onderneming voldoet aan de hoogste eisen van cyberveiligheid. Bij een routinecontrole ontdekt een IT-medewerker iets verdachts...

Een hacker?
"Het viel de medewerker op dat er een gebruikersnaam was aangemaakt zonder tussenkomst van de bevoegde systeembeheerder. Met die gebruikersnaam had iemand toegang tot een van onze servers, waarop een scala aan persoons- en bedrijfsgegevens stond. Alle alarmbellen gingen af: we waren niet alleen gehackt, de hacker was ook nog actief!"

Hoe is dat mogelijk bij een ICT-dienstverlener?
"Ik begrijp de vraag. Laat ik het zo stellen: het feit dat we deze onbevoegde persoon zo snel op het spoor waren, bewijst onze expertise en strikte naleving van de veiligheidsprotocollen. Een minder strak georganiseerd bedrijf had nooit gemerkt dat er een hack was geweest. De hacker moet een zwakke plek in ons systeem hebben ontdekt. Uiteraard heb ik hier erg slecht van geslapen. Het is onze corebusiness om data van klanten veilig op te slaan. De consequenties van een dergelijk incident moet je niet onderschatten. Niet alleen wij maar ook onze klanten lopen de kans op ernstige schade."

Welke acties heeft u ondernomen?
"Omdat het ons niet lukte om het lek boven water te krijgen en de hacker te verwijderen, hebben we onze verzekeraar ingeschakeld via de hotline. De response adviseur stelde een team van deskundigen samen. In een telefonische vergadering bespraken wij het incident met een IT-specialist en een gespecialiseerd jurist. Er moest snel worden gehandeld. Er stond immers een achterdeurtje open naar belangrijke gegevens."

Moest uw bedrijf offline?
"We hebben geen bedrijfsstilstand gehad. Niemand van onze klanten heeft tijdens de zoektocht naar het lek en de hacker hinder ondervonden. Samen met de IT-specialist werkten onze IT'ers het weekend door om de hacker succesvol te verwijderen van het netwerk en het lek te dichten."

Weet u wie er achter de hack zat?
"Helaas niet. Ook was het niet mogelijk om vast te stellen of er persoonsgegevens of bedrijfsgegevens van klanten zijn ontvreemd. De hacker was daartoe in de gelegenheid, maar we konden niet zien wát hij heeft gedaan."

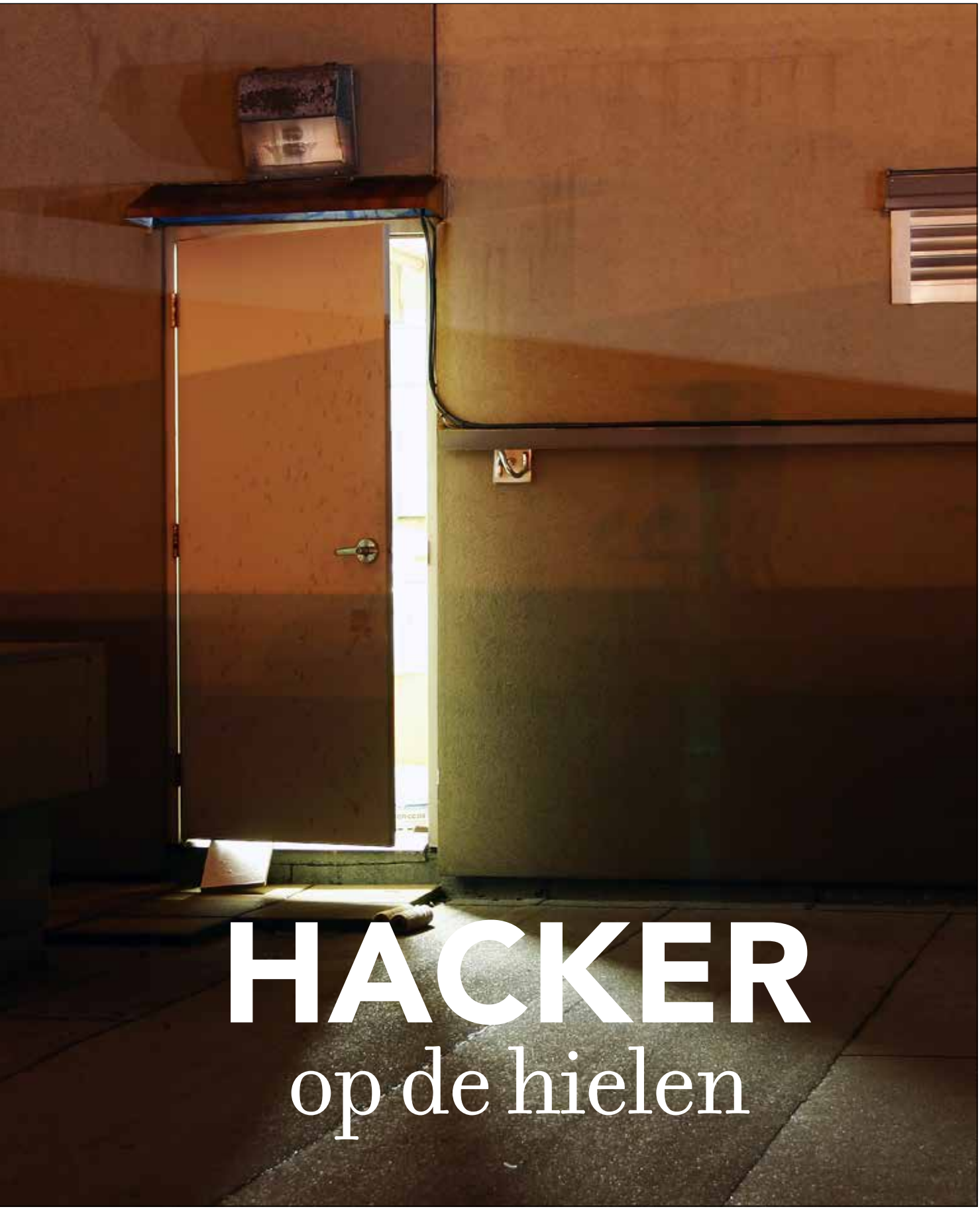
Hoe is dit afgerond?
"De juridisch adviseur onderzocht op basis van het IT-rapport of het melden van een mogelijk lek aan de Autoriteit Persoonsgegevens nodig was. Het advies luidde om dit wel te doen. De adviseur begeleidde ons hierin. Onze klanten hebben we niet op de hoogte gesteld. Dat heeft alles te maken met het feit dat we de hacker zo snel op het spoor waren. De zwakke plek in het systeem kan het gevolg zijn van een menselijke fout. Om een dergelijk incident in de toekomst te voorkomen hebben we adviezen van de IT-specialist opgevolgd. Al met al is de schade zeer beperkt gebleven, ook voor onze klanten."

AIG EUROPE, NETHERLANDS

Het incident bij de ICT-dienstverlener bewijst weer: hoe goed de beveiliging ook is, een hacker die naar binnen wil, blijft het proberen tot het lukt. Zwakke plekken in het systeem zijn vaak het gevolg van menselijke fouten, ondanks correcte technische beveiligingsmaatregelen. Investeer daarom niet alleen in techniek, maar ook in bewustwording en training van personeel. Totale kosten voor dit incident (gedekt door de verzekering): € 83.479.

De dekking van de AIG CyberEdge verzekering bestaat onder meer uit:

- Uitgebreide diensten voor het managen van (vermeende) cyberincidenten, waaronder juridische diensten en IT-diensten, herstel van reputatie en kennisgeving datalekken betrokkenen en toezichthouder
- Kosten van verweer en boetes opgelegd door de toezichthouder
- Aansprakelijkheid en kosten van verweer voortvloeiend uit cyberincidenten
- Cyber-/privacyafpersing
- Cyberdiefstal van geld of geldswaarden en goederen



HACKER
op de hielen

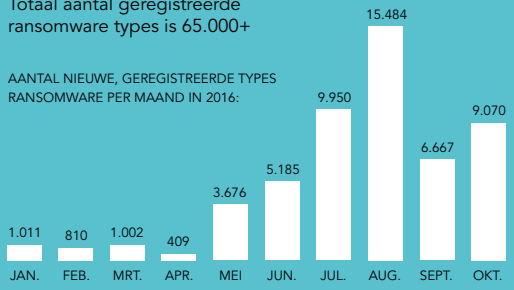
WELKE RISICO'S LOOPT UW

Cyberaanvallen in cijfers

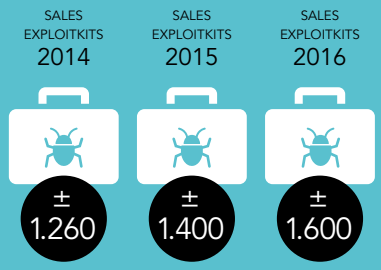
1. GEPLANDE AANVALLEN (VAN BUITENAF)
DRIE VOORBEELDEN:

1a. Ransomware
is een malware (software om computersystemen te verstoren) die gegevens op een computer blokkeert. Pas wanneer de gebruiker losgeld heeft betaald, worden de gegevens gedeblokkeerd.
Totaal aantal geregistreerde ransomware types is 65.000+

AANTAL NIEUWE, GEREGISTREERDE TYPES RANSOMWARE PER MAAND IN 2016:

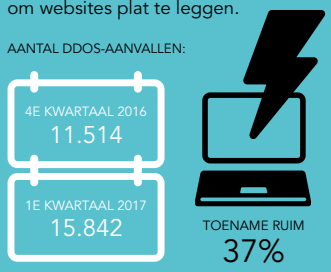


1b. Exploitkits
zijn kant-en-klare toolkits die louche softwareontwikkelaars verkopen.
Met zo'n toolkit besmet iemand eenvoudig uw computersystemen met malware.



1c. DDoS-aanvallen
(Distributed Denial of Service) zijn aanvallen waarbij een computersysteem crasht door het sturen van grote hoeveelheden data.
Deze methode wordt vaak gebruikt om websites plat te leggen.

AANTAL DDOS-AANVALLEN:

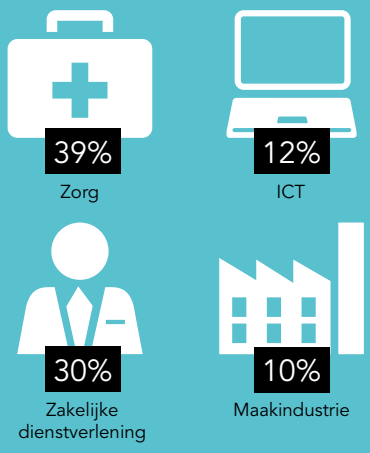


2. MENSELIJKE FOUTEN (WEL/NIET OPZETTELIJK)

Bijna 80% van de cyberrisico's ontstaat door menselijke fouten

3. TECHNISCH FALEN (VAN SYSTEMEN, SERVERS, HARD- EN SOFTWARE)

Bedreiging cybercrime per sector



Gevolgen van cybercrime

- Privacyschending
- Bedrijfsschade door stagnatie van processen
- Eis van losgeld
- Reconstructiekosten (herstel database)
- (Gevoelige) informatie openbaar, beschadigd of verloren
- Reputatieschade
- Boete van Autoriteit Persoonsgegevens
- Aansprakelijkheidsclaims

Voorbeelden van datalekken

1. Medische gegevens ingezien door onbevoegden
2. Persoonlijke gegevens van werknemers ingezien door onbevoegden (bijvoorbeeld kopieën van rijbewijzen, paspoorten, bankgegevens, wachtwoorden)
3. Verlies van een laptop met onversleutelde, financiële of anderszins gevoelige informatie
4. Een versleutelde laptop met belangrijke data is gestolen en er is geen back-up voorhanden
5. Bij een hack zijn klantgegevens en wachtwoorden ontvreemd
6. Persoonsgegevens ongeoorloofd ingezien vanwege kwetsbaarheid webapplicatie
7. Een envelop met creditcard- en/of betalingsgegevens is niet versnipperd maar in de vuilnisbak gegooid

Bronnen
- Kaspersky Security Bulletin Overall Statistics for 2016 (Kaspersky Lab, 2016)
- Distributed Denial of Service (DDoS) Threat Report Q1 2017 (Nexusguard, 2017)
- Meldplicht datalekken facts & figures: overzicht feiten en cijfers 1e kwartaal 2017
- Infographic Cyberrisico's in Nederland (Van Lanschot Chabot, 2016)
- Exploit DB

ORGANISATIE?

Cyberaanvallen voorkomen

ONLINE GEDRAG MEDEWERKERS VOL RISICO'S

24%
gebruikt dezelfde online opslag voor zakelijk en privé

1 op de 4 personen deelt accountinformatie met anderen

logt niet uit na het werken

STAPPENPLAN

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Deze nieuwe Europese privacywet geldt voor alle organisaties die persoonsgegevens verwerken, dus ook voor het midden- en kleinbedrijf en zzp-ers.
Neem de juiste maatregelen:

1. Wijs iemand aan die verantwoordelijk is voor de implementatie van de AVG

2. Inventariseer welke persoonsgegevens u verwerkt en hoe

3. Breng wettelijke en contractuele verplichtingen in kaart

4. Bepaal uw ambitie-niveau. Hoe belangrijk acht u de zorgvuldige verwerking van persoonsgegevens?

5. Stel de benodigde processen, standaarden en handleidingen vast

6. Actualiseer uw contracten

7. Train uw personeel

8. Controleer periodiek of de praktijk nog aansluit bij uw ambitie

Heeft u professionele ondersteuning?

RISICOBEHEER EN VERZEKEREN

Adequaat crisismanagement (coaching, juridisch onderzoek, forensisch onderzoek, melding AP, kredietbewaking & PR)

Eigen schade (afpersing, bedrijfsstilstand, herstelkosten, cyberdiefstal & boetes)

Schade aan derden (privacy aansprakelijkheid, aansprakelijkheid voor netwerkbeveiliging en media aansprakelijkheid)

Froonacker Van de Witte
assurantiën - risicobeheer

Voorstraat 61
8801 LB Franeker
0517 399 999
info@frovdw.nl
www.frovdw.nl

ACCOUNTANCY EN ADVIES

Scherpe risicoanalyse cybersecurity

Privacy audits

Gerechtelijke deskundigheid

Forensisch onderzoek

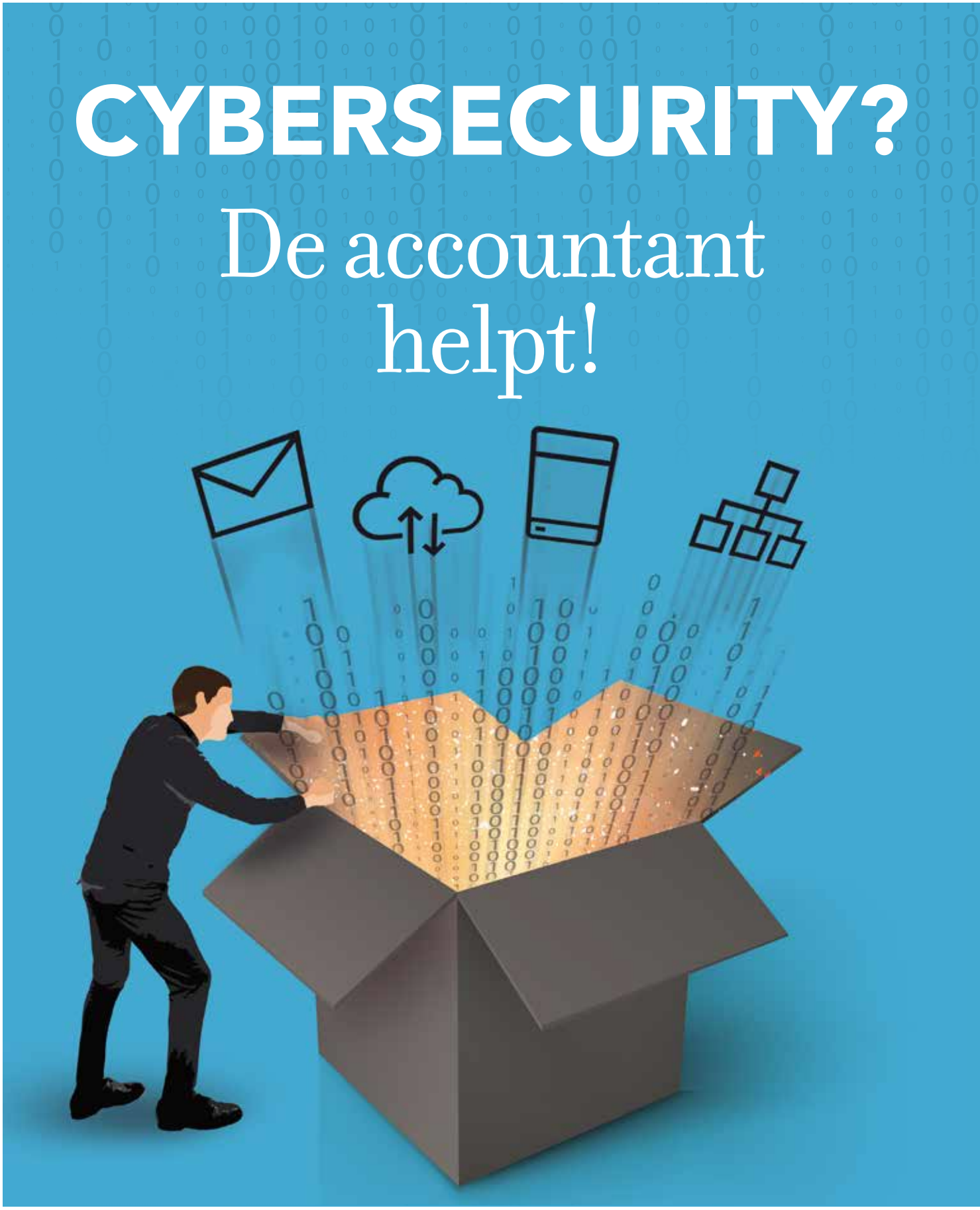
Incident management

Van der Veen & Kromhout
registeraccountants • belastingadviseurs

Drachten: 0512 584 800
drachten@kromhout.com
Gorredijk: 0513 468 468
gorredijk@kromhout.com
Joure: 0513 480 480
joure@kromhout.com
www.kromhout.com

CYBERSECURITY?

De accountant helpt!



“Stel jezelf de vraag: hoe afhankelijk ben ik van welke data?”

Ligt de mkb-ondernemer wel genoeg wakker van ICT-beveiliging? Zijn de risico's voor de continuïteit van de onderneming wel genoeg onderkend? Cruciale vragen waarbij de mkb-accountant als geen ander kan helpen.

Bij het bespreken van tussentijdse cijfers en de jaarrekening gaat de accountant met de ondernemer ook in gesprek over de toekomst. Want die cijfers zijn dé gevalideerde basis voor onder andere begrotingen, visies en plannen. De accountant heeft, zeker in het mkb, een vertrouwensrol. De accountant is kritisch. Ziet risico's. Doet eigenlijk alles wat mogelijk is om de continuïteit van de onderneming te waarborgen. Validatie van de betrouwbaarheid van de beschikbare data en de IT-omgeving is daarbij belangrijk. Niet alleen voor de jaarrekening, maar juist voor de ondernemer zelf.

DE KANSEN EN RISICO’S VAN DIGITALISERING

IT zorgt soms voor minder functiescheidingen, omdat de ‘oude’ papieren processen in de IT-omgeving niet goed worden ingericht. Daarnaast worden processen meer en meer gedigitaliseerd. Hele administraties worden gedigitaliseerd en via SBR gaan de cijfers automatisch naar overheidsinstanties als de Kamer van Koophandel, de Belastingdienst en het CBS.

Continu monitoren op basis van actuele bedrijfsinformatie wordt dé standaard. De ondernemer beschikt dan over actuele financiële informatie waarmee de onderneming direct kan worden bijgestuurd. Dat mag een grote kans worden genoemd. Maar tegelijkertijd nemen ook de risico's toe. Hoe afhankelijker ondernemers worden van data en systemen, hoe kwetsbaarder ze zijn op dat gebied. Geen toegang tot de systemen en data verstoort direct de bedrijfsvoering en vormt een bedreiging voor de bedrijfscontinuïteit. Daarom is het van belang te analyseren hoe afhankelijk de onderneming is van systemen en data en of de juiste maatregelen zijn genomen om de beschikbaarheid van data en systemen te waarborgen.

PRAGMATISCHE AANPAK

“In het mkb moet je pragmatisch naar cyber- en datarisico’s kijken”, zegt Rolf Rudolphy, registeraccountant, IT-auditor en de ICT-manager bij Van der Veen & Kromhout (www.kromhout.com). “De eerste vraag is: hoe afhankelijk ben je van data? Een handelsonderneming met een geïntegreerd ERP-systeem en een webshop heeft een groter probleem als ze niet meer bij hun data kunnen, dan een schilder. Als accountantskantoor hebben we natuurlijk veel vertrouwelijke gegevens van onze klanten. Die gegevens moeten we goed beschermen. Niet omdat we bang zijn voor boetes van de Autoriteit Persoonsgegevens, maar omdat wij dat gewoon als onze taak zien. Daarom hebben we de afgelopen jaren zelf veel geïnvesteerd in cybersecurity. En die kennis gebruiken we ook om onze klanten, van klein tot groot, optimaal advies te kunnen geven.”

Neem contact op met Rolf Rudolphy via rjrudolphy@kromhout.com of 0513 468 468.

Van der Veen & Kromhout
registeraccountants • belastingadviseurs

VOOR ELKAAR, MET ELKAAR

RISICOBEHEER IN VERZEKERINGEN

Froonacker Van de Witte is al ruim 50 jaar een betrouwbare en deskundige partner op het gebied van verzekeringen en financiële dienstverlening voor ondernemers en particulieren die zich thuis voelen bij een nuchtere en eerlijke aanpak.

Froonacker Van de Witte
assurantiën - risicobeheer

Voorstraat 61, 8801 LB Franeker | tel: (0517) 39 99 99 | www.frovdw.nl | whatsapp: 06 - 44 26 64 64

"Als u geen toegang heeft tot uw systemen en data, komt uw bedrijfscontinuïteit keihard in het geding"

IDENTIFICEREN VAN KWETSBAARHEDEN

De accountant vervult hierin een signalerende en adviserende rol. Kent de onderneming en de cultuur. Snapt als geen ander hoe de onderneming functioneert en kent de bedrijfsprocessen. Deze kennis is nodig voor het samenstellen van de jaarrekening, het afgeven van een accountantsverklaring of het opstellen van managementrapportages. Maar de accountant kent ook de kwetsbaarheden van de onderneming en kan vanuit die kennis cyber- en datarisico's goed inschatten en opschalen naar specialisten als dat nodig is. Want cybersecurity is een vak apart. Zeker bij crisisincidenten zoals ransomware. Accountantskantoren zoals Van der Veen & Kromhout hebben deze specialisten in dienst, waardoor ze de klant op het gebied van preventie en bewustzijn en bij incidenten van het juiste advies kunnen voorzien.

HET START BIJ BEWUSTZIJN

Weet u waar uw onderneming kwetsbaar is? Hoe is het beveiligingsbewustzijn binnen de onderneming? In een wereld waarbij elk systeem aan het internet verbonden is, moet er iemand zijn die de onderneming kan doorgronden. Iemand die vertelt of de ondernemer de juiste maatregelen heeft getroffen om de beschikbaarheid van systemen en data te waarborgen. Zeker in onze kenniseconomie. Accountants en achterliggende IT-experts kunnen de onderneming testen. Zijn er voldoende maatregelen genomen om weerstand te bieden tegen dreigingen? Dat is een belangrijke vraag om de ondernemer wakker en alert te houden.

Voorkomen is nog altijd beter dan genezen, zeker bij cyber- en datarisico's. Want als u geen toegang heeft tot uw systemen en data, verstoort dat direct uw bedrijfsvoering en komt uw bedrijfscontinuïteit keihard in het geding...

Ransomware is een serieuze bedreiging waar iedere ondernemer rekening mee moet houden. De tegenstanders zijn geen kruimeldieven maar internationale criminele organisaties die er honderden miljoenen euro's mee verdienen. Toch zijn er voldoende mogelijkheden om een aanval met ransomware te voorkomen, of - als die zich toch voordoet - de gevolgen te beperken. Kijk voor 11 tips op www.kromhout.com/nieuws/ransomware-steeds-groter-probleem.

Bewerken of verwerken van persoonsgegevens: OVEREENKOMST ESSENTIEEL!

In april 2016 was een groot datalek in Amersfoort volop in het nieuws. De krantenkoppen logen er niet om: 'Wijkteams slordig met privacygevoelige gegevens' en 'Verontrusting na gelekte cliëntgegevens'. Wat was er aan de hand? In de gemeente Amersfoort zijn de persoonlijke gegevens van bijna 2.000 cliënten van wijkteams gelekt.

Wat blijkt: een ambtenaar had een lijst met gegevens per abuis naar een verkeerd e-mailadres gestuurd. Wekenlang probeerden ambtenaren de fout onder de pet te houden en weg te poetsen. Het lek is niet gemeld overeenkomstig de Wet meldplicht datalekken. Het gevolg was dat de positie van de verantwoordelijke wethouders wankelde en een forse boete dreigt wegens overtreding van de wet.

Het datalek in Amersfoort kon ontstaan omdat daar meerdere partijen betrokken zijn bij de bewerking van persoonsgegevens. Door het ontbreken van heldere onderlinge afspraken deelde de instantie privacygevoelige gegevens per e-mail. Vanwege een menselijke fout kwamen de gegevens vervolgens terecht bij een verkeerd adres.

WAKE-UP CALL

Dit incident is voor veel bedrijven en instellingen een wake-up call: want hoe kunt u zelf de krantenkoppen en andere mogelijke gevolgen van een datalek voorkomen?
"Dat kunt u eenvoudig doen door een goede bewerkersovereenkomst op te stellen", vertelt Anne Bergsma, directeur van Froonacker Van de Witte Assurantiën uit Franeker. "In aanvulling op andere technische en organisatorische maatregelen die u dient te nemen om de kans op een datalek of ander cyberrisico te verlagen, maakt u in die bewerkersovereenkomst afspraken met derden over de bescherming van persoonsgegevens. Bijvoorbeeld met een ICT-leverancier, een hosting- of een andere partij die u inschakelt voor de verwerking van persoonsgegevens. Deze partijen noemen we 'bewerkers'."

WAT IS EEN BEWERKERSOVEREENKOMST

Om de noodzaak van een goede bewerkersovereenkomst op waarde te schatten nemen we eerst het begrip zelf onder de loep. Een bewerkersovereenkomst of data processing agreement (DPA) komt uit de privacyregelgeving. Daarin wordt onderscheid gemaakt tussen de begrippen 'verantwoordelijke' en 'bewerker'.
De ***verantwoordelijke*** (controller) is degene die het doel van - en de middelen voor - de verwerking van persoonsgegevens vaststelt. Denk hierbij aan een bedrijf dat persoonsgegevens van zijn werknemers bijhoudt met betrekking tot de salarisadministratie (naam, adres, bankrekeningnummer, enzovoorts). Het bedrijf is verantwoordelijk voor die gegevens. De ***bewerker*** (processor) is degene

WAT ZIJN PERSOONS-GEGEVENS?

'Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatie-nummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.'

'BEWERKER' WORDT 'VERWERKER'

Met de intreding van de Europese Privacyverordening op 25 mei 2018 worden de begrippen 'bewerker' en 'bewerkersovereenkomst' hernoemd tot 'verwerker' en 'verwerkersovereenkomst'.

ADVIES

Wilt u advies over uw bestaande of nieuwe verwerkersovereenkomst? Neem dan contact op met directeur en zakelijk adviseur Anne Bergsma van Froonacker Van de Witte Assurantiën B.V. Hij helpt u graag met het analyseren en opstellen van adequate overeenkomsten.

0517 399 999
a.bergsma@frovdw.nl

www.frovdw.nl

Froonacker Van de Witte
assurantiën - risicobeheer

die deze persoonsgegevens ten behoeve van de verantwoordelijke verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. In bovengenoemd voorbeeld is een salarisadministratiekantoor, dat voor het genoemde bedrijf de salarisadministratie afhandelt, een bewerker.

Een bewerkersovereenkomst is derhalve een onderlinge, schriftelijke overeenkomst tussen de verantwoordelijke en de bewerker, waarin wordt vastgelegd hoe de bewerker met de persoonsgegevens moet omgaan. En - hoe kan het ook anders - het valt onder de verantwoordelijkheid van de verantwoordelijke dat dit ook daadwerkelijk gebeurt.

WANNEER IS EEN BEWERKERS-OVEREENKOMST ESSENTIEEL?

Zodra een verantwoordelijke persoonsgegevens laat verwerken door een bewerker, is een bewerkersovereenkomst tussen beide partijen altijd verplicht. Dit geldt tevens als de bewerker bijvoorbeeld een dochteronderneming van het verantwoordelijke bedrijf is, of in het buitenland is gevestigd. Telkens wanneer een verantwoordelijke het verwerken van persoonsgegevens uitbesteedt, is een schriftelijke overeenkomst vereist.

Wat staat erin?

Hieronder vindt u een selectie van de belangrijkste onderdelen in een bewerkersovereenkomst:

- **Bewerking in overeenstemming met instructies van de verantwoordelijke**
  De bewerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken, maar alleen om uitvoering te geven aan de instructies van de verantwoordelijke.
- **Geheimhouding**
  In deze bepaling wordt aan de bewerker een geheimhoudingsplicht opgelegd, eventueel gecombineerd met een boetebeding. Overigens is opzettelijke niet-naleving van deze geheimhoudingsplicht strafbaar gesteld in het Wetboek van Strafrecht.
- **Beveiligingsmaatregelen**
  De verantwoordelijke draagt zorg dat de bewerker passende technische en organisatorische maatregelen neemt om de persoonsgegevens te beveiligen tegen fraude, afpersing, verlies en dergelijke.
- **Inschakelen van derden en onderaannemers**
  In de overeenkomst wordt vastgelegd of, en onder welke voorwaarden, de bewerker sub-bewerkers mag inschakelen.
- **Locatie van de data**
  De verantwoordelijke moet weten in welke landen zijn data worden opgeslagen. Dit is mede van belang met het oog op de verplichtingen die gelden bij doorgifte van persoonsgegevens naar het buitenland.
- **Audits**
  De verantwoordelijke moet kunnen controleren of de bewerker zich houdt aan de gemaakte afspraken. Dit gebeurt vaak in de vorm van een audit (onderzoek) door de verantwoordelijke of door een onafhankelijke derde. In de bewerkersovereenkomst kunnen partijen hier nadere afspraken over maken.
- **Aansprakelijkheid en verzekeringsplicht**
  De wet bepaalt dat de verantwoordelijke kan worden aangesproken als iemand schade lijdt doordat de Wet bescherming persoonsgegevens (Wbp) niet wordt nageleefd. Dit geldt zelfs als de schade het gevolg is van nalatigheid van de bewerker, die in dat geval ook zelf aansprakelijk is. Het is verstandig om in de bewerkersovereenkomst heldere afspraken te maken over deze verdeling van aansprakelijkheid. Verantwoordelijke en bewerker doen er ook goed aan om afspraken te maken over adequate verzekeringsdekking(en) aan de zijde van de bewerker. Zodat deze bij een calamiteit voldoende continuïteit kan waarborgen.

VIRTUELE RISICO'S, *ECHTE* SCHADE

ALS HET DAN TOCH FOUT GAAT…

… dan maakt u zich al druk genoeg om het onderzoek waaraan uw organisatie onderworpen wordt. Wel zo fijn wanneer alle kosten gedekt zijn op uw cyberverzekering. Zoals de kosten voor het onderzoek, maar ook bedrijfsstilstand, imagoherstel, losgeld, enzovoorts. Wij helpen u graag – op een nuchtere manier – met het maken van de juiste risicobeheer keuzes. Zo blijft de continuïteit van uw bedrijf optimaal gewaarborgd.

Froonacker Van de Witte
assurantiën - risicobeheer

Voorstraat 61, 8801 LB Franeker | tel: (0517) 39 99 99 | www.frovdw.nl

OOK UW ORGANISATIE IS SINDS 1 JANUARI 2016 VERPLICHT OM ALLE DATALEKKEN DIRECT TE MELDEN BIJ DE AUTORITEIT PERSOONSGEGEVENS (AP). VANAF 2018 GAAT DEZE INSTANTIE NALEVING HIERVAN NÓG STRENGER CONTROLEREN. BENT U OP DE HOOGTE WAT DIT VOOR U BETEKENT?

Meldt u datalekken niet, te laat of verkeerd, dan kunnen momenteel boetes van maximaal € 820.000 worden opgelegd. Per 25 mei 2018 geldt de nieuwe Algemene verordening gegevensbescherming (AVG). Hierin is het maximale boetebedrag verhoogd tot € 20.000.000 of 4% van de wereldwijde omzet (indien deze uitkomst hoger is).

Aantal datalekken

± 5.700

Aantal meldingen van datalekken bij de AP in heel 2016

± 2.300

Aantal meldingen van datalekken bij de AP in Q1 2017

Veel voorkomende datalekken

45%

Persoonsgegevens verstuurd naar een verkeerd adres

22%

Hardware of dossier met gegevens kwijt-geraakt/gestolen

7%

Hacking/ malware/ phishing

Een datalek vindt dus lang niet altijd met opzet of door cybercriminelen plaats. Het kan ook bij uw organisatie onverhoopt voorkomen.

RISICO-INSCHATTING UW ORGANISATIE

Uw bedrijf heeft

66% KANS

om cyberschade op te lopen.

Onder cyberschade vallen zowel aanvallen van buitenaf als het per ongeluk lekken van data. 'Social engineering' blijkt een succesvolle methode waarmee cybercriminelen informatie aan mensen ontfutselen.

HOE ZORGT U ERVOOR DAT DIE KANS FORS DAALT?

- Organisatorische verbeteringen aanbrengen
- Technische aanpassingen doorvoeren
- Bewustzijn van medewerkers verhogen

€

Schade door cybercrime kost Nederlandse organisaties jaarlijks 10 miljard euro.

Schade door diefstal: 1 miljard euro.

BESTUURDERS-AANSPRAKELIJKHEID

Cybercrime brengt veel bedrijven in een financiële wurggreep. Bij faillissement - en de curator constateert dat bestuurders nalatig hebben gehandeld - kan dit ook consequenties hebben voor de bestuurders persoonlijk. Kortom: u kunt hoofdelijk aansprakelijk worden gesteld vanwege het niet, te laat of verkeerd melden van een datalek of het nalaten van beheermaatregelen, zoals bijvoorbeeld het afsluiten van een adequate verzekering.

Top 3 bedrijfsrisico's in Nederland

1. Bedrijfsonderbrekingen 35%
2. Cyberincidenten 32%
3. Marktontwikkelingen 32%

Opvallend is dat cyberincidenten in 2012 nog een minimaal bedrijfsrisico vormden. Nu staan cyberincidenten in de top 3!

Retouradres
Postbus 533
2400 AM Alphen aan den Rijn

PostNL
Port Betaald

WILT U WETEN HOE U UW ORGANISATIE OPTIMAAL KUNT BEVEILIGEN TEGEN CYBERAANVALLEN EN UW KWETSBAARHEID ZO MINIMAAL MOGELIJK KUNT HOUDEN? LEES VERDER OP PAGINA 23.

Bronnen
- https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/taken-en-bevoegdheden/onderzoek-en-handhaving (AP, 2017)
- Meldplicht datalekken facts & figures: overzicht feiten en cijfers 1e kwartaal 2017
- Allianz Risk Barometer – Top Business Risks 2017
- Infographic Cyberrisico's in Nederland (Van Lanschot Chabot, 2016)
- Deloitte

Zakelijke cyberrisico's

Ontwikkelingen

- Toename van phishing via sms en whatsapp
- Criminelen spelen in op Covid-19 pandemie
- Grotere DDoS-aanvallen
- Kwetsbaarheden door ketenafhankelijkheid
- Internet of Things vergroot digitale kwetsbaarheid
- Dreiging van afpersing toegenomen
- Organisaties ook doelwit als springplank naar andere organisaties
- Cybercrime-as-a-service is in opkomst

Gemiddeld schadebedrag per bedrijf: **€ 340.500**

Gemiddelde schade naar bedrijfsgrootte

Kleinbedrijf (tot 50 medewerkers) **€ 14.000**

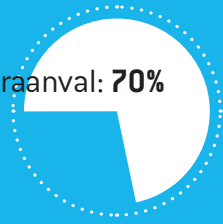
Middelbedrijf (tot 250 medewerkers) **€ 184.000**

Grootbedrijf (tot 1000 medewerkers) **€ 715.000**

Enterprise (>1000 medewerkers) **€ 551.000**

Aantal bedrijven dat cyberaanval meldt: **68%**

- Virus of worm: **24%**
- Ransomware: **17%**
- DDoS: **15%**
- Meer dan 4 aanvallen in een jaar: **30%**



Aantal bedrijven met schade in productieketen als gevolg van cyberaanval: **70%**

Aantal bedrijven met schade als gevolg van uitval clouddiensten: **27%**

Impact

21% omzetverlies door onderbreking bedrijf

21% verlies van klantvertrouwen

17% wisseling van management

16% reputatieschade

14% boetes

12% daling aandeelhouderswaarde

Bron: NCSC, Rathenau, Hiscox en Deloitte