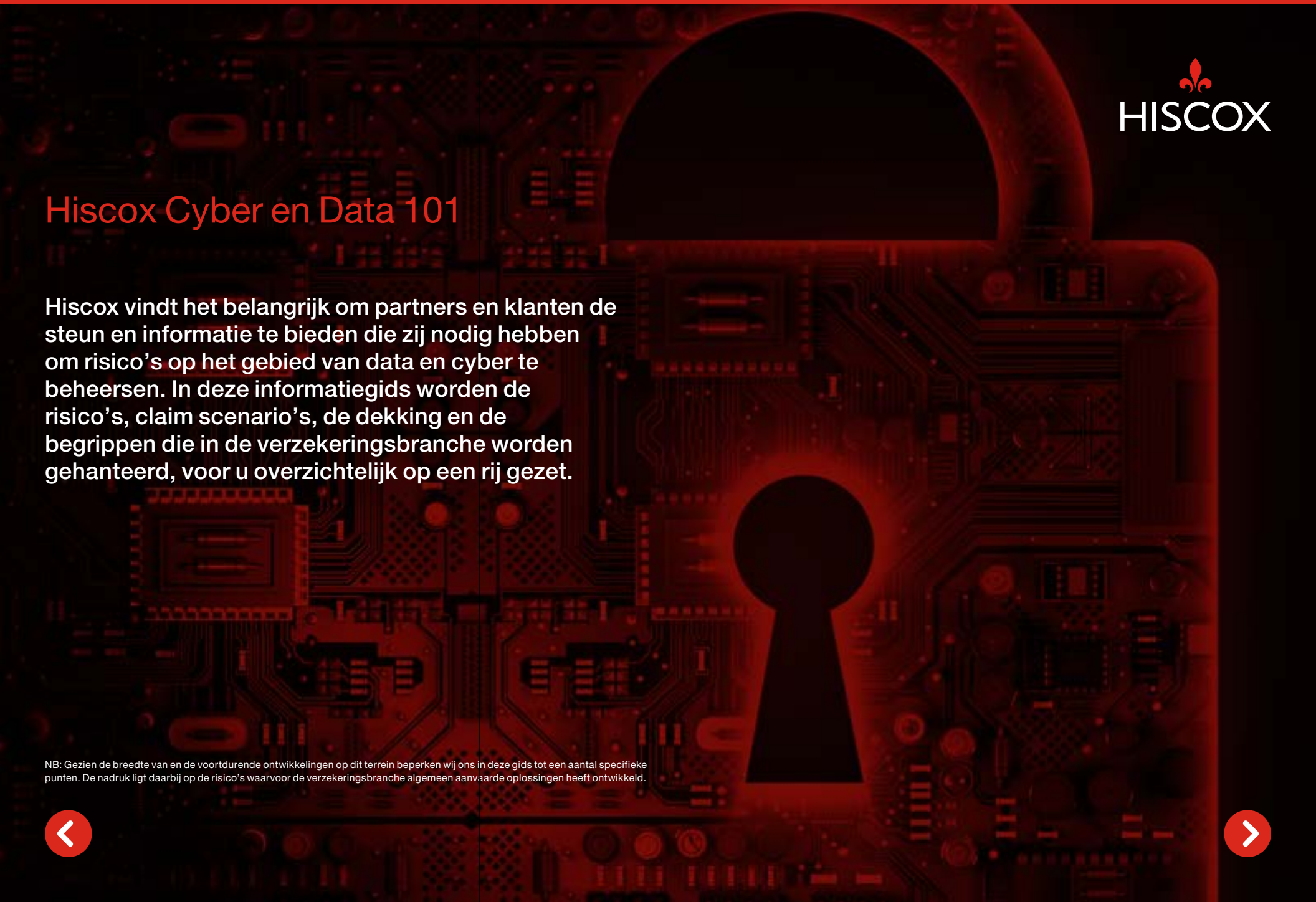


Hiscox Cyber en Data 101

Hiscox vindt het belangrijk om partners en klanten de steun en informatie te bieden die zij nodig hebben om risico's op het gebied van data en cyber te beheersen. In deze informatiegids worden de risico's, claim scenario's, de dekking en de begrippen die in de verzekeringsbranche worden gehanteerd, voor u overzichtelijk op een rij gezet.

NB: Gezien de breedte van en de voortdurende ontwikkelingen op dit terrein beperken wij ons in deze gids tot een aantal specifieke punten. De nadruk ligt daarbij op de risico's waarvoor de verzekeringsbranche algemeen aanvaarde oplossingen heeft ontwikkeld.

De wereld om ons heen

Door technologie kunnen we met elkaar in contact komen op manieren die nog niet zo heel lang geleden ondenkbaar waren. Met een druk op een knop maken we doktersafspraken, bestellen we eten, kopen we artikelen, betalen we met creditcards enz. We laten overal digitale vingerafdrukken achter; bedrijven moeten doordrongen zijn van de risico's die het verzamelen van al die persoonsgegevens met zich meebrengen.

Zij bewaren en gebruiken een hoeveelheid onderling verbonden gegevens die exponentieel toeneemt. Aan hen is de wettelijke verplichting en de maatschappelijke taak om op een veilige manier met die gegevens om te gaan. Sluwe en vindingrijke cybercriminelen weten vaker dan ooit sluiproutes te vinden. Wetgevers, burgers en ondernemers lijken altijd net een stap achter te lopen als het gaat om de bescherming van persoonsgegevens.

Welke gegevens zijn blootgesteld aan risico?

Persoonsgegevens
Gegevens aan de hand waarvan personen kunnen worden geïdentificeerd, zoals BSN-nummer, rijbewijsnummer, bankrekeninggegevens, gebruikersnamen en wachtwoorden van online accounts, medische gegevens en zorgverzekeringsinformatie.

Beschermde gegevens omtrent genoten gezondheidszorg
Gegevens over de verlening en betaling van gezondheidszorg aan de hand waarvan personen kunnen worden geïdentificeerd.

Betaalkaart-gegevens
Gegevens van betaalpassen en creditcards.

Waarom stelen cybercriminelen persoonsgegevens?

Persoonsgegevens zijn simpelweg veel geld waard. Criminelen kunnen gestolen persoonsgegevens en vertrouwelijke informatie eenvoudig te gelde maken, bijvoorbeeld door fraude te plegen met gestolen BSN-nummers of door vertrouwelijke informatie te koop aan te bieden op de zwarte markt.

Ter bescherming van persoonsgegevens zijn strenge regels opgelegd aan het bedrijfsleven; bedrijven die een fout maken of gehackt worden, moeten de kosten van de inbreuk betalen. Torenhoge kosten en ingewikkelde regelgeving maken het voor bedrijven moeilijk om zich zonder hulp te beschermen tegen de impact van een inbreuk op persoonsgegevens.

De feiten

Kwaadwillenden tasten systemen voortdurend af op zoek naar de zwakheden in de beveiliging van systemen die toegang hebben tot waardevolle vertrouwelijke informatie en persoonsgegevens. Veel bedrijven denken dat het met inbreuken op de privacy en gegevens wel los zal lopen, maar dat is een misvatting, zoals blijkt uit de volgende drie feiten:

Feit 1: nog nooit waren omvang en kosten van inbreuken zo hoog als nu

Feit 2: elke sector en elk bedrijf, van groot tot klein, loopt risico

Feit 3: geen enkele organisatie is immuun voor interne en externe bedreigingen

FEIT 1: Nog nooit was de omvang en waren de kosten van inbreuken zo hoog als nu

Inbreuken op gegevens worden steeds groter en het aantal getroffen records per gegevensinbreuk neemt toe.

2,144,583,675

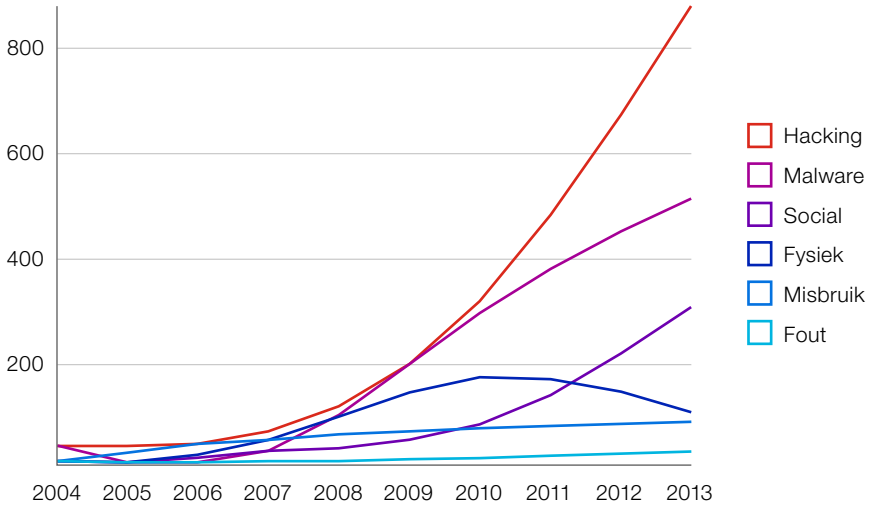
records gingen verloren door inbreuken in 2014[1]

37% meer inbreuken

ten opzichte van 2013[1]

TYPEN INBREUKEN DOOR DE JAREN HEEN

Hacking is de meest voorkomende oorzaak van gegevensverlies en het aantal hackingincidenten neemt snel toe.[2]



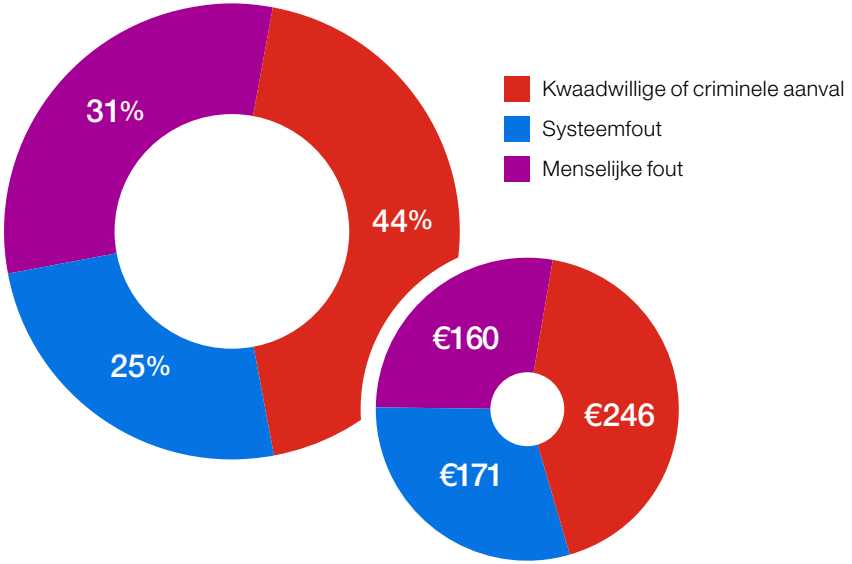
Bovendien zijn de uitgaven bij de afwikkeling van een gegevensinbreuk schrikbarend hoog, ongeacht de omvang van het bedrijf. Hieruit voortvloeiende kostenposten zijn opsporing/forensisch, escalatie, kennisgeving, herstel en inkomsten- en imagoverlies.[3]

€

- gemiddelde kosten na gegevensinbreuk in 2014: **€ 3,4 miljoen**
- gemiddelde kosten door derving in 2014: **€ 1,4 miljoen**
- gemiddeld aantal records dat verloren is gegaan per inbreuk in 2014: **21.158**
- gemiddelde kosten per record waarop inbreuk is gemaakt in 2014: **€ 182**

MEEST VOORKOMENDE TYPEN INBREUKEN EN DAARMEE SAMENHANGENDE KOSTEN PER RECORD

Kwaadwillig hacken is de achterliggende oorzaak van gegevensinbreuken die het meest voorkomt en voor de hoogste kosten zorgt. Andere inbreuken zijn terug te voeren op fouten veroorzaakt door een systeem of een werknemer.[4]



[1] Source: http://blog.mint.com/how-to/data-privacy-day-how-to-keep-your-information-safe-infographic012815/?display=wide
[2] Source: verizonenterprise.com/DBIR/2014
[3] Source: Ponemon Institute LLC 2014 Cost of Data Breach Study: United States
[4] Source: Ponemon Institute LLC 2014 Cost of Data Breach Study

FEIT 2: Elke sector en elk bedrijf, van groot tot klein, loopt risico

Enkele sectoren springen er uit als opvallende doelwitten die bijna de helft (49%) van alle inbreuken in 2014 te verduren kregen. De kosten per record waarop inbreuk is gemaakt, zijn in bepaalde sectoren hoger dan in andere.

SECTOR	2014 %	KOSTEN PER RECORD[2]
Zakelijke & Professionele dienstverlening	17%	€ 203
Detailhandel	14%	€ 114
Financiële dienstverlening	10%	€ 214
Media & Entertainment	8%	€ 166
Bouw & Techniek	8%	Nvt
Overheid & Internationale organisaties	7%	€ 156

SECTOR	2014 %	KOSTEN PER RECORD[2]
Juridische dienstverlening	7%	Nvt
High-Tech & IT	7%	€ 164
Gezondheidszorg	6%	€ 287
Transport	5%	€ 260
Luchtvaart & Defensie	3%	Nvt
Overige	8%	Nvt

60% van de kleine en middelgrote ondernemingen sluit na zes maanden de poorten als gevolg van de schade door een inbreuk

Helaas zijn de meeste kleine organisaties niet in staat om de kosten voor de afwikkeling van een gegevensinbreuk te dragen.[3]

22% kans op een inbreuk op 10.000 records of minder gedurende een periode van twee jaar

Organisaties van alle soorten en maten kunnen getroffen worden. Vooral kleine en middelgrote ondernemingen zijn kwetsbaar omdat de meeste niet over de middelen beschikken om een deugdelijk cyberbeveiligingssysteem op te tuigen.[4]

[1] Bron: FireEye M-Trends 2015 Report
[2] Ponemon Institute LLC 2014 Cost of Data Breach Study
[3] Bron: Stockton, Gary. 'Experian Data Breach resolution Advises Small Businesses to be Prepared for a Data Breach'. Experian Business Information Services. November 2013.
[4] Bron: Ponemon Institute LLC 2014 Cost of Data Breach Study

Feit 3: Geen organisatie is immuun voor zowel interne als externe bedreigingen

Door de staat gesteund
Een groep in dienst van een staatsinstelling.

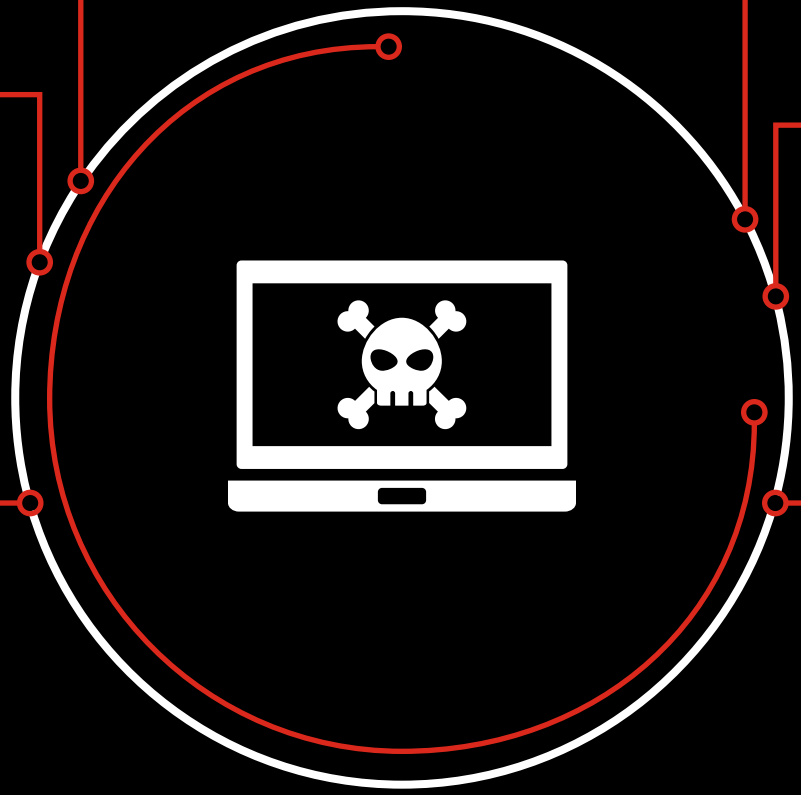
- Chinese staatshackers.
- Russische staatshackers.
- Elektronisch leger van Syrië.

Scriptkiddies
Personen of groepen meestal met beperkte kennis die op eigen initiatief handelen en niet vallen onder een andere dreigingscategorie.

- Een jongere die 'voor de grap' het netwerk van de school doet crashen.
- Personen die websites verminken om indruk op iemand te maken (niet vanuit politieke motieven).
- Groepen die met de botte bijl geprefabriceerde malware of botnets inzetten voor malafide doeleinden.

Hacktivist
Een persoon of groep die aanvallen uitvoert om ergens de aandacht op te vestigen of om te verhinderen dat anderen zich inzetten voor zaken als bijvoorbeeld de vrijheid van meningsuiting.

- Anonymous.
- Lulzsec.
- WikiLeaks.



Georganiseerde misdaad
Criminele groepen die betrokken zijn bij illegale activiteiten om geld af te persen of worden ingehuurd om een aanval uit te voeren.

- Producenten van ransomware.
- Personen die gegevens stelen om ze op de zwarte markt te verkopen.

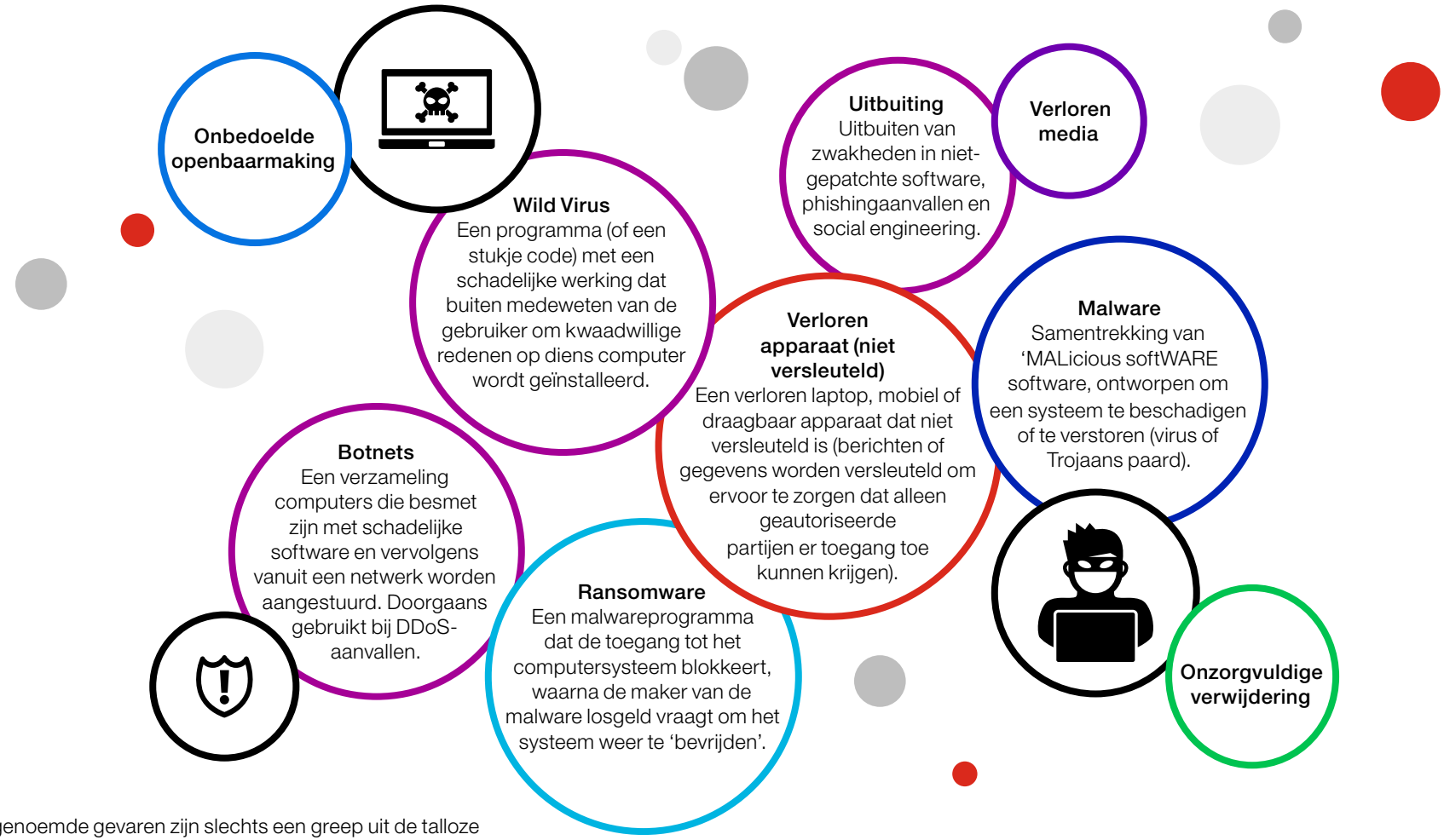
Insiders
Werknemers of andere bevoorrechte gebruikers aangesloten bij een organisatie.

- Aannemers.
- Werknemers.

Cyberterrorist
Iemand die aanvallen uitvoert om angst of paniek te zaaien. De persoon wordt gedreven door ideologische of politieke motieven of maakt deel uit van een bekende terreurgroep.

Bron: https://www.surfwatchlabs.com/threat-categories
https://www.surfwatchlabs.com/threat-categories#Actor

Op uiteenlopende manieren breken cybercriminelen in bij organisaties en profiteren ze van systeemstoringen of menselijk fouten.



Bovengenoemde gevaren zijn slechts een greep uit de talloze mogelijkheden en methoden waar cybercriminelen gebruik van maken

Risico's

Wat zijn de belangrijkste risico's waar risicomanagers en anderen alert op moeten zijn?

First Party-risico's

Omvatten eigen kosten als gevolg van een inbreuk of een datalek:

- Kosten van digitaal forensisch onderzoek (om de omvang en reikwijdte van de inbreuk of van het gegevensverlies vast te stellen) – de kosten kunnen sterk uiteenlopen, afhankelijk van hoe groot of ingrijpend de inbreuk is
- Melden en Inlichten van gedupeerden – de tarieven kunnen nogal verschillen maar veel aanbieders hebben tarieven afgesproken die uiteenlopen van € 1,25 to € 5 per persoon
- Kosten voor public relations en crisismanagement
- Ransomware betalingen door cyberafpersing
- Kosten van herstel van ICT-systemen

Third Party-risico's

Omvatten de kosten die worden gemaakt door inbraak of aansprakelijkheid:

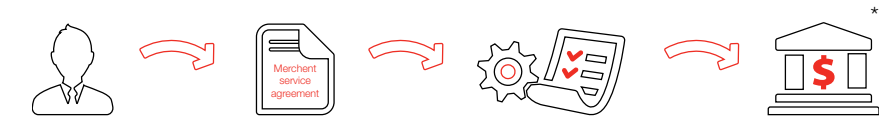
- Kosten voor uitgifte nieuwe betaalkaart
- Kosten van fraude met een betaalkaart
- PCI boetes
- Boetes
  - Boetes opgelegd door de CBP (College Bescherming Persoonsgegevens)
  - Boetes / schadevergoedingen van andere instanties
- Vanwege identiteitsdiefstal
- Vanwege verlies van intellectueel eigendom of vertrouwelijke bedrijfsgegevens van derden
- Vanwege netwerkverstoring
- Lichamelijk letsel als gevolg van verloren gegevens
- Psychische en emotionele schade door openbaarmaking van privégegevens
- Overdracht of verspreiding van een computervirus/-worm of schadelijke software als gevolg van onachtzaamheid

Voorschriften van de Payment Card Industry (PCI)/ Data Security Standard (DSS)

De Payment Card Industry Security Standards Council, waarin Visa, Mastercard, AmEx, Discover en JCB zijn verenigd, is een niet-gouvernementeel samenwerkingsverband dat protocollen heeft opgesteld waaraan handelaren en dienstverleners zich moeten houden. Klanten die de protocollen niet volgen kunnen worden beboet. Kleine landen hebben PCI/DSS-voorschriften opgenomen in hun wetgeving inzake gegevensbescherming.

Overtredingen van PCI/DSS-regels hebben meerdere gevolgen: betaalkaartmaatschappijen leggen wervende banken (banken die handelaren werven voor het aannemen van betaalkaarten) boetes wegens niet-naleving op van € 5.000 tot € 100.000 per maand en banken wentelen deze boetes vaak af op de handelaar.

De betalingsverwerker is er veel aan gelegen niet vast te zitten aan vergoedingen in geval van een schending en banken willen verplichtingen doorgeven aan andere partijen. Als diensten van handelaren of overeenkomsten inzake betalingsverwerking ongunstig uitpakken voor een bedrijf, kan het gebeuren dat alle kosten van schadeloosstelling, inclusief die van frauduleuze debiteringen en voor uitgifte van nieuwe kaarten, voor rekening van dat bedrijf komen.



Raadpleeg de PCI-website om het toepasselijke complianceniveau vast te stellen en om te kijken welke stappen nodig zijn om compliant te worden https://www.pcisecuritystandards.org/

*het schema is een sterk vereenvoudigde weergave van de werkelijkheid. Er kunnen andere tussenpersonen of regelingen aanwezig zijn.

VRAAG HET AAN EEN HISCOX EXPERT

Ik verwerk maar 100 kaarten per jaar, moet ik dan toch PCI-compliant worden? Hoe word ik PCI-compliant?

Volgens de PCI Compliance Guide is de PCI-standaard van toepassing op ALLE organisaties of handelaren die kaarthoudergegevens accepteren, doorgeven of opslaan, ongeacht de omvang van of het aantal transacties. Bedrijven waarvan is vastgesteld dat ze niet compliant zijn, kunnen door de betaalkaartmaatschappijen worden beboet. Raadpleeg de PCI-website om na te gaan onder welke handelaarscategorie u valt en welke stappen nodig zijn om aan de eisen te voldoen.

Ik ben PCI-compliant, dus kan ik in geval van een inbreuk niet verantwoordelijk worden gesteld, klopt dat?

Niet per se. PCI-compliant zijn betekent dat er passende controles zijn ingevoerd ter beveiliging van transacties met betaalkaarten en de opslag, waarbij regelmatig wordt getoetst of de controles aansluiten op de ontwikkelingen in de sector. Ben u PCI compliant, dan scheelt dat aanmerkelijk in de kosten van boetes die kaartuitgevers opleggen en, nog belangrijker, is uw beveiliging up-to-date.

Dekking

Waar moeten bedrijven zich tegen verzekeren om de vele risico's af te dekken?

Een algemeen geldende aanpak om cyber en data risico's adequaat af te dekken bestaat niet. Bedrijven moeten elk hun eigen risico's in kaart brengen en verzekeringen afsluiten ter dekking van de risico's die inherent zijn aan hun specifieke activiteiten.

Privacybescherming

Dekt de kosten van verweer tegen en afwikkeling van claims in verband met de behandeling van persoonsgegevens en vertrouwelijke bedrijfsgegevens. Biedt dekking in geval van nalatigheid, schending van privacy of overtreding van de wetgeving inzake consumentenbescherming, contractbreuk en onderzoeken van regelgevende instanties. Geeft dekking bij problemen door uitval van de netwerkbeveiliging, inclusief overdracht van een virus door onachtzaamheid en onopzettelijke deelname aan een DDoS -aanval gericht tegen een derde.

Kosten van inbreuk

Dekt de kosten in verband met de reactie op een inbreuk, zoals forensisch onderzoek om de inbreuk te bevestigen en vast te stellen, kosten voor melding aan de betrokkenen, kredietbeschermingsdiensten, waaronder kosten voor de bemanning van een callcenter die klanten kan aanbieden te controleren op verdachte transacties, alsmede kosten van crisismanagement en voor public relations.

Cyber business interruption online

Biedt dekking tegen financiële schade, zoals verlies aan inkomsten wanneer netwerkafhankelijke bedrijfsactiviteiten stil komen te liggen. Vroeger waren bedrijfsstagnaties het gevolg van brand, overstroming enz., maar door de voortschrijdende techniek zijn er nieuwe gevaren ontwikkeld zoals virussen, programmeerfouten en computerhacking.

Schade door hackers

Dekt de kosten van het hercreëren of herstellen van beschadigde gegevens, systemen of programma's. In een digitale wereld bestaat eigendom uit meer dan alleen materiële zaken. Het is dus nodig om een specifieke verzekering af te sluiten waarmee kosten voor het herstel van immateriële activa in de vorm van gegevens kunnen worden gedekt.

Cyberafpersing

Dekt de kosten van verweer en van adviseurs die onderzoek doen en assistentie verlenen. Ook wordt de schade vergoedt tot het betalen van losgeld of geëiste zaken of diensten.

Cyber aansprakelijkheid (multimedia)

Dekt de kosten van verweer tegen en afwikkeling van claims die voortvloeien uit online-content op een website of op sociale media (volgens welke reclameteksten of -brochures lasterlijk zijn of inbreuk maken op handelsmerken). Websites van bedrijven, sociale media en digitale reclame zijn kwetsbaar. Bovendien bestaat het gevaar van cybersquatting.

Voor meer informatie over producten van Hiscox kunt u contact opnemen met uw lokale adviseur.

Risicobeheersing

Een alomvattende benadering van privacybeveiliging is noodzakelijk om het risico van gegevensinbreuk en de schade na een inbreuk te beperken. Met een combinatie van best practices, verzekering en een responsplan kan de preventie van en de reactie op gegevensinbreuken strategisch worden benaderd.

Waarom is risicobeheersing belangrijk?[1]

- Aangetoond is dat de gemiddelde kosten van een gegevensinbreuk € 14 per record lager uitvallen wanneer een solide veiligheidsbeleid wordt gehanteerd.

- Gebleken is dat de gemiddelde kosten van een gegevensinbreuk € 6 per record lager uitvallen bij aanstelling van een privacy officer.

Hoe kunnen bedrijven hun risico beperken?[2]

- ✓ Neem privacy- en gegevensbescherming integraal op in de bedrijfscultuur
- ✓ Belast één enkele persoon met de eindverantwoordelijkheid voor beveiliging en gegevensbescherming
- ✓ Implementeer een programma voor continue opleiding en bewustmaking van het personeel
- ✓ Zorg voor waterdichte contracten met leveranciers en relaties
- ✓ Identificeer en classificeer de door de organisatie verzamelde en opgeslagen informatietypen/ soorten
- ✓ Beperk het aantal verzamelde en bewaarde persoonsgegevens en vertrouwelijke informatie tot het strikt noodzakelijke minimum
- ✓ Evalueer en actualiseer de bestaande veiligheidsmaatregelen, -plannen en -procedures
- ✓ Voer continu risicobeoordelingen uit en ga na hoe de vastgestelde risico's kunnen worden vermeden of beperkt
  - — Administratieve voorzorgsmaatregelen
  - — Fysieke voorzorgsmaatregelen
  - — Technische voorzorgsmaatregelen
- ✓ Bereid u voor op incidenten
- ✓ Verklein de risico's met Cyber en Data Risks by Hiscox

[1]Ponemon Institute, 2014 Cost of Data Breach Study
[2]ePlace BreachProtection™

De tools van Hiscox voor risicobeheersing helpen bij het voorkomen en aanpakken van alle aspecten van een inbreuk op persoonsgegevens en vertrouwelijke informatie.

Dienstverlening voorschadepreventie

- Guide of risksscan – mede mogelijk gemaakt door onze partners
- Eén uur juridische dienstverlening en advisering als hulp bij risicobeheersing
- Schadepreventie en advisering – mede mogelijk gemaakt door eRisk Hub® en NetDiligence®

Breach Respons Team

- Stappenplan dat uiteenzet welke maatregelen na een gegevensinbreuk genomen moeten worden – mede mogelijk gemaakt door eRisk Hub® en NetDiligence®
- Eén gratis uur begeleiding en advies om uw reactie na een inbreuk op poten te zetten (mobiele app beschikbaar) – mede mogelijk gemaakt door eRisk Hub® en NetDiligence®
- Een lijst van dienstverleners die tegen vooraf bepaalde tarieven hulp bij inbreuken verstrekken – mede mogelijk gemaakt door eRisk Hub® en NetDiligence®
- eRisk-directory van externe deskundigen uit vakgebieden die de aanloop naar en de nasleep van een inbreuk bestrijken – mede mogelijk gemaakt door eRisk Hub® en NetDiligence®
- Specifiek crisismanagementteam belast met het indammen en beheersen van gevallen van cyberafpersing – mede mogelijk gemaakt door Control Risks

Maak kennis met onze partners in de bestrijding van inbreuken

Control Risks
Sinds 1975 heeft Control Risks bij 2.600 afpersingszaken in 129 landen adviezen verstrekt aan klanten. Een toegewijd team van specialisten houdt zich jaarlijks bezig met gemiddeld 155 afpersingszaken, waaronder afpersing met bedreiging. Daarnaast beschikt Control Risks over een gespecialiseerd team dat zich richt op cybercriminaliteit, waaronder cyberafpersing.

Risk Management Assistance
Het eerste vertrouwelijke consult is kosteloos. Daarnaast wordt één uur gratis juridisch advies verstrekt waarbij inzicht wordt gegeven in de risico's en wordt uiteengezet hoe risico's die gewoonlijk leiden tot het soort claims die onder een privacypolis van Hiscox vallen, zoveel mogelijk kunnen worden beperkt. Voor vragen over het minimaliseren van zakelijke risico's kunnen onze polishouders zich wenden tot een erkend advocatenkantoor met een specialisatie op het gebied in kwestie.

eRisk Hub® Breach Response Resources
eRisk Hub®, mede mogelijk gemaakt door NetDiligence®, stelt tools en middelen beschikbaar om onze polishouders te helpen inzicht te krijgen in de risico's, een responsplan op te stellen en de gevolgen van een gegevensinbreuk op een organisatie zoveel mogelijk te beperken. De tools en diensten voorzien in een stappenplan dat uiteenzet welke maatregelen na een gegevensinbreuk genomen kunnen worden, toegang tot begeleiding en advies om de reactie na een inbreuk te formuleren (gratis eerste consult), en een eRisk-directory waarmee externe deskundigen uit vakgebieden die de aanloop naar en de nasleep van een inbreuk bestrijken, snel kunnen worden getraceerd.

Zie pagina 26 voor disclaimers.

VRAAG HET AAN EEN **HISCOX EXPERT**

Wat gebeurt er als er is ingebroken op mijn systeem? Met wie neem ik contact op?
Als uw organisatie niet over een Incident Respons Plan beschikt, hebt u hopelijk gebruikgemaakt van de diensten met toegevoegde waarde die wij onze polishouders aanbieden voor het opzetten van een plan van aanpak bij incidenten. Neem contact op met uw verzekeringsagent en kijk in uw verzekeringspolis wat u moet doen om de schade in te dienen. Als polishouder van Hiscox heeft u toegang tot een 24 uur per dag bereikbare telefoonnummer, een leveranciersportal (eRisk Hub) met de betreffende contactpersonen en een van de meest ervaren schadeafhandelingsteams in het land. Schadeclaims worden bij Hiscox binnen 24 uur bevestigd. Vanwege de uiterst complexe nationale regelgeving voor melding van gegevensinbreuken is het belangrijk dat onze verzekerden tijdig in actie komen en een responsteam paraat hebben.

Kan ik een beroep doen op mijn eigen voorkeursaanbieders? Zo ja, hoe verloopt dan de procedure?
Hiscox bouwt aan sterke banden met onze leveranciers en is tarieven overeengekomen die de responskosten zoveel mogelijk beperken. Indien uw een beroep wilt doen op een aanbieder die niet met Hiscox samenwerkt, kunnen wij daarmee akkoord gaan. U moet dan de naam, ervaring en achtergrond van het bureau opgeven, alsmede diens relevante specialismen, tarieven en tariefstructuren. Het is raadzaam om direct schriftelijke toestemming te vragen wanneer u een beroep doet op uw verzekeringspolis; dan hoeft u dat niet meer te doen wanneer de chaos na een inbreuk heeft toegeslagen.

Claims Scenarios

Elk bedrijf loopt privacyrisico's. Hieronder zijn verschillende scenario's uitgewerkt waarin bedrijven te maken krijgen met kosten als gevolg van inbreuken op de privacy.

Accountantskantoren
Bij een accountantskantoor gaat een backupstation verloren waarop namen, adressen en BSN-nummers van alle belastingklanten zijn opgeslagen. Omdat op het station persoonsgegevens werden bewaard, moet elke klant worden benaderd en moet aan elk van hen fraudecontrole worden aangeboden, ongeacht of er ooit wat met de informatie zal worden gedaan.

Een computersysteem van een accountantskantoor wordt gehackt, waardoor betalingsgegevens van honderden klanten gevaar lopen. Het kantoor moet opdraaien voor de kosten van alle gedupeerde klanten en voor de kosten van uitgifte van nieuwe creditcards.

Het computersysteem van een accountantskantoor wordt gehackt. De BSN-nummers en financiële gegevens van belastingaangiftes van duizenden klanten zijn in het geding, evenals de gegevens van alle vaste en tijdelijke werknemers. Het kantoor moet alle getroffen partijen inlichten en fraudecontrolediensten aanbieden.

Reclamebureaus
Een ontevreden werknemer van een bureau voor digitale reclame geeft vertrouwelijke gegevens over gevolgd klikgedrag door aan een concurrent van een klant van het bureau. De klant daagt het bureau voor de rechter vanwege contractbreuk en nalatigheid.

Een reclamebureau zet een nieuwe reclamecampagne op voor een prominente klant. De campagne lekt uit voor de geplande lanceringsdatum, reden voor de klant om het bureau voor de rechter te dagen.

Landbouw
Een werknemer van een veevoerleverancier verliest een laptop waarop gevoelige gegevens, waaronder factuurgegevens, van zijn klanten zijn opgeslagen. Hoewel niet zeker is of er ooit wat met die gegevens zal worden gedaan, is het de verantwoordelijkheid van de leverancier dat alle bedrijven waarvan de gegevens zijn gecompromitteerd op de hoogte worden gesteld.

Het computersysteem van een groot agrarisch bedrijf wordt gehackt. Gevoelige gegevens, waaronder namen, BSN-nummers en geboortedata komen op straat te liggen. Het bedrijf moet al zijn vaste en seizoensmedewerkers inlichten en fraudecontrolediensten aanbieden.

Biotechnologische en farmaceutische bedrijven
Een farmaceutisch bedrijf is halverwege een grote klinische proef van een veelbelovend geneesmiddel. Het computersysteem wordt gehackt waardoor gevoelige patiëntinformatie, waaronder BSN-nummers en medische gegevens, wordt gecompromitteerd. Het bedrijf moet alle getroffen patiënten op de hoogte stellen en fraudecontrole aanbieden. Bovendien moet de proef worden gestopt en worden overgedaan.

Een biotechnologisch bedrijf werkt aan een nieuw genetisch gemodificeerd voedingsproduct. Gegevens over het onderzoek komen voordat de studie is voltooid onbedoeld via e-mail terecht bij een mediabedrijf. De voedingsmiddelenfabrikant daagt het laboratorium voor de rechter.

Energie
Het computersysteem van een leverancier van zonne-energie wordt gehackt waardoor de betaalgegevens van alle klanten alsmede gevoelige persoonsgegevens op straat komen te liggen. De kosten voor kennisgeving aan alle getroffen personen en de verlening van fraudecontrolediensten moeten door de leverancier worden betaald.

De bouw
De computers van een bouwbedrijf worden besmet met een virus dat onbedoeld wordt doorgegeven aan potentiële en bestaande klanten en aan leveranciers. Het bedrijf is aansprakelijk voor de kosten die zij moeten maken om het virus te verwijderen en gegevens te herstellen.

De vertrouwelijke ontwerpplannen voor een project voor de ontwikkeling van multifunctionele gebouwen worden door een ontevreden medewerker van de aannemer die de bouwopdracht heeft binnengehaald, gelekt naar een concurrent. De projectontwikkelaar daagt de aannemer voor de rechter wegens schending van de geheimhoudingsovereenkomst.

Adviesbureaus
Bij een bureau voor personeelsadvisering raakt iemand een laptop kwijt. Namen, adressen en BSN-nummers van honderden contractmedewerkers waren er in opgeslagen. Ongeacht of de informatie ooit wordt verspreid, moet het bureau de getroffen werknemers inlichten en fraudecontrole aanbieden.

Enkele consultants van een bureau voor managementadvies werken tijdens een project op locatie bij een klant. Een van de consultants stuurt per ongeluk een vertrouwelijk memo naar een grote e-maillijst met adressen van zowel interne als externe ontvangers. De klant daagt het adviesbureau voor de rechter.

Amusement
De nieuwe single van een populaire artiest wordt door een medewerker van een platenbedrijf per ongeluk vrijgegeven aan sites waar gratis muziek kan worden gedownload. De artiest daagt het bedrijf voor de rechter wegens gederfde royalty's.

Gaming
Een game-hostingbedrijf wordt gehackt waardoor verschillende populaire gamingsites enkele dagen plat liggen. De ontwikkelaars van de games dagen het hostingbedrijf voor de rechter wegens gederfde royalty's.

Een populaire online game-franchise bereidt de lancering voor van de nieuwste versie van zijn flagship-product. Er had een demoversie klaar moeten staan om te worden gedownload, maar in plaats daarvan is de volledige versie klaargezet, die vervolgens door duizenden gebruikers gratis wordt gedownload. De ontwikkelaar, marketeer en anderen leiden schade door gederfde inkomsten.

Overheidsinstellingen
Het computersysteem wordt gehackt van een overheidsinstelling die toeziet op een programma voor volwassenen personen met een handicap. De persoonsgegevens van de deelnemers aan het programma zijn gecompromitteerd. De instelling is verplicht om de getroffen deelnemers en hun zorgverleners of wettelijke vertegenwoordigers in te lichten en fraudecontrolediensten aan te bieden.

Advocatenkantoren
Het computersysteem van een advocatenkantoor wordt gehackt waardoor vertrouwelijke informatie over spraakmakende echtscheidingszaken bij de media terechtkomt. Het kantoor wordt door beide partijen in de echtscheidingszaak voor de rechter gedaagd.

Een nieuwe medewerker in een advocatenkantoor gooit een afschrift van vertrouwelijke betalingsinformatie van klanten in de openbare papiercontainer in plaats van het document door de papierversnipperaar te halen. Het kantoor moet de klanten ervan in kennis stellen dat hun gegevens mogelijk gecompromitteerd zijn en hun fraudecontrole aanbieden.

Een laptop van een advocatenkantoor dat gespecialiseerd is in collectieve rechtszaken wordt gestolen. Er staat gevoelige informatie op, zoals BSN-nummers en medische gegevens, van een groot aantal eisers in een geding tegen een fabrikant van medische apparatuur. Het advocatenkantoor moet de eisers inlichten en fraudecontrolediensten aanbieden.

Productie
Een uitvinder geeft een fabrikant de opdracht een beperkt aantal producten te vervaardigen waarop nog geen octrooi is verleend. Een werknemer van de fabrikant verstuurt per ongeluk een e-mailbericht met de productspecificaties aan potentiële concurrenten. De fabrikant wordt voor de rechter gedaagd wegens schending van de geheimhoudingsovereenkomst en andere schade.

Het computersysteem van een productiebedrijf wordt gehackt waardoor de gevoelige gegevens van alle voltijd- en contract medewerkers zijn gecompromitteerd. Het bedrijf moet alle getroffen werknemers inlichten en fraudecontrole aanbieden.

Mediabedrijven
Een mediabedrijf ontwikkelt een uitgebreid mediaplan voor een nieuw product van een klant. Een e-mailbericht met daarin vertrouwelijke gegevens over het product die bedoeld zijn voor de klant, wordt per ongeluk verzonden naar de e-mailadressen op een persdistributielijst, waardoor de buitenwereld ruim vóór de lancering al op de hoogte is van de productgegevens. De klant daagt het mediabedrijf voor de rechter wegens contractbreuk en andere schade.

Op het computersysteem van een mediabedrijf zijn grote hoeveelheden statistische gegevens van klanten opgeslagen, waaronder sleutelwoorden voor zoekmachine-optimalisatie, betaling-per-klik-campagnes, enz. Het systeem wordt gehackt en alle gegevens lopen gevaar. Een aantal klanten spant een rechtszaak aan wegens vermeende nalatigheid.

Non-profitorganisaties
Een non-profitorganisatie raakt een laptop kwijt waarop de lijst van donoren is opgeslagen. De organisatie moet iedereen die op de lijst staat inlichten en fraudecontrole aanbieden, ongeacht of de informatie ooit wordt verspreid.

Uitgeverijen
Een bekende schrijver schrijft onder pseudoniem een nieuw boek in een ander genre. De uitgever spreekt met de schrijver af dat de ware identiteit van de schrijver niet wordt onthuld maar een ontevreden medewerker lekt de echte naam van de schrijver naar de pers. De schrijver daagt de uitgever voor de rechter wegens contractbreuk.

Het computersysteem voor orderverwerking van een uitgever van e-books wordt gehackt en gevoelige betalingsgegevens worden gecompromitteerd. De uitgever moet al zijn klanten inlichten en aanbieden gedurende een jaar fraudecontrolediensten te verlenen. De kosten daarvan zijn voor zijn rekening.

Detailhandel
In een winkel wordt het POS-systeem gehackt waardoor de nummers van betaalpassen en creditcards van duizenden klanten op straat komen te liggen. De winkel moet de uitgevers van de kaarten inlichten, de kosten voor vervanging van de kaarten betalen en fraudecontrolediensten aanbieden aan de gedupeerden.

IT-ontwikkelaars
Een ontwikkelaar verliest een back-upstation waarop de code voor een nieuwe applicatie is opgeslagen. De klant daagt de ontwikkelaar voor de rechter wegens nalatigheid en de ontstane schade door vertraging in de uitrol van het project.

Aanbieders van technische diensten
Door een probleem in een servicesysteem van een aanbieder wordt de website en het intranet van verschillende klanten platgelegd. De aanbieder wordt aangeklaagd wegens schade door bedrijfsstagnatie en de kosten voor herstel van verloren gegane gegevens.

Telecommunicatie
Het computernetwerk van een aanbieder van telecommunicatiediensten wordt gehackt waardoor inbreuk is gepleegd op de betalingsgegevens van duizenden klanten. De aanbieder is verplicht om alle gedupeerde klanten in te lichten, de kosten te betalen voor het uitgeven van nieuwe creditcards, te betalen in geval van fraudeaangiften en fraudecontrole aan te bieden. Hij draait bovendien op voor boetes omdat hij verzuimd heeft gevoelige gegevens te versleutelen.

Vakbonden
Een laptop waarop persoons- en pensioengegevens zijn opgeslagen van gepensioneerde vakbondsmedewerkers wordt kwijtgeraakt. Ongeacht of de gegevens ooit worden verspreid, moet de vakbond alle gedupeerde gepensioneerden inlichten en fraudecontrolediensten aanbieden.

Ontwikkeling van websites
Een ontwikkelaar ontwerpt een nieuwe website voor een e-commercebedrijf. De site gaat de lucht in maar crasht daarna onmiddellijk. De ontwikkelaar doet er drie dagen over om het probleem op te lossen. Ondertussen ligt de site stil. Het bedrijf daagt de ontwikkelaar voor de rechter wegens schade door gederfde inkomsten.

Een zorgverzekeraar lanceert een nieuwe website maar het wachtwoordsysteem werkt niet goed waardoor onbevoegden toegang hebben tot persoonsgegevens van leden. De verzekeraar klaagt de ontwikkelaar aan voor de kosten van kennisgeving aan de leden en de levering van fraudecontrolediensten.

Veelgestelde vragen

Het thema privacy is met veel verwarring omgeven. Hieronder wordt getracht licht te werpen op veelgestelde vragen van klanten over risico's op het gebied van privacy en de dekking daarvan.

CYBER EN DATA RISKS VERZEKERING PRIVACYPOLIS

Welk risico loopt een klant? De risico's betreffen in het algemeen de persoonsgegevens die zij onder beheer hebben, zoals BSN-nummers, rijbewijsnummers, gegevens van betaalkaarten waarmee goederen, diensten en rekeningen worden betaald, gevoelige gegevens van klanten, verzamelde medische gegevens, enz.

Waarom moet u weten over hoeveel records een bedrijf beschikt? Hoe hoger het aantal gegevensrecords, des te hoger het risico én de kosten na een inbreuk.

WAAROM MIJN KLANT EEN CYBER EN DATA RISKS POLIS NODIG HEEFT

Mijn andere polis biedt al dekking hiervoor. Is dat niet voldoende? Mogelijk, maar meestal niet. In de meeste gevallen is de dekking zeer beperkt en wordt slechts een gering bedrag in euro's toegekend. Het kan bijvoorbeeld zijn dat alleen de Third Party-kosten worden vergoed of dat de maximumdekking voor First Party-kosten beperkt is tot slechts € 50.000. Een complete verzekeringspolis bij inbreuken op privacy en gegevens is profijtelijk voor elk bedrijf en biedt de geruststelling dat de kosten van een potentiële inbreuk geen ontwrichtende werking zullen hebben op de bedrijfsvoering.

Als mijn werkelijke risico alleen First Party-gegevens betreft (zoals gegevens van werknemers), heb ik dan zo'n polis dan wel nodig? Elk bedrijf heeft de taak en verplichting om namens werknemers beheerde gegevens te beschermen. Hetzelfde geldt voor vertrouwelijke gegevens van het bedrijf zelf. Geen enkel bedrijf is immuun tegen aanvallen. Een polis van Hiscox biedt dekking voor werknemersgegevens.

Ik ben geen doelwit zoals Sony, KPN of AMSL. Waarom zou ik me zorgen maken? Grote bedrijven halen het nieuws. Kleine niet. Niettemin, als het gaat om inbreuken op gegevens is het niet de vraag of het gebeurt, maar wanneer het gebeurt. Er bestaat een zwarte markt waar gestolen gegevens worden gekocht en verkocht, en hackers worden steeds slimmer. Target, KPN, Sony en andere grote organisaties hebben complete afdelingen die zich bezighouden met het analyseren van de risico's waaraan het bedrijf is blootgesteld en die meewerken aan het opzetten van beleid en procedures waarmee ze zichzelf kunnen beschermen, maar hackers weten nog steeds gaten in de verdediging te slaan. Kleinere bedrijven die geen netwerkbeveiligers in dienst hebben en niet de middelen hebben om hun gegevens te beschermen, zijn voor hackers een gemakkelijke prooi.

Wie sluit tegen cyberrisico's een dekking af? Bedrijven die dit toenemende risico willen beperken. Het wordt een 'must have'-dekking.

Waarom zou ik twijfelen aan mijn IT-afdeling als ze zeggen dat ze al hun zaakjes op orde hebben? Target, Sony en andere grote bedrijven hebben complete afdelingen die zich bezighouden met IT-beveiliging maar ze bleken kwetsbaarder dan ze dachten. Eén simpele fout of vergissing, zoals het niet updaten van software, het niet instellen van de juiste procedures voor authenticatie van derdenleveranciers, het kwijtraken van een niet-versleutelde laptop waarop gevoelige gegevens zijn opgeslagen, of een medewerker met kwaad in de zin, kan leiden tot een inbreuk. De risico's groeien mee met de technologische ontwikkelingen en hackers gaat steeds slimmer en geraffineerder te werk.

Heb ik deze dekking wel nodig als ik gegevens van klanten niet opsla op mijn netwerk? Ja. U slaat klantgegevens weliswaar niet op, maar u hebt er wel toegang tot. Uzelf kunt de oorzaak zijn van een inbreuk op gegevens van uw klanten en zo contractbreuk veroorzaken. Bedrijfsinformatie valt eveneens onder de dekking van een polis tegen inbreuk op gegevens en privacy. Aansprakelijkheid bestaat ook voor gegevens van werknemers.

Ik heb maar een heel klein bedrijf. Loop ik dan nog steeds enig risico van inbreuk op gegevens? Elk bedrijf is blootgesteld aan privacyrisico's, hetzij via gevoelige gegevens van werknemers, hetzij via betalingen die van derden worden geïnd, geleverde diensten enz. Sommige risico's zijn groter dan andere maar het is belangrijk om te benadrukken dat elk bedrijf met werknemers in dienst aansprakelijk is voor verlies van Third Party-gegevens (met inbegrip van gegevens van werknemers). Een inbreuk kost het kleinste bedrijf met de geringste risico's gemiddeld €188.000. De kosten stapelen zich razendsnel op.

De verwerking van betaalkaarttransacties besteed ik uit aan een derde. Op dat gebied loop ik dus geen risico, klopt dat? Volgens de PCI Compliance Guide, geldt de PCI-standaard voor ALLE organisaties of handelaren, ongeacht de omvang van of het aantal transacties, die gegevens van kaarthouders accepteren, doorgeven of opslaan. En het simpele feit van uitbesteding aan een derde partij ontslaat u niet van de plicht te voldoen aan de PCI-voorschriften. Misschien kunt u zo het risico verminderen en daarmee de PCI-compliance wat vergemakkelijken, maar dat betekent nog niet dat er volledig aan PCI voorbij kan worden gegaan.

Als mijn klantgegevens zijn opgeslagen in de cloud berust de aansprakelijkheid toch bij de cloudaanbieder? Dat is niet zeker. Het is in het belang van de verzekerde om contracten op dit gebied zorgvuldig door te spreken met een juridisch adviseur. Zelfs als het risico beperkt is, kan het nog steeds dat de aansprakelijkheid bij de verzekerde wordt gelegd.

DE FEITEN

Welke sectoren sloten altijd al aansprakelijkheidsverzekeringen af en welke sectoren zijn daar bijgekomen? De meeste aansprakelijkheidsverzekeringen worden afgesloten door banken, gezondheidszorginstellingen en bedrijven in de technische branche. Ze worden tegenwoordig ook steeds meer afgesloten door bedrijven van uiteenlopende grootte en uit uiteenlopende sectoren, overheden, onderwijsinstellingen en producenten.

Wat zijn de gemiddelde kosten van een gegevensinbreuk? De gemiddelde kosten blijven schommelen maar liggen volgens toonaangevende bronnen uit de wereld van de cyberbeveiliging op zo'n € 188.000. Hoe groter het bedrijf, des te hoger de kosten. Maar ongeacht de grootte van het bedrijf geldt wederom: hoe meer gevoelige gegevens het bedrijf verzamelt, des te hoger de kosten.

RISICO'S

Hoe gaat cybercriminaliteit in zijn werk? Het volgende scenario ontspint zich: Een hacker die zich voordoet als leverancier, klant of werknemer krijgt een werknemer van de verzekerde zo ver dat die geld overmaakt op de rekening van de hacker. De misleiding kan de vorm aannemen van phishing, spear phishing en andere trucs die door middel van e-mail, text message, instant message, de telefoon of andere elektronische middelen worden uitgehaald.

Wat is een record precies? Wat doe ik als ik meerdere bestanden van dezelfde persoon in mijn bezit heb? Wilt u weten om hoeveel records het in totaal gaat of hebt u alleen het aantal personen nodig? Niet-openbare persoonsgegevens zoals bepaald in nationale, regionale, plaatselijke of buitenlandse wet- of regelgeving kunnen bestaan uit, maar zijn niet beperkt tot, onbeveiligde vertrouwelijke gezondheidsinformatie, BSN-nummers, persoonsgebonden belastingidentificatienummers, rijbewijsnummers, nummers van een identiteitskaart of paspoort, bankrekeningnummers en nummers van betaalpassen of creditcards. Wat wij willen weten is het aantal afzonderlijke gegevenselementen die een verzekerde in totaal bezit. Indien meerdere gegevenselementen van dezelfde persoon zijn opgeslagen in het netwerk van de verzekerde of op locatie bij de verzekerde, willen wij informatie hebben over de ter plekke gehanteerde bewaar- en duplicatieprocedures.

Hebben privacypolissen gevolgen voor websites? Ja, want deze polissen zijn in veel opzichten te beschouwen als een overeenkomst met uw klanten. Belangrijker nog, als u uw gegevensbeschermingsprocedures geheim wilt houden en niet wilt vertellen met wie u gegevens van anderen deelt, kan dat in strijd zijn met privacyregelgeving.

Aan welke regelgeving zijn bedrijven in het algemeen onderworpen? Voor gegevens van betaalkaarten de PCI/DSS-regels. Deze gegevens zijn samen met BSN-nummers, financiële en medische gegevens enz. ook onderworpen aan nationale, regionale en lokale voorschriften.

Waarom is het zo belangrijk om aan de PCI-regels te voldoen? Wat gebeurt er als ik die regels niet naleef? Iemand die zich niet houdt aan de PCI-regels kan een boete krijgen van kaartuitgevers en voor de rechter worden gedaagd door diverse partijen die opkomen voor boze consumenten die slachtoffer zijn van inbreuken op hun gegevens.

Mijn Point-of-Sale-leverancier zegt dat hij PCI-compliant is. Dat betekent dat ik ook compliant ben, klopt dat? Niet per se, de meeste handelaren zijn blootgesteld aan enig risico. De enige manier om volledig te ontkomen aan de noodzaak om PCI-compliant te worden, is door uitbesteding van het gehele betalingsverwerkingsproces. In de meeste gevallen wordt bij de verwerking een beroep gedaan op in ieder geval een deel van uw netwerkinfrastructuur. Dit betekent dat ook handelaren onderworpen zijn aan de PCI-standaard.

Wat is het verschil tussen een boete en een assessment van de PCI? Uitgevers van betaalkaarten (Visa, Mastercard enz.) kunnen naar eigen goeddunken boetes opleggen die variëren van € 5.000 tot € 100.000 per maand voor overtreding van de PCI-voorschriften. De boetes hebben een punitief doel en hebben geen betrekking op schadevergoeding aan banken door fraude met betaalkaarten. PCI-assessments gaan gepaard met aansprakelijkheden en kosten die zijn uitgewerkt in een overeenkomst inzake diensten van handelaren of inzake betalingsverwerking. Dergelijke overeenkomsten kunnen bepalingen bevatten inzake kosten voor uitgifte van nieuwe passen en van frauduleuze debiteringen na een inbreuk.

DEKKING

Wat is het verschil tussen First Party- en Third Party-dekking en wat is hun respectieve belang? Met een First Party-verzekering dekt de verzekerde zijn eigen schade als gevolg van kennisgeving aan gedupeerden, digitaal forensisch onderzoek om na te gaan hoe de inbreuk heeft kunnen plaatsvinden, herstel, bedrijfsstagnatie enz. Met een Third Party-verzekering dekt de verzekerde de kosten als gevolg van aansprakelijkheid collectieve rechtszaken en andere aanspraken die door externe partijen worden ingesteld.

Wat zijn vertrouwelijke bedrijfsgegevens als handelsgeheimen buiten beschouwing worden gelaten? In dat geval hebben vertrouwelijke bedrijfsgegevens betrekking op informatie waarvan openbaarmaking schade zou toebrengen aan het bedrijf. De informatie kan bestaan uit verkoop- en marketingplannen, productplannen, documenten over ontwerpen en uitvindingen, gegevens over klanten en toeleveranciers, financiële gegevens enz. die naar hun aard niet openbaar zijn.

Aan welke limieten moet ik denken? Dat hangt af van de grootte van het bedrijf en van het risico. De limieten stijgen navenant mee met de grootte van het bedrijf en de gevoeligheid van de gegevens.

Wat houdt 'dekking per persoon' in? In plaats van een waarde in euro's te bepalen voor meldings- en fraudecontrolekosten stelt de verzekeraar het maximumaantal personen vast die tegen deze schade zijn gedekt (geen vastgesteld eurobedrag).

Dekt een cyberverzekeringspolis het rechtstreeks verlies van gelden? De meeste cyberverzekeringspolissen zijn bedoeld om de schade door verlies van gegevens, niet van gelden (rechtstreeks) te dekken. Bij Hiscox kunnen we voor bepaalde risico's de dekking uitbreiden. Onze polis tegen cybercriminaliteit biedt dekking tegen inbreuken op gegevens, bijvoorbeeld bankgegevens die worden gestolen om rekeningen van bedrijven of instellingen te plunderen.

Biedt de polis dekking tegen 'social engineering'? Social engineering is een methode om personen door misleiding beveiligde gegevens afhandig te maken. Slachtoffers van social engineering zijn kwetsbaar door hun ingeboren aard om anderen te vertrouwen en te willen helpen. De meeste verzekeringspolissen dekken verlies van gegevens ongeacht hoe het verlies tot stand is gekomen, al moet wel goed worden gekeken wat de polis hier precies over zegt.

Dekt de polis ook gegevensverlies veroorzaakt door malafide medewerkers? De meeste verzekeringspolissen dekken de kosten van gegevensverlies ongeacht de wijze waarop het verlies zijn beslag heeft gekregen. Er zijn echter ook polissen die gegevensinbreuken veroorzaakt door malafide medewerkers uitsluiten. De dekking van de verzekeringspolissen van Hiscox tegen standaardinbreuken op gegevens door malafide medewerkers is overeenkomstig de voorwaarden van de polis, maar bepaalde situaties waarbij leidinggevend personeel van de organisatie betrokken is, kunnen in de polis zijn uitgesloten.

Zijn ook gegevens op papier gedekt? In bijna alle polissen op dit gebied zijn papieren gegevens meeverzekerd, maar het is zaak de polis hier altijd even op na te slaan. De polis van Hiscox voor privacybescherming definieert persoonsgegevens als gegevens in enigerlei vorm die onder uw zorg, beheer en toezicht staan, of die onder zorg, beheer en toezicht staan van om het even welke derde voor wie u volgens de wet aansprakelijk bent. Een inbreuk op papieren gegevens zou vallen onder de standaardbepalingen van de Hiscox-polis.

Is er wereldwijde dekking? Wat houdt dat precies in? Moet de zaak worden voorgelegd aan een rechtbank in de Verenigde Staten? Wij bieden wereldwijde dekking maar onze jurisdictie bij claimsafhandeling beperkt zich tot het juridisch rechtsgebied zoals vermeld op de polis.

Biedt de polis ook dekking tegen offlinerisico's? Zowel digitale als papieren gegevens vallen onder de polisdekking.

RISICOBEHEERSING

Waarom is het belangrijk om personeel te instrueren? In een groot aantal gevallen is het verlies aan gegevens te wijten aan de onachtzaamheid van een werknemer, bijvoorbeeld doordat hij of zij een laptop in een taxi of vliegtuig heeft laten liggen, persoonsgegevens per ongeluk naar de verkeerde e-mailadressen heeft gestuurd, of simpelweg in een gesprek die plaatsvindt in het publieke domein privégegevens heeft onthuld. Werknemers moeten leren om zorgvuldig en discreet met dergelijke informatie om te gaan.

Waarom is het afsluiten van overeenkomsten inzake handelaarsdiensten belangrijk? Bij overeenkomsten die u sluit met betalingsverwerkers is er vaak een aansprakelijkheid jegens banken in geval van een inbreuk op gegevens van betaalkaarten. De kleine lettertjes kunnen ervoor zorgen dat u met veel meer akkoord gaat dan u denkt.

Wat is versleuteling? Informatie zodanig coderen dat alleen bevoegden er toegang toe hebben. Versleuteling is zeer belangrijk bij het beoordelen van de risico's, omdat een inbreuk op versleutelde gegevens aanzienlijk minder kosten met zich brengt dan een inbreuk op onversleutelde gegevens. Versleuteling is een waarborg in veel zaken die betrekking hebben op wettelijke bepalingen inzake privacybescherming.

Onze laptops zijn met wachtwoorden beschermd. Is dat niet voldoende? Houdt dit in dat ze versleuteld zijn? Nee. Versleuteling is het coderen van gegevens op een harde schijf om ze onbruikbaar te maken totdat ze met een versleutelingscode weer worden gedecodeerd. Beveiliging met alleen een wachtwoord betekent simpelweg dat een hacker het wachtwoord kan omzeilen om zich toegang te verschaffen tot intacte, niet-versleutelde gegevens.

Wat is het verschil tussen versleuteling en bescherming met een wachtwoord? Hoe versleutelt mijn bedrijf gegevens? Versleuteling is een methode waarmee berichten of gegevens met gecodeerde symboolreeksen onbruikbaar worden gemaakt. De methode wordt doorgaans gebruikt voor de beveiliging van onlinecontact met banken en voor de bescherming van creditcardgegevens. Bij onlinebankieren verschijnt er in de adresbalk een pictogram van een slot in beeld, hetgeen betekent dat de bank de browsersessie heeft versleuteld. Vaak worden op mobiele apparaten wachtwoorden gebruikt om versleuteling mogelijk te maken. Apple is begonnen met de versleuteling van persoonsgegevens op het meest recente besturingssysteem, iOS 8, mits de correcte instellingen zijn ingeschakeld. Een aantal leveranciers biedt aan bedrijfsgegevens te versleutelen. Verzekerden zouden zich moeten wenden tot hun risicomanager voor nadere informatie over hoe dit aanvullende beveiligingsprotocol moet worden geïmplementeerd.

Wat zijn uw diensten met toegevoegde waarde? Wij hebben directe toegang tot vooraanstaande partners en de eRisk Hub. Hun diensten zijn voor onze verzekerden gratis beschikbaar. Onze partners leveren op het gebied van risicobeheersing uitgebreide maatregelen, procedures, instructies en andere tools voor verzekerden om inbreuken te voorkomen. Daarnaast wordt voorzien in onlinemateriaal op het gebied van compliance, e-mailupdates, procedures en voorbeeldformulieren, training van medewerkers, responsplannen in geval van gegevensinbreuken en volledige telefonische ondersteuning. eRisk Hub®, mede mogelijk gemaakt door NetDiligence®, stelt tools en middelen beschikbaar om onze verzekerden te helpen inzicht te krijgen in de risico's, een responsplan op te stellen en de organisatorische gevolgen van een gegevensinbreuk op de organisatie zoveel mogelijk te beperken. In dat kader wordt ook een inbreukadviseur en een responsteam beschikbaar gesteld.

Begrippenlijst

Hieronder volgt een lijst van belangrijke termen op het gebied van gegevensinbreuken en Cyber en Data Risks verzekering.

APT (Advanced Persistent Threat - geavanceerde aanhoudende bedreiging): een tegenstander die op zeer hoog en verfijnd deskundigheidsniveau opereert en over aanzienlijke middelen beschikt om met inzet van meervoudige aanvalsvectoren (cybervectoren, fysieke vectoren en manipulatie) zijn doelstellingen te realiseren. APT-aanvallen kunnen worden geleid in opdracht van buitenlandse naties waarbij de daders zich continu richten op een specifiek doelwit.

ASP (Application Service Provider): een bedrijf dat op software gebaseerde diensten verleent en beheert vanuit een centraal datacentrum op internet.

Authenticatie: het proces waarbij de identiteit en andere kenmerken van een entiteit worden geverifieerd. Kan ook deel uitmaken van meervoudige authenticatie, het proces waarbij meervoudige factoren worden ingezet bij de identificatie en authenticatie van een persoon.

Blackhat: een hacker die met kwaadaardige bedoelingen inbreekt in een computersysteem of netwerk.

Blacklist: een lijst van entiteiten of personen die geblokkeerd zijn of uitgesloten van toegang of privileges.

Bot: een heimelijk geïnfecteerde computer die met het internet is verbonden en die op afstand met kwade bedoelingen bestuurd kan worden door een beheerder (of hacker).

Botnet: een verzameling computers die besmet zijn met schadelijke software en vervolgens vanuit een netwerk worden aangestuurd. Doorgaans gebruikt bij DDoS-aanvallen (zie aldaar).

Brute Force Attack: een methode op basis van trial-and-error die wordt aangewend door middel van applicaties voor het kraken van versleutelde gegevens, zoals wachtwoorden, waarbij alle mogelijke wachtwoordcombinaties worden uitgeprobeerd. Een 'woordenboekaanval' is een voorbeeld hiervan. Deze primitieve hackingmethode is zeer tijdrovend en de aanval kan met een basisbeveiliging worden afgeslagen.

Children's Online Privacy Protection Act (COPPA): Amerikaanse wetgeving van de Federal Trade Commission (FTC) die van toepassing is op websites die gegevens verzamelen van minderjarigen jonger dan 19 jaar.

Cloud computing: de algemene term om de levering van gehoste diensten via het internet te beschrijven. Cloud computing stelt bedrijven in staat om IT-middelen als nutsvoorziening te gebruiken, zoals bij telefoniediensten, zonder dat ze daarvoor een eigen hardware-infrastructuur hoeven op te bouwen en te onderhouden ('infrastructuur' en 'platform' worden dan gezien als 'diensten').

Cloud hosting: de algemene term om een dienst te beschrijven waarbij gegevens en hulpmiddelen door een hostingfaciliteit worden opgeslagen. Een cloudinfrastructuur kan daarbij als openbaar, particulier of hybride instrument worden geïmplementeerd. De voordelen daarvan zijn dat het verzamelen van overbodige data en zwakke punten (single points of failure) worden vermeden, de flexibiliteit groter wordt en de kosten beperkt zijn.

Collocatie (of Co-locatie): het huren door bedrijven van vastgoed, koeling, energie en bandbreedte van een hostingfaciliteit, die hen in staat stelt hun eigen materiaal (servers, opslag) te plaatsen binnen de omgeving van de hostingfaciliteit (doorgaans in beveiligde kooien). De meeste collocatiefaciliteiten voorzien tevens in goede veiligheidsmaatregelen, branddetectie, gefilterde voeding en backup-generatoren om de continuïteit van de bedrijfsvoering te waarborgen.

Cryptografie: het beschermen van gegevens door ze om te zetten in een onleesbaar formaat (vercijferde text). De vercijferde tekst kan weer in een leesbaar formaat worden omgezet (gedecodeerd) door middel van een geheime sleutel. Versleuteling en distributie van versleutelingscodes kan op allerlei manieren worden toegepast. Zo kan gebruik worden gemaakt van de veelgebruikte PGP-software (Pretty Good Privacy).

Cybermisleiding: mensen met behulp van verschillende technieken, zoals spear phishing, phishing en hacken van e-mail, geld en gevoelige gegevens afhandig maken.

Digitaal forensisch onderzoek: toepassing van onderzoeks- en analysetechnieken om bewijs te vergaren uit een computer en vervolgens zodanig veilig te stellen dat het geschikt is om aan een rechtbank te presenteren. Deze onderzoeken vormen de eerste stap in de vaststelling van de omvang, reikwijdte en oorzaak van een inbreuk op gegevens.

Dumpster Diving: het rondsnuffelen in vuilnis op zoek naar gevoelige gegevens die niet naar behoren zijn verwijderd.

DDoS: Distributed Denial of Service Attack. Een aanval waarbij meerdere geïnfecteerde systemen worden ingezet om het doelwitsysteem te overspoelen met netwerkverkeer, waardoor dat systeem komt plat te liggen.

EMR: Electronic Medical Records. Term die vaak wordt gebruikt wanneer men het heeft over systemen voor het beheer van elektronische dossiers die binnen de gezondheidszorg worden gebruikt.

EMV: Europay, MasterCard en Visa. Internationale standaard voor de onderlinge werking tussen chipkaarten en geldautomaten, ingezet door de betaalkaartenbranche voor gebruik bij verkooppuntsystemen waarbij de kaart gelezen wordt.

Firewall: systeem dat onbevoegde toegang tot of vanuit een particulier netwerk voorkomt. Firewalls kunnen via hardware en software worden geïmplementeerd.

Firmware: software opgeslagen in een read-only memory (ROM) die in hardwarecomponenten is geïntegreerd.

First Party-(verzekering): dekking die een verzekerde wordt geboden tegen schade die niet voortvloeit uit een door een derde ingesteld rechtsgeding. Onder de dekking vallen kennisgeving, fraudecontrole, bedrijfsstagnatie, gegevensactiva en cyberafpersing.

Fraudecontrole: een dienst voor gedupeerde betrokkenen waarbij wordt aangeboden toe te zien op de kredietactiviteit. Deze dienst, die normaliter gebaseerd is op een maandelijks tarief, houdt in dat bij de betrokkenen wordt gemeld als er verdachte kredietactiviteiten plaatsvinden die verband houden met hun identiteit.

FTP: File Transfer Protocol, een protocol dat uitwisseling/ doorgifte van bestanden via het internet vergemakkelijkt.

Gegevensaggregatie: enorme hoeveelheden gevoelige gegevens centraal doorgeven of opslaan in een centrale opslagplaats.

Beschermde gezondheidsgegevens: Gegevens over een gezondheidssituatie, verstrekking van gezondheidszorg of betaling van zorg die in verband kunnen worden gebracht met een specifiek individu. Een en ander wordt ruim geïnterpreteerd; ook delen van een medisch dossier van een patiënt of diens betalingsgeschiedenis vallen eronder.

Hacktivism: term die verwijst naar de beweegredenen achter bepaalde hackinggebeurtenissen. Aanvallen kunnen ingegeven zijn door politieke of maatschappelijke motieven in plaats van zuiver financiële motieven.

Hardware: computerhardware bestaat uit fysieke componenten, zoals drives, schermen, toetsenborden en chips.

Hashing: het transformeren van een willekeurige reeks karakters in een doorgaans kortere reeks van vaste lengte, ook wel sleutel genoemd. Deze sleutel vertegenwoordigt de originele reeks. Hashing wordt veelal gebruikt om items in een database te indexeren en op te halen, omdat het item met de kortere reeks sneller kan worden gevonden. De methode wordt ook gebruikt in veel cryptografische algoritmen.

HIE: Health Information Exchange. Deze term wordt gebruikt voor de elektronische uitwisseling van gezondheidsinformatie tussen organisaties binnen een regio, gemeenschap of ziekenhuissysteem. HIE kan ook betrekking hebben op de organisatie die de uitwisseling faciliteert.

IaaS: Infrastructure as a Service. Gebruikt om aan te geven dat computerinfrastructuur wordt geleverd in de vorm van een dienst (via het internet).

Inbraak: het zich verschaffen van wederrechtelijke toegang tot een systeem door een onbevoegde. Inbraak kan worden vastgesteld door middel van een inbraakdetectiesysteem (IDS).

Inbreuk (gegevens): een beveiligingsincident waarbij gevoelige, beschermde of vertrouwelijke gegevens worden gekopieerd, doorgegeven, bekeken, toegeëigend of gebruikt door een daartoe onbevoegde persoon. Gegevensinbreuken zijn ook onderworpen aan specifieke overheidsdefinities die als uitgangspunt kunnen dienen wanneer een bepaalde respons op inbreuken vereist is.

Inbreukkosten: de kosten die gepaard gaan met diensten die verleend worden als reactie op de inbreuk. Het gaat daarbij om (doorgaans) verzekerbare bedragen die kosten van digitaal forensisch onderzoek van computers, kennisgeving aan gedupeerden en fraudecontrole kunnen omvatten. Inbreukkosten vallen onder de dekking van de First Party- verzekering en vloeien normaliter voort uit een inbreukincident en niet uit een rechtszaak. Verzekeringspolissen kunnen in de betreffende diensten voorzien, hetzij op vrijwillige basis, hetzij enkel in reactie op een gegevensinbreuk die aanleiding is voor de toepassing van bepaalde nationale, regionale of lokale wetgeving inzake gegevensinbreuken.

Inbreukrespons: de handelingen in reactie op een gegevensinbreuk. Er zijn bedrijven die beschikken over uitgewerkte plannen van aanpak bij een gegevensinbreuk die stap voor stap aangeven wat er moet gebeuren nadat de inbreuk heeft plaatsgevonden. Er volgen in de regel een groot aantal actiefasen die zich onder andere richten op analyse van het incident, kennisgeving aan de betrokkenen, indammen van de schade en communicatie/herstel. Verzekeringsmaatschappijen kunnen derdenleveranciers inschakelen om het proces in geval van een inbreuk in goede banen te leiden.

Incident Respons Plan: een door een organisatie ingevoerd plan van aanpak om het hoofd te bieden aan de gevolgen van een beveiligingsinbreuk of aanval. In dit plan wordt bepaald wat een incident inhoudt. Daarnaast bevat het een stappenplan met maatregelen ten aanzien van tijdschema's, rollen/verantwoordelijkheden, contactgegevens en andere onderdelen die nodig zijn om een inbreuksituatie te beheersen.

Keylogger: malware (virus) waarmee men de toetsaanslagen van een computergebruiker kan registreren.

Met deze volgsoftware kunnen de registraties meestal worden gecodeerd en wordt de doorgifte van de gegevens aan een hacker verborgen.

Kennisgeving: in cyberverzekeringstermen betekent dit het inlichten van de gedupeerde betrokkenen op wier gegevens inbreuk is gepleegd. Vanaf januari 2016 heeft Nederland een meldingswetgeving ingevoerd waarin gedefinieerd is wat persoonsgegevens zijn en wanneer gedupeerden moeten worden ingelicht. Diverse ontwerpwetten zijn nog in behandeling.

Kritische infrastructuur: het onderliggende geheel van faciliteiten, systemen, sites en netwerken die noodzakelijk zijn voor de functionaliteit.

Kwetsbaarheid: een onvermoede tekortkoming in de software of in systemen die kan worden uitgebuit.

Malafide medewerker: een medewerker die zich onbevoegd en met kwade bedoelingen toegang verschaft tot gegevens of een medewerker die gevoelige informatie verkoopt voor eigen financieel gewin. Malafide medewerkers kunnen ook proberen uit wraak (bijvoorbeeld omdat zij zich onheus bejegend voelen) een bedrijfsnetwerk aanvallen.

Malware: samentrekking van MALicious softWARE. Deze software is bedoeld om een systeem te beschadigen of te verstoren (virus of Trojaans paard).

PaaS: Platform as a Service. Een via internet geleverd model van een computerplatform die in de vorm van een uitbestede dienst wordt geleverd, zodat de ontvanger geen eigen hardware/software hoeft te beheren.

Packet: een gegevenspakket dat tussen oorsprong en bestemming van een netwerk (of het internet) kan worden verstuurd.

Betaalkaartgegevens. In de PCI SSC worden kaarthoudergegevens aangeduid als Primary Account Number (PAN), waaronder het volledige nummer samen met de volgende gegevens wordt verstaan: naam kaarthouder, vervaldatum, servicecode. Bij gevoelige authenticatiegegevens is voorzien in bescherming door middel van, onder andere, een volledige magneetstrip, CAV2, CVC2, CVV2, CID en PIN.

PCI DSS: de PCI SSC heeft in de PCI Data Security Standards het beveiligingsniveau omschreven waaraan organisaties die transacties met betaalpassen verwerken, minimaal moeten voldoen. Vanaf maart 2015 zijn er vier PCI DSS-niveaus, die elk zijn vastgesteld op basis van het volume aan betaalkaarten die een bedrijf jaarlijks behandelt. De meest veeleisende compliancenorm die PCI SSC heeft vastgesteld is PCI-niveau 1, de minst veeleisende is PCI-niveau 4 (gekoppeld aan een beperkt betalingskaartvolume). Meer informatie is te vinden onder: https://www.pcisecuritystandards.org/

PCI (Standards Council): het bestuursorgaan van de PCI. De PCI Security Standards Council (PCI SSC) is in september 2006 opgericht door American Express, Discover Financial Services, Japan Credit Bureau, MasterCard Worldwide en Visa International. In augustus 2014 telde de website van PCI SSC 688 deelnemende organisaties.

PCI Assessments (naleving): controles op de naleving van de PCI DSS (zie aldaar). In bepaalde omstandigheden mogen handelaren die lagere volumes afhandelen zelfbeoordelingen uitvoeren. In de meeste situaties met hoge kaartvolumes kan het nodig zijn volledige beoordelingen (eventueel ter plekke) uit te voeren. Nalevingscontroles worden door een gekwalificeerde veiligheidsbeoordelaar (QSA - Qualified Security Assessor (zie aldaar)) verricht.

PCI Assessments (boetes): geldboetes die bedrijven moeten betalen wegens inbreuk op gegevens van betaalkaarten. In de boete kunnen de kosten zijn verwerkt van het opnieuw uitgeven van kaarten en van niet-verhaalbare frauduleuze geldopnames met de gestolen kaarten. Dergelijke kosten worden in de regel doorberekend aan het gedupeerde bedrijf op basis van hun contracten, met name overeenkomsten inzake handelaarsdiensten of overeenkomsten inzake betalingsverwerking. Aangezien banken die betaalkaarten uitgeven niet rechtstreeks contracten afsluiten met bedrijven die betaalkaarten van klanten accepteren, worden deze kosten als het ware doorgegeven binnen een contractuele keten waarbij de betalingsverwerker in het midden zit. Sommige verzekeringspolissen bieden expliciet dekking tegen dergelijke uit contractbreuk voortvloeiende kosten, maar andere weer niet.

PCI Fines and Penalties: geldboetes die wervende banken opleggen wegens overtreding van de PCI-regels. De boetes kunnen variëren van € 5.000 tot € 100.000 per maand, maar details worden niet openlijk besproken of breed bekendgemaakt.

PCI QSA: erkende bedrijven die aanbieden een ander bedrijf op PCI-compliance te beoordelen. Voldoen de bedrijven aan de PCI DSS, dan kan certificering plaatsvinden. Erkende gekwalificeerde veiligheidsbeoordelaars, ofwel QSA-bedrijven, zijn te vinden onder:

https://www.pcisecuritystandards. org/approved_companies_providers/ qsa_companies.php

Penetration testing (Pen Testing): een "Whitehat"-hacker of -script inzetten in een poging om een bedrijfsnetwerk te penetreren. Met deze voorzorgsmethode komen kwetsbaarheden aan het licht die anders verborgen zouden zijn gebleven.

Persoonsgegevens: Gegevens aan de hand waarvan personen kunnen worden geïdentificeerd. Definities van overheden en in wetten en andere regelgeving lopen echter uiteen. Persoonsgegevens kunnen beschermde gezondheidsgegevens bevatten maar ook gegevens van betaalkaarten, BSN-nummers en een waaier aan andere gevoelige gegevens.

Phishing: beproefde techniek van hackers of anderen met kwade bedoelingen, die zich voordoen als vertrouwde entiteiten met als doel de gebruiker gevoelige of privégegevens te ontfutselen. Varianten hierop zijn "spear phishing" (een afzonderlijke gebruiker of een afdeling is het doelwit) of "whale phishing" (mensen met een belangrijke functie of veel geld zijn het doelwit).

Phreaking: door middel van een computer of ander apparaat inbreken op een telefoonsysteem. Het systeem wordt zodanig gemanipuleerd dat de dader gratis kan telefoneren en facturen bij iemand anders in rekening worden gebracht. Dit is een van de oudste vormen van "hacking".

POS (Point of Sale): fysieke locatie waar goederen en diensten worden gekocht en verkocht gepaard gaande met de vastlegging van informatie en betaalgegevens. Afhankelijk van de context kan POS ook verwijzen naar het softwareplatform dat wordt gebruikt voor de verzameling en/of doorgifte van deze informatie.

Ram Scraping: een techniek die door uiteenlopende malware wordt toegepast (BackOff-variant). Gegevens van betaalkaarten worden gelicht uit een machinegeheugen voordat ze worden versleuteld.

Ransomware: een type malware dat de toegang tot het geïnfecteerde computersysteem blokkeert waarna de afperser losgeld vraagt om het systeem weer te 'bevrijden'.

Redundancy's: gedupliceerde exemplaren van gegevens, infrastructuur of andere gevoelige/ kritische informatie of infrastructuur. Externe en geografisch gespreide redundancy's zijn typisch gegevens waar alle kwaadwillende ogen op zijn gericht.

SaaS: Software as a Service. Deze methode voorziet in de levering via internet (of de cloud) van softwarefunctionaliteit als alternatief voor de installatie van de software op de apparatuur van de eindgebruiker.

SCADA: Supervisory Control and Data Automation. Wordt toegepast voor de beheersing van industriële en productieprocessen.

Sleutel: moet worden ingegeven om de versleuteling ongedaan te maken en de gegevens weer leesbaar te maken.

Social Engineering: een methode om personen door misleiding beveiligde gegevens afhandig te maken. Slachtoffers van social engineering zijn kwetsbaar door hun ingeboren aard om anderen te vertrouwen en te willen helpen.

SPAM: elektronische junkmail of berichten.

Spoofing: verzamelnaam voor verschillende manieren waarop hardware en software om de tuin kunnen worden geleid. Het manipuleren van telefoonnummers, IP-adressen of andere unieke identificatiecodes valt ook onder spoofing.

Spyware: software die heimelijk informatie over een computergebruiker vergaart zonder dat de gebruiker het in de gaten heeft, meestal voor reclamedoeleinden.

SSL: Secure Sockets Layer. SSL is een protocol voor de doorgifte van gegevens via internet door middel van cryptografische systemen die twee sleutels gebruiken om de gegevens te coderen. Veel internetbrowsers geven aan dat de aansluiting met SSL beschermd is door bij het URL-veld een pictogram in de vorm van een hangslotje of een veiligheidscertificaat af te beelden.

Third Party-(verzekering): verzekering waarbij de dekking in werking treedt als gevolg van aanspraak die door een derde is ingesteld. In een privacy- of cybercontext gaat het dan meestal om aansprakelijkheidsstelling vanwege psychisch leed, identiteitsdiefstal, openbaarmaking van inbreuk op privacy gegevens of aanvallen op de netwerkbeveiliging.

Threat Agent: een individu of groep die een dreiging vormt. De dreiging heeft meestal betrekking op misbruik voor uiteenlopende doeleinden van activa van een bedrijf.

Tokenization: methode waarbij gevoelige gegevens door een niet-gevoelig equivalent (token) wordt vervangen.

Trojaans paard: een programma (malware) ontworpen om beveiliging van een computersysteem te doorbreken en, wanneer dat gelukt is, zijn schadelijk werk verricht (meestal diefstal van gegevens of besmetting van computers).

Uitbuiting: misbruik maken van een zwakke plek in de beveiliging. Uitbuiten van onvermoede en niet-gepatchte hiaten in de softwarecode die de software kwetsbaar maken voor onbevoegde toegang of integriteitsinbreuken.

Versleuteling: berichten of gegevens zodanig coderen dat alleen bevoegden er toegang toe hebben. De gegevens kunnen hiermee nog steeds worden onderschept, maar door de versleuteling kan geen toegang tot de inhoud worden verkregen. *Zie ook: Cryptografie*

Virus: een programma (of een stukje code) met een schadelijke werking dat buiten medeweten van de gebruiker om kwaadwillige redenen op diens computer wordt geïnstalleerd.

Whitehat: een benaming voor "ethisch hacken". Whitehat hacking is iets waar een potentieel doelwit zelf om vraagt om onvermoede zwakke plekken in de beveiliging bloot te leggen.

Worm: een programma of algoritme dat zichzelf vermenigvuldigt op een computernetwerk en daar zijn schadelijke werk verricht.

Zero-Day: hiermee worden kwetsbaarheden in de beveiliging uitgebuit op dezelfde dag waarop de kwetsbaarheden publiekelijk of algemeen bekend worden. Het lek wordt meestal later onschadelijk gemaakt door middel van beveiligingspatches of updates die door de softwareleverancier worden vrijgegeven.

De inhoud van dit document en de bijbehorende materialen is niet bedoeld als juridisch, zakelijk of verzekeringsadvies dat verband houdt met de behoeften van specifieke individuele bedrijven.

Disclaimers

BreachProtection™ is uitsluitend verantwoordelijk voor de inhoud en advies verstrekt op breachprotection.com. De informatie die via breachprotection.com wordt verstrekt, mag niet worden opgevat als juridisch of ander professioneel advies. Neem voor uw specifieke situatie contact op met uw juridisch adviseur of andere deskundigen voor het inwinnen van adequaat juridisch en overig advies.

De verantwoordelijkheid voor alle verstrekte inhoud en adviezen berust uitsluitend bij het advocatenkantoor of andere bronnen waarop voor dit risicobeheersingsmateriaal een beroep is gedaan.

Wanneer u een advocatenkantoor in de hand neemt of een dienstverrichter om de inbreuk te herstellen is de dekking van de desbetreffende kosten onderworpen aan de voorwaarden van uw polis. In bepaalde gevallen is voorafgaande toestemming vereist van uw verzekeringsmaatschappij. Het is raadzaam dat u zich vertrouwd maakt met de polisvoorwaarden. Informatie die verstrekt wordt via de Hiscox eRisk Hub® portal dient niet gelezen te worden als juridisch of professioneel advies. Neem voor uw specifieke situatie contact op met uw juridisch adviseur of andere deskundigen voor het inwinnen van adequaat juridisch en overig advies.

Wanneer u een beroep doet op de diensten van Control Risk is de dekking van de desbetreffende kosten onderworpen aan de voorwaarden van uw polis. In bepaalde gevallen is voorafgaande toestemming vereist van uw verzekeringsmaatschappij. Het is raadzaam dat u zich vertrouwd maakt met de polisvoorwaarden.