Veroorzakers

Veroorzakers van cybercriminaliteit zijn doorgaans hackers. Deze handelen soms uit financieel gewin, maar soms ook met zogenaamd goede bedoelingen. Deze hackers kunnen interne medewerkers zijn - personeel of ingehuurde krachten - maar vooral ook mensen van buitenaf.
We kennen allemaal wel het verhaal over de whizzkid die in zijn kamertje via zijn computer inbreekt op het netwerk van een bedrijf of organisatie. Op deze manier kan bijvoorbeeld de bedrijfswebsite worden gehackt, waardoor er geen omzet meer wordt gemaakt via internet. Of er kunnen wel orders worden geplaatst, maar de betalingen gaan naar de hackers in plaats van naar de ondernemer.
Maar dat zijn niet de enige vormen van schade. De ondernemer kan ook ernstige schade oplopen indien er door cybercriminaliteit schade ontstaat bij een ander bedrijf. Het netwerk van iDeal kan bijvoorbeeld worden gehackt en daardoor loopt de ondernemer schade op. Zelfs als zijn eigen ICT op orde is, loopt de ondernemer toch risico. De mogelijkheden voor het verzekeren van dit risico zijn in ons land nog niet zo groot. In de VS is dit al wel 'big business'. Het Verbond van Verzekeraars verwacht ook in Nederland een sterke groei van deze cyberrisico-producten.

Rubrieken

De enkele verzekeraar die in ons land een cyberrisico-product aanbiedt, geeft de mogelijkheid te kiezen uit een zestal rubrieken:

1. Hacking
Deze rubriek biedt dekking voor de schade veroorzaakt door hackers, te weten:

- Reparatie, vervanging of herstel van websites, programma's of data
- Kosten van de gestolen software of van de data
- Kosten van onderzoek en advies in systeembeveiliging
- Kosten van forensisch onderzoek naar de oorzaak van een 'hack'
- Boetes als gevolg van datalekken

2. Systeeminbraak
Deze rubriek dekt de eigen kosten als gevolg van inbraak op systemen of data, te weten:

- Kosten van forensisch onderzoek
- Kosten van communicatie met klanten, toezichthouders, Justitie, creditmaatschappijen, e.a.
- Kosten van extra klantenondersteuning, bijvoorbeeld via een callcenter
- Kosten van crisismanagement, reputatieherstel en pr-campagnes

3. Privacy
Op deze rubriek zijn de gevolgen gedekt van gestolen privacygevoelige gegevens, te weten:

- Kosten van onderzoek door Justitie of creditcardmaatschappijen
- Claims van individuele personen
- Boetes opgelegd door toezichthouders of eventuele andere verplichte vergoedingen

Ook als bedrijven zich hebben verzekerd tegen cyberrisico's, zullen ze alles moeten doen om een cyberincident te voorkomen. Niet alleen omdat de premies daardoor laag blijven en de verzekeringsvoorwaarden het voorschrijven, maar ook omdat niet alle schade onder de dekking valt (zoals imagoschade) en omdat de wetgever het eist. In artikel 12 van de Wet bescherming persoonsgegevens staat dat een bedrijf passende beveiligingsmaatregelen moet nemen bij het verwerken van persoonsgegevens. Alhoewel deze wetgeving alleen gekoppeld is aan het mogelijk lekken van persoonsgegevens, kunnen contractpartners ook een passende beveiliging verwachten bij het verwerken van gevoelige bedrijfsinformatie.

4. Digitale aansprakelijkheid
Onder deze rubriek is dekking indien de website of een mailbericht onbedoeld het auteursrecht schendt, laster verspreidt of een virus bevat.

5. Afpersing

Deze module biedt dekking tegen de schade van hackers die de website of de data gijzelen (door middel van zogenoemde 'ransomware').

- Vergoeding van het gevraagde losgeld, tot een bepaalde limiet
- Kosten van bijstand van een security-adviesbureau.

6. Bedrijfsschade (omzetverlies door cyberaanvallen)

Deze module dekt de eventuele kosten van het omzetverlies door een DDos-actie of andere aanval op computersystemen, zoals de uitval van een webwinkel.

Een bijkomend voordeel voor de onderneming bij het sluiten van een cyberverzekering is de professionele assistentie van de verzekeraar en haar partners bij het voorkomen en beperken van schade bij een hackeraanval, dataverlies en andere incidenten.

De verzekeringsdekking verschilt natuurlijk sterk per verzekeraar. Daarnaast kan deze ook van moment tot moment verschillen, aangezien de markt volop in ontwikkeling is.

Preventie

De verzekeraar verlangt van de verzekeringnemer preventieve maatregelen om cyberrisico's tegen te gaan. Dit doen ze niet alleen om de risico's te beperken, maar ook omdat dit een wettelijke grondslag heeft. In artikel 12 van de Wet bescherming persoonsgegevens (Wbp) staat dat een bedrijf 'passende beveiligingsmaatregelen' moet nemen bij het verwerken van persoonsgegevens. Hoewel dit met name de persoonsgegevens betreft, is de link naar gevoelige bedrijfsinformatie snel gelegd.
Voorbeelden van passende beveiligingsmaatregelen zijn:

- Een beleidsdocument voor informatiebeveiliging
- Het toewijzen van verantwoordelijkheden voor informatiebeveiliging
- Beveiligingsbewustzijn
- Fysieke beveiliging en beveiliging van apparatuur
- Toegangsbeveiliging
- Logging en controle
- Correcte verwerking in toepassingssystemen
- Beheer van technische kwetsbaarheden
- Incidentenbeheer
- Afhandeling van datalekken en beveiligingsincidenten
- Continuïteitsbeheer
- Monitoring van bedrijfsnetwerken
- Versleuteling van gegevens

Doelgroep

Bedrijven die zeer afhankelijk zijn van IT-systemen of die veel gegevens beheren, hebben vooral baat bij een cyberverzekering. Dit geldt zowel voor kleine als grote ondernemingen.
Kleine ondernemingen, omdat ze vaak niet over voldoende kennis en middelen beschikken. Grote ondernemingen, omdat die steeds vaker doelwit zijn van cybercriminaliteit.
Het maakt overigens niet uit of een bedrijf zelf de automatisering uitvoert, of deze heeft uitbesteed. In de Wet bescherming persoonsgegevens (Wbp) is immers vastgelegd dat het bedrijf zelf verantwoordelijk blijft voor de integriteit en de beveiliging van de verzamelde (gevoelige) gegevens.

Schade bij cyberincidenten

Een andere manier om naar de verzekeringsdekking te kijken, is die in twee hoofdmoten:

- de schade aan derden
- de schade die de onderneming zelf oploopt (eigen schade).

Om de dekking verder te verduidelijken, kijken we naar de schade zoals deze zich door de tijd heen ontwikkelt.

Voordat het cyberincident zich manifesteert
Wanneer er een vermoeden is van een cyberincident, kan er al schade ontstaan. Soms worden bedrijven afgeperst onder dreiging van een DDoS-aanval of het bewust lekken van privacygevoelige gegevens. Het kan nodig zijn dat een verzekerde uit voorzorg extra IT-capaciteit inkoopt, om op deze wijze de DDoS-aanval te voorkomen. Hiermee zijn kosten gemoeid die kunnen worden verzekerd. Ook de begeleiding en betaling van afpersing kunnen afgedekt worden met een verzekering.

Tijdens de manifestatie van het cyberincident
In deze fase gaat het allereerst om kosten die worden gemaakt om het probleem te onderzoeken, bijvoorbeeld door een forensisch ICT-specialist. Het doel van dit onderzoek is om het risico te beperken en de organisatie te beschermen.
Wanneer zich een datalek voordoet, kan de organisatie hiervoor aansprakelijk worden gesteld. Deze aansprakelijkstelling kan ontstaan doordat een melding is gedaan van een lek bij een bevoegde autoriteit, of juist doordat die melding niet is gedaan. In de samenleving begint steeds meer het bewustzijn te leven dat individuen organisaties aansprakelijk kunnen stellen voor geleden schade in verband met gegevensverwerking en -lekken. De gedupeerden kunnen een civielrechtelijke actie starten op basis van een onrechtmatige daad. Ook deze schade en kosten van verweer zijn verzekerbaar. Daarnaast kunnen de kosten van een wettelijk verplichte notificatie richting de gedupeerden onderdeel zijn van de verzekeringsdekking.
Als gevolg van een cyberincident kunnen het interne en externe netwerk van een organisatie worden stilgelegd, waardoor inkomsten worden gemist. Met een bedrijfsschadedekking worden deze gemiste inkomsten vergoed. Hierbij kan ook worden gedacht aan betalingsplatforms van banken.

Herstelfase
In deze fase gaat het om kosten die worden gemaakt om het probleem te herstellen. Denk aan het herstel van het IT-systeem en het herstel van verloren data. Ook de kosten die gepaard gaan met de notificatie bij toezichthouders, zoals het inhuren van juridische experts, kunnen worden gedekt. Daarnaast bestaan er verzekeringsdekkingen die de kosten voor de inhuur van een communicatieadviesbureau vergoeden om reputatieschade te voorkomen of te beperken.

Controlefase
In deze fase gaat het om de kosten van toezichtrechtelijke procedures en kredietmonitoringdiensten (om te zien of bijvoorbeeld gestolen creditcardgegevens worden misbruikt).
Het is te verwachten dat het bewustzijn over deze risico's bij ondernemers sterk zal toenemen. Daarmee zullen er ongetwijfeld meerdere aanbieders en verzekeringsmogelijkheden ontstaan.

Samenloop

Het samenlooprisico is vooral aanwezig in combinatie met (computer)fraudeverzekeringen. Op zowel de cyberverzekering als de fraudeverzekering bestaat dekking voor financiële gevolgen van frauduleus handelen door werknemers en derden. Kosten die gemaakt worden om fraudeschade te voorkomen, zijn over het algemeen alleen te claimen op de cyberverzekering.
Bij brand- en technische verzekeringen is materiële schade in principe gedekt. Dus als bij cyberincidenten materiële schade ontstaat, dan biedt de brandverzekering mogelijk uitkomst. De overlap is minimaal. Dat geldt ook voor aansprakelijkheidsverzekeringen. Schade als gevolg van cyberrisico’s worden over het algemeen gezien als zuivere vermogensschade en dat is uitgesloten op de aansprakelijkheidsverzekering voor bedrijven (AVB).
Beroepsfouten zijn onder dit type verzekering uitgesloten; daarvoor bestaat de beroepsaansprakelijkheidsverzekering (BAV). Deze dekt de zuivere vermogensschade die uit een beroepsfout ontstaat. Bij een datalek kan sprake zijn van een beroepsfout. De mogelijke aansprakelijkheid die hieruit voortvloeit, is gedekt onder de BAV.
De schade hoeft echter niet het gevolg te zijn van een beroepsfout. Dit maakt dat schade die ontstaan is door een datalek, niet of niet altijd kan worden verzekerd op een beroepsaansprakelijkheidsverzekering of een AVB, omdat er vaak geen sprake is van zaak- of

letselschade. Daarnaast gaat het bij datalekken vaak om schade aan de organisatie. Deze laat zich lastig kwantificeren. Zo is bijvoorbeeld de omvang van reputatieschade moeilijk in te schatten.
Ook de traditionele bedrijfsschadeverzekeringen zijn niet toegerust voor de nieuwe cyberrisico's van bedrijven. Er is immers (vaak) geen zaakschade, zoals bij brand of een aanrijding. Zaakschade als oorzaak van de bedrijfsstilstand is een voorwaarde voor dekking op een traditionele bedrijfsschadeverzekering.

Wet meldplicht datalekken

Vanaf 1 januari 2016 riskeren organisaties een forse boete als zij de privacytoezichthouder en de gedupeerden in het ongewisse laten over ernstige beveiligingsincidenten. Op 26 mei 2015 is de Wet meldplicht datalekken door de Eerste kamer aangenomen. Daaruit vloeit voort dat er sinds 1 januari 2016 een algemene meldplicht datalekken is voor alle organisaties die voor eigen doeleinden persoonsgegevens verwerken. De enorme datalekken bij het supermarktconcern Target en de vreemdgangerssite Ashley Madison zijn schokkende voorbeelden van de bedreigingen waarmee organisaties en betrokkenen tegenwoordig wereldwijd te maken hebben. Bij Target ging het om gelekte creditcardgegevens van maar liefst 40 miljoen klanten. Van de Canadese vreemdgangerssite Ashley Madison zijn de gegevens van 37 miljoen klanten door hackers online gezet.
Om de risico's van dataverlies zoveel mogelijk te beperken, heeft de Nederlandse wetgever een algemene meldplicht datalekken ingevoerd. De verplichting tot het melden van datalekken door verantwoordelijken wordt geregeld door het opnemen van aanvullende bepalingen in de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet (Tw).
De toezichthouder, de Autoriteit Persoonsgegevens (AP) (beter bekend als het College bescherming persoonsgegevens (CBP)), kan bestuursdwang toepassen of een dwangsom of bestuurlijke boete opleggen wanneer zij constateert dat de wet wordt overtreden of wanneer de overtreder een bindende aanwijzing niet opvolgt. Dit wil zeggen dat de AP de bevoegdheid heeft om afscherming, uitwissing of vernietiging van gegevens te gelasten. Bestuursdwang houdt ook in dat als de overtreder niet binnen een redelijke termijn zelf maatregelen neemt om de situatie te herstellen, de overheid gegevens mag afschermen, uitwissen of vernietigen. De kosten van dit overheidsingrijpen zijn voor de overtreder. De boetes kunnen oplopen tot € 820.000 of zelfs tot 10% van de jaaromzet, als dat een meer passende bestraffing is.
Datalekken kunnen ontstaan door hackers, maar ook door het gebruik van verouderde software. Daarnaast kunnen datalekken ontstaan door simpele menselijke fouten, zoals een kwijtgeraakte USB-stick of het slordig omgaan met wachtwoorden. Van de meeste datalekken hoor je niets. Alleen de meest serieuze gevallen komen in het nieuws. In Nederland heeft met name de DigiNotar-affaire uit 2011 veel aandacht getrokken.
Boetes zijn in het algemeen niet gedekt op (klassieke) verzekeringspolissen. Het verzekeren van boetes kan in strijd worden geacht met de openbare orde, omdat de verzekering de prikkel van de boete wegneemt. Er zijn echter cyberverzekeringen die boetes wel dekken. Het verzekeren van een (bestuurlijke) boete kan onder omstandigheden toch aanvaardbaar zijn, als een organisatie te maken krijgt met een datalek door bijvoorbeeld hacking, terwijl toch alle redelijke beveiligingsmaatregelen zijn genomen.