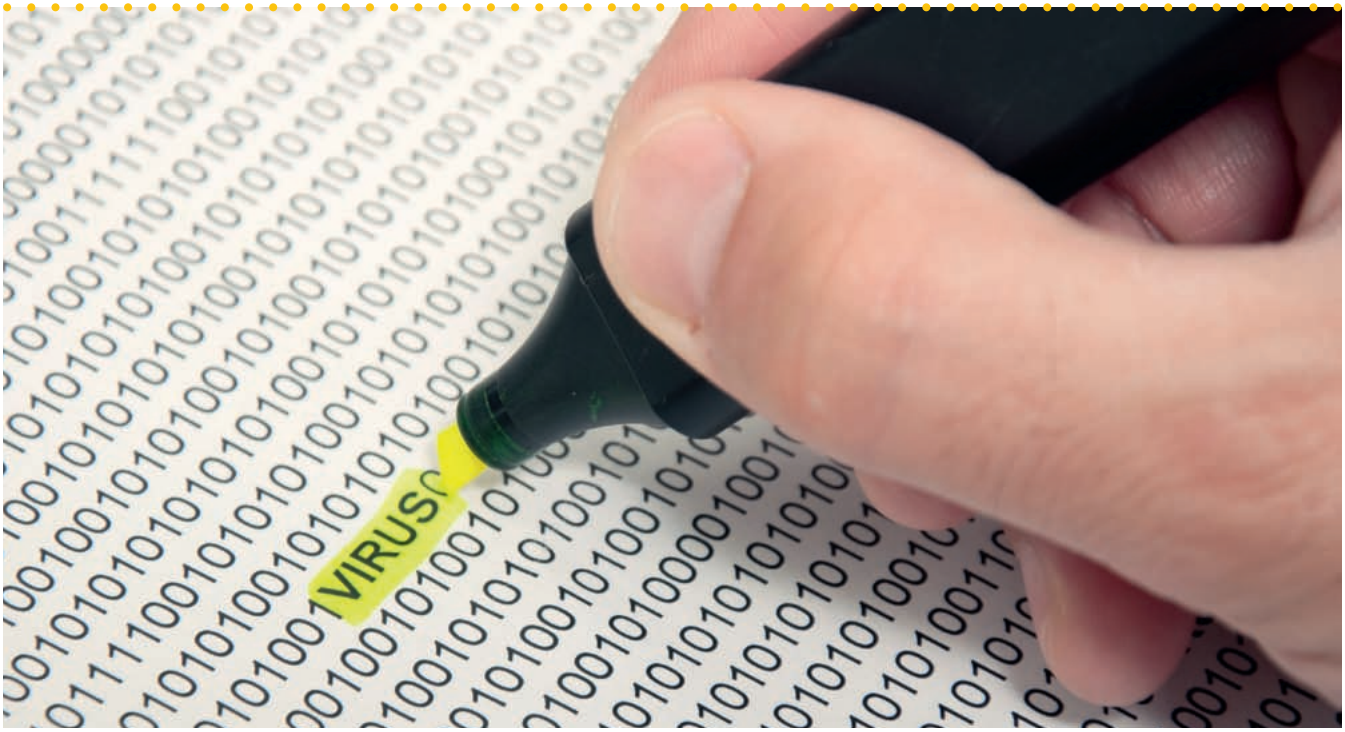
CYBERINCIDENTEN EN NIEUWE WETGEVING **GEVEN CYBERADVIES EEN BOOST**



Adviseurs schadeverzekeringen zakelijk kunnen anno 2015 niet meer om advies rond cyberrisico's heen. Aan de ene kant niet vanwege de dagelijkse praktijk: een toenemend aantal cyberincidenten dat overheden en bedrijfsleven treft. Aan de andere kant niet vanwege de wet- en regelgeving: kennis over cyberrisico's is onderdeel van de verplichte PE-actualiteiten 2015 zoals die zijn vastgesteld door de minister van Financiën. Daarnaast wordt het Wetsvoorstel meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp per 1 januari 2016 ingevoerd.

Een toenemend aantal adviseurs neemt, zo merk ik tijdens workshops, het onderwerp cyberrisico's mee in hun verzekeringstechnische risicoanalyse. Daartoe is ook alle aanleiding. Door de toenemende digitalisering van de maatschappij worden organisaties steeds kwetsbaarder voor risico's die die digitalisering met zich mee brengt. De gevolgen van een calamiteit zoals brand in het bedrijfsgebouw worden steeds groter naarmate meer gegevens digitaal zijn vastgelegd. Denk aan uitval van systemen en aan beschadiging of verloren gaan van digitale gegevens Maar denk ook aan het risico dat digitale gegevens in handen komen van onbevoegden.

Het versleuteld opslaan van gegevens (encryptie) kan melden datalek voorkómen

WAT ZIJN CYBERRISICO'S?

Het cyberrisico wordt wel omschreven als het financiële nadeel dat een organisatie oploopt door of via computer- en/of ICT-systemen, zonder dat er sprake is van materiele schade. Het risico van materiële schade aan computersystemen door bijvoorbeeld diefstal of brand is van oudsher een verzekerbaar risico op bijvoorbeeld de inventaris- of computerverzekering.

- Cyberrisico's ontstaan door:
- cybercriminaliteit;
- menselijke fouten;
- technisch falen van ICT-systemen.

De schade kan zich voordoen op diverse manieren. Denk aan het verliezen van gegevens, bedrijfsstagnatie, aansprakelijkheid en boetes. De financiële schade die daardoor ontstaat, kan optreden voorafgaand aan het cyberincident, tijdens het incident en na het incident in de herstel- en controlefase. Bij schade voorafgaand aan het incident moet u denken aan (de kosten van) het afslaan van een aanval via het internet op een website of computersysteem. Heeft het incident zich voorgedaan, dan kan het gaan om de schade door bedrijfsstilstand,

de herstelkosten van gegevensverlies of de kosten om de systemen permanent te monitoren. Maar het kan natuurlijk ook de aansprakelijkheidsschade betreffen van derden die schade hebben geleden of een boete omdat niet voldaan is aan wet- en regelgeving.

OVERHEID EN CYBERRISICO'S

De overheid heeft al geruime tijd in de gaten dat de samenleving door cyberrisico's fors ontwricht kan raken. Zo heeft het ministerie van Veiligheid en Justitie een Nationaal Cyber Security Centrum (NCSC) ingericht. Het NCSC is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. De missie van het NCSC is het bijdragen aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving. Het NCSC is internationaal het Nederlandse aanspreekpunt op het gebied van ICT-dreigingen en cybersecurity-incidenten. Ook is het NCSC een sleutelfiguur in de operationele coördinatie bij een grote ICT-crisis.

De minister van Financiën heeft op voorstel van het CDFD, het College Deskundigheid Financiële Dienstverlening, eind vorig jaar een voorzichtige eerste aanzet gedaan om advies over cyberrisico's tot verplichte kost voor de adviseur Schade Zakelijk te maken. Aan de PE-actualiteiten 2015 is een kennistoetsterm '*De kandidaat kent het fenomeen cyberverzekering*' toegevoegd. Ongetwijfeld zal die toetsterm in de toekomst niet op zichzelf blijven staan, want met deze kennis alleen kom je er niet. Als onderdeel van de verzekeringstechnische risicoanalyse zullen ook vaardigheden en competenties rond de inventarisatie, analyse en advies rond cyberrisico's en beheer en claimbehandeling van cyberrisksverzekeringen tot de gereedschapskist van de adviseur moeten gaan behoren.

Daarnaast zijn Tweede en Eerste Kamer in de loop van 2015 akkoord gegaan met invoering van het Wetsvoorstel meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid CBP. De regering heeft inmiddels de invoeringsdatum vastgesteld op 1 januari 2016. Het doel van de meldplicht is om tot een betere bescherming van persoonsgegevens te komen. Een meldplicht kenden webhosters en telecomproviders al langer op basis van de Telecommunicatiewet.

INHOUD WETSVOORSTEL

Door het Wetsvoorstel meldplicht datalekken wordt onder meer de Wet bescherming persoonsgegevens (Wbp) aangepast.

MELDPLICHT DATALEK AAN CBP

Er wordt in het eerste lid van een nieuw artikel 34a een verplichting ingevoerd tot melding aan het College bescherming persoonsgegevens (CBP) van een inbreuk op de beveiliging. Het betreft dan inbreuken die leiden tot een aanzienlijke kans op ernstige nadelige gevolgen, dan wel tot ernstige gevolgen voor de bescherming van persoonsgegevens die worden verwerkt. De meldplicht rust op de verantwoordelijke voor de verwerking van persoonsgegevens. Volgens de Wbp is de verantwoordelijke voor een verwerking degene die het doel en de middelen voor de verwerking vaststelt. Dat kan dus een persoon, bedrijf, organisatie of een overheidsinstelling zijn die persoonsgegevens vastlegt of laat vastleggen. De verantwoordelijke is niet altijd de bewerker en daarom wordt in een aangepast artikel 14 van de Wbp ook geregeld dat de verantwoordelijke moet zorgdragen dat de bewerker, naast reeds bestaande verplichtingen, de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplichting tot melding van een datalek.

MELDPLICHT AAN BETROKKENE

In het tweede lid van artikel 34a Wbp is vastgelegd dat de verantwoordelijke voor de verwerking van persoonsgegevens alle betrokkenen direct ('onverwijld') in kennis stelt van de inbreuk indien de inbreuk waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer. Daarbij moet een behoorlijke en zorgvuldige informatievoorziening gewaarborgd zijn. Financiële ondernemingen als bedoeld in de Wet op het financieel toezicht zijn uitgezonderd van de meldplicht net als, onder voorwaarden, aanbieders van openbare elektronische communicatiediensten als telecomproviders.

Het CBP kan, indien het van oordeel is dat inbreuk waarschijnlijk ongunstige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkene, verlangen dat alsnog een kennisgeving aan betrokkene wordt gedaan indien de verantwoordelijke voor de persoonsgegevens geen kennisgeving had gedaan.

De meldplicht vervalt indien passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens. Het versleuteld opslaan van gegevens (encryptie) is zo'n beschermingsmaatregel die kan voorkómen dat een datalek gemeld moet worden aan alle betrokkenen.

Het aantal Nederlandstalige polisvoorwaarden is op één hand te tellen

VOORBEELD

Uit een huisartsenpraktijk wordt de server met daarop de patiëntengegevens ontvreemd. De patiëntgegevens zijn niet versleuteld. Naast de NAW-gegevens betreft dat ook patiëntgegevens als BSN-nummer, geboortedatum, bankrekeningnummer, polisnummer zorgverzekering en behandelgegevens. De huisartsenpraktijk zal op basis van de meldplicht alle patiënten moeten informeren dat door de diefstal van de server waarschijnlijk privacygevoelige gegevens in handen van onbevoegden zijn gekomen. Indien de huisartsenpraktijk gekozen had voor het gecodeerd opslaan van de patiëntgegevens, dan had de melding aan de patiënten achterwege kunnen blijven!

BOETEBEVOEGDHEID CBP

Het CBP krijgt de mogelijkheid om bestuurlijke boetes op te leggen als

VERANTWOORDELIJKE VERSUS BEWERKER

De verantwoordelijke is niet de bewerker van de persoonsgegevens. Een bewerker is een persoon of organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed, bijvoorbeeld een administratiekantoor. Een bewerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens, maar heeft wel een aantal afgeleide verplichtingen voor onder meer beveiliging en geheimhouding van de gegevens en vanaf 1 januari 2016 dus ook als het gaat om de meldingsplicht van een datalek.
Voorbeeld: een werkgever heeft de loonadministratie uitbesteed aan een administratiekantoor. De werkgever is de verantwoordelijke voor de gegevensverwerking, de salarisverwerker is de bewerker in de zin van de Wbp.

niet in overeenstemming wordt gehandeld met bepalingen in de Wbp. Het CBP moet dan overigens in de meeste gevallen eerst een bindende aanwijzing geven, eventueel gekoppeld aan een termijn waarbinnen de aanwijzing moet zijn opgevolgd. Die aanwijzing hoeft niet eerst gegeven te worden als sprake is van een opzettelijke overtreding of een overtreding die het gevolg is van een ernstig verwijtbare nalatigheid. De bestuurlijke boete is ten hoogste het bedrag van de zesde categorie volgens art. 23, 4e lid Wetboek van Strafrecht. Dat bedrag is sinds 1 januari 2014 810 duizend euro bij niet-nakoming van de bindende aanwijzing. Het College kan, na overleg met de verantwoordelijke minister, nadere beleidsregels stellen over de toepassing van de boetebevoegdheid. Als het gaat om een rechtspersoon kan, indien die boete geen passende bestraffing zou zijn naar het oordeel van het CBP, een geldboete worden opgelegd tot ten hoogste tien procent van de jaaromzet van de rechtspersoon in het boekjaar voorafgaande aan de uitspraak of beschikking.

De werking van de boetebeschikking wordt opgeschort totdat de bezwaar- of beroepstermijn is verstreken of, indien bezwaar is gemaakt respectievelijk beroep is ingesteld, op het bezwaar respectievelijk het beroep is beslist.

ADVIESPRAKTIJK

Voor de adviespraktijk is het van belang de cyberrisico's bespreekbaar te maken bij de klant. Alleen met een goede inventarisatie en analyse van de risico's is een passend advies uit te brengen. Een advies dat nadrukkelijk aandacht zal moeten besteden aan de genomen en mogelijk nog te nemen preventiemaatregelen op het gebied van gegevensbeveiliging en privacybescherming. In de Wbp ligt namelijk in artikel 12 vast dat een bedrijf passende beveiligingsmaatregelen moet nemen bij het verwerken van persoonsgegevens. Daarnaast stellen verzekeraars in de polisvoorwaarden van cyberriskverzekeringen ook eisen aan het beveiligingsniveau wanneer cyberrisico's aan hen worden overgedragen.

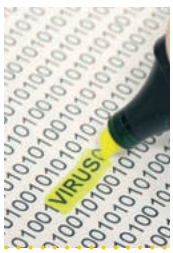
Voorbeelden van preventiemaatregelen ter voorkoming van cyberrisico's zijn:

- het opstellen van een beleidsdocument over informatiebeveiliging;
- het benoemen van interne verantwoordelijken en het vastleggen van taken;
- inventariseren van kwetsbaarheden en afhankelijkheden (bijvoorbeeld verwerking bij derden);
- fysieke beveiliging van informatiesystemen;
- toegangsbeveiliging van de organisatie;
- toepassingen van rollen en rechtenstructuur bij verstrekking inlog- en passwordgegevens aan medewerkers;
- loggen en controleren van het gebruik van ICT-systemen (onder meer monitoren netwerkgebruik, virusscanners);
- correct gebruik software;
- versleutelen van gegevens;
- opstellen en toepassen incidentenprotocol.

VERZEKERINGSDEKKINGEN

In die gevallen waarin op basis van het advies de adviseur een voorstel voor een cyberriskpolis doet, moet eerst de markt verkend worden. Vanaf circa 2011 hebben zich vrijwel uitsluitend buitenlandse risicodragers in de Nederlandse markt gemeld met cyberriskpolissen. De geboden dekkingen lopen nogal uiteen. Een complicatie is dat het aantal Nederlandstalige polisvoorwaarden op één hand is te tellen. Ook zijn er polisvoorwaarden waarvan bij nadere bestudering blijkt dat die soms een slechte vertaling zijn van Engelstalige polisvoorwaarden. Daaraan zijn dan enige artikelen toegevoegd (mededelingsplicht en klachtregeling uit de Wet financieel toezicht) om ze geschikt te maken voor gebruik in Nederland.

De nu in de markt beschikbare Nederlandstalige voorwaarden kennen in grote lijnen, even los van de benamingen, twee hoofdrubrieken:



De beschikbare cyberriskpolissen kennen veel uitsluitingen: een uitdaging voor de adviseur!

HOOFDRUBRIEK DIGITALE AANSPRAKELIJKHEID

Deze rubriek dekt de aansprakelijkheid van de verzekerde voor schending van privacy of vertrouwelijkheid door een cyberincident, bij uitbesteding of voor ongewild besmetten van netwerken van derden door een beveiligingslek. Die aansprakelijkheid is niet gedekt op de Aansprakelijkheid Bedrijven (AVB), omdat de AVB gebruikelijk alleen dekking biedt voor zaak- of letselschade.

HOOFDRUBRIEK EIGEN SCHADE

Deze hoofdrubriek kent een aantal subrubrieken die van verzekeraar tot verzekeraar verschillen qua dekking. Veelvoorkomende subrubrieken zijn:

- kosten van onderzoek en analyse datalek;
- kosten melding aan overheid;
- kosten communicatie (naar onder meer betrokkenen);
- kosten dataherstel;
- netwerkonderbreking (stagnatie);
- afpersing;
- boetes.

De in de markt beschikbare cyberriskpolissen kennen daarnaast veel uitsluitingen, zowel algemene uitsluitingen als ook uitsluitingen per rubriek. Dat biedt een uitdaging voor de adviseur bij de vergelijking en de uitleg aan de klant!

MODELPOLIS CYBERRISK

In juni 2015 is onder de vlag van VNAB, de Vereniging Nederlandse Assurantie Beurs, het Platform Cyberrisk van start gegaan. Dat platform heeft onder andere als doel kennisbundeling, kennisdeling en advies. Met als uiteindelijke doel: de ontwikkeling van een modelpolis cyberrisk. Die is hard nodig en zal mogelijk ook zijn uitstraling in de markt hebben en zorgen voor meer uniformiteit in de dekkingsrubrieken en gebruikte terminologie.

P.B. (Berrie) van der Heide RMiA
De auteur is registermakelaar in assurantiën, lid van de redactieraad van De Beursbengel **en is daarnaast actief als opleider/auteur voor opleidingsinstituten in de verzekeringsbranche.**

BRONNEN
- www.ncsc.nl
- www.cpbweb.nl
- https://www.rijksoverheid.nl/actueel/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-CBP-1-januari-2016-van-kracht
- https://www.eerstekamer.nl/behandeling/20150210/gewijzigd_voorstel_van_wet
- Position paper Verbond van Verzekeraars Virtuele risico's, echte schade, oktober 2013
- www.vnab.nl