Begrippenlijst Cyber & Data

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 Cloud infrastructuur 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 back-up-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.

Begrippenlijst Cyber & Data

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.
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.
Firmware	Software opgeslagen in een read-only memory (ROM) die in hardwarecomponenten is geïntegreerd.
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 hacking gebeurtenissen. Aanvallen kunnen ingegeven zijn door politieke of maatschappelijke motieven in plaats van zuiver financiële motieven.
Hardware	Computer hardware 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.

Begrippenlijst Cyber & Data

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 derden leveranciers 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 België 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.

Begrippenlijst Cyber & Data

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 compliance norm 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.
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”.
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.

Begrippenlijst Cyber & Data

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 method 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.
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*
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).

Begrippenlijst Cyber & Data

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.

Begrippenlijst Cyber & Data

Typologie van Cyber Risico's

Door de staat gesteunde acties

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.

Begrippenlijst Cyber & Data

VEELGESTELDE VRAGEN

Het thema privacy is met veel verwarring omgeven. Hieronder wordt getracht licht te werpen op veel gestelde 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 VERZEKERING 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 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 derden leveranciers, 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.

I**k 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.

Begrippenlijst Cyber & Data

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 PCIstandaard 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 € 3.400.000. 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, tekst 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, BSNnummers, 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 privacy polissen 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 debitering na een inbreuk.

Begrippenlijst Cyber & Data

DEKKING

Wat is het verschil tussen First Party- en Third Partydekking 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 claim afhandeling 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.

Begrippenlijst Cyber & Data

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.