vanbreda
RISK & BENEFITS

Cyberrisico's

Bescherm uw onderneming tegen de toenemende cyberrisico's

Inhoudstafel

1. Inleiding

Cyberverzekeringen

Brand, ziekte of een ongeval – uiteraard hoopt u dat zulk onheil u bespaard blijft. De kans dat u er vroeg of laat mee te maken krijgt, is echter bestaande. Daarom stelt u alles in het werk om te voorkomen dat tegenspoed in uw leven de bovenhand kan krijgen. Van een ziekteverzekering tot een verzekering burgerlijke aansprakelijkheid, op gepaste wijze dekt u zich in tegen tal van risico's. Niet alleen vindt u dat de meest verstandige beslissing, u beschouwt het ook als vanzelfsprekend. Soms is het zelfs verplicht, zoals bij een autoverzekering.

Wat opvalt is dat u er helemaal anders tegenaan kijkt wanneer het om risico's gaat in de digitale wereld. Allicht bezit u een computer, een tablet, een smartphone. Deze apparaten zijn standaard uitgerust met beveiligingssoftware. De realiteit leert ons echter dat zelfs de meest geavanceerde toepassingen niet opgewassen zijn tegen hackers die te kwader trouw handelen. Zij kraken uw apparaat, gaan met gevoelige informatie aan de haal en misbruiken mogelijk uw identiteitsgegevens.

De gevolgen zijn nog desastreuzer wanneer zulke cybercriminelen de computersystemen van ondernemingen in het vizier nemen. Gevoelige informatie wordt publiek gemaakt. Klantgegevens worden online te grabbel gegooid. Soms gaan ze zelfs zo ver dat geautomatiseerde bedrijfsprocessen bewust in de war worden gestuurd. In een klap kan een hacker uw bedrijf lamleggen. Dat is zonder enige twijfel een van de grootste nachtmerries van elke ondernemer.

Uit onze eigen cyberstudies blijkt dat één op de drie bedrijven dat vandaag verzekerd is tegen cybercrime al effectief een schadegeval heeft gehad. Bij 45% van die bedrijven kwam de bedrijfsactiviteit daarbij ook tot stilstand. Intussen wint deze nieuwe vorm van criminaliteit verder terrein en nemen de onheilsscenario's steeds groteskere vormen aan. En hoewel we een stijging zien van het aantal bedrijven dat zich indekt tegen dit nieuwe risico, blijft dit aantal minimaal in vergelijking met het aantal afgesloten brandverzekeringen. Merkwaardig, toch?

In dit e-book worden de gevaren alsook de gevolgen van cybercrime blootgelegd. Vanbreda biedt tot slot tal van verzekeringsoplossingen waarmee elk bedrijf zich kan indekken. Die stellen we ook graag kort aan u voor.

2. Elk bedrijf is kwetsbaar voor cybercrime

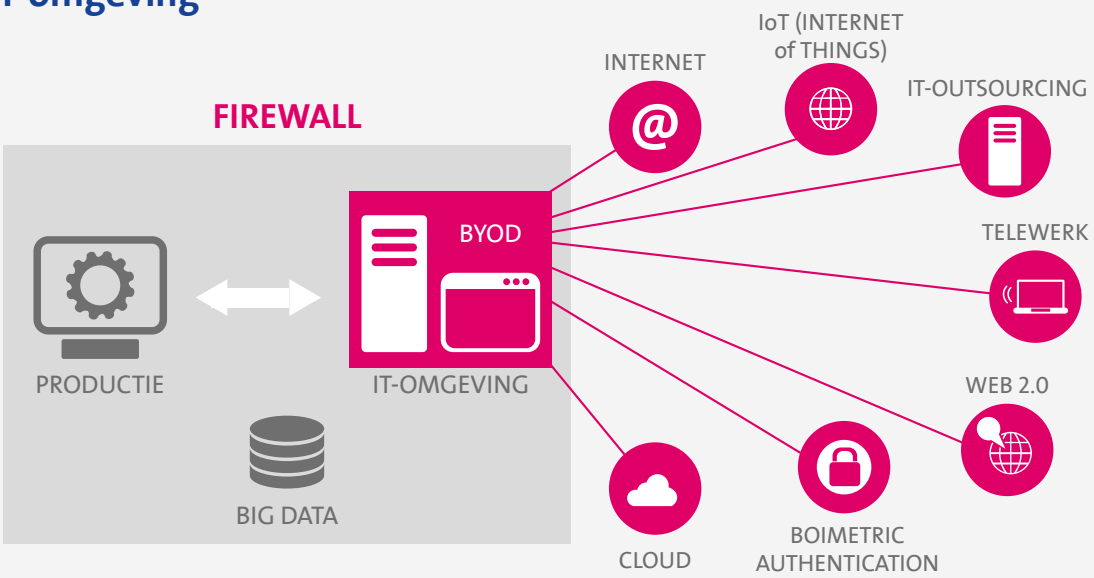
Cybercriminaliteit vormt een risico voor elke onderneming. Toch leeft bij heel wat ondernemers het idee dat zij niet ten prooi kunnen vallen aan hackers. Ze menen dat uitsluitend kapitaalintensieve sectoren en grote spelers in het vizier lopen, met name multinationals en financiële instellingen.

Niets is minder waar. De omvang van een bedrijf is voor hackers irrelevant, hoe onwaarschijnlijk dat ook mag klinken. Eerder dan de economische slagkracht vormt de mate van beveiliging van een onderneming het doorslaggevende criterium. Hackers speuren veelal naar de makkelijkste prooi. Dat zijn niet zelden de kleine kmo's. De praktijk leert ons dat deze niet alleen zelf rechtstreeks aangevallen worden, maar dat hackers hen vaak ook als een opstap zien naar een groter bedrijf waarmee de kmo nauw samenwerkt.

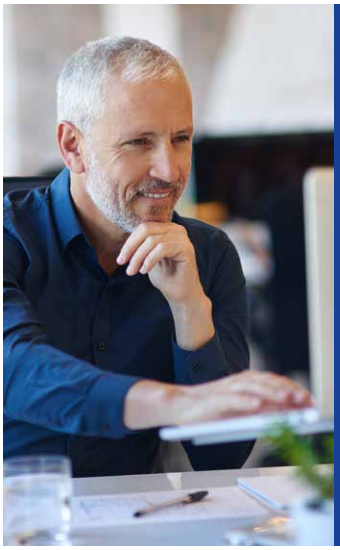
IT is de ruggengraat van uw onderneming

De noodzaak van een cyberverzekering is niet sectorgerelateerd. De aandacht van hackers gaat immers resoluut naar de medewerkers als zwakste schakel binnen een (slecht beveiligde) IT-omgeving, niet naar het profiel van desbetreffend bedrijf. In zowat alle sectoren is die omgeving vandaag wijdvertakt. Van productieprocessen tot interne communicatieplatformen, alles staat met elkaar in verbinding. Het is die uitgestrektheid van de IT-omgeving die bedrijven vandaag zo kwetsbaar maakt.

IT-omgeving



Het cyberrisico is bij de meeste bedrijven dan ook bijzonder groot. Zo faciliteert een IT-omgeving niet alleen e-mail-verkeer, cloudtoepassingen, thuiswerken, smartphones gekoppeld aan een bedrijfsaccount, IT-outsourcing, de opslag van klantgegevens, enz. Ook productielijnen zijn hieraan steeds vaker gekoppeld. De IT-omgeving is zo uitgegroeid tot de ruggengraat van elke onderneming. Het hoeft dan ook niet te verbazen dat een gerichte aanval die onderneming moeiteloos kan lamleggen.



Praktijkvoorbeeld:

Patrick (52) is de eigenaar van een familiebedrijf dat machines bouwt. Hijzelf staat eerder sceptisch tegenover cybercrime. Hij gelooft dat de impact enorm kan zijn, maar in zijn bedrijf ziet hij niet meteen een cyberrisico opduiken.

Tot aan het licht komt dat in elke machine die het bedrijfsterrein verlaat een stukje software zit dat blijvend communiceert met een centrale server in België. Schort er wat met de machine of is een onderhoud noodzakelijk, dan wordt een melding verstuurd. Wat betekent dat de server van Patrick via elke verkochte machine gehackt kan worden, met verregaande schade aan de productieketen als gevolg.

Het cyberrisico dat het bedrijf liep, was op dat ogenblik gigantisch.

Datacenters vergroten de kwetsbaarheid van bedrijven

Om zowel praktische als veiligheidsredenen brengen ondernemingen (gevoelige) data onder in gespecialiseerde datacenters. Maar hoe deze externe partners de beveiliging van vertrouwelijke informatie organiseren, is voor de klant doorgaans koffiedik kijken. Eén ding is zeker: de klant behoudt de verantwoordelijkheid. Dat staat zwart op wit in de contracten die deze datacenters hanteren.

Datacenters kunnen zo een vals gevoel van veiligheid in de hand werken. Zelfs wanneer hackers een datacenter viseren en gevoelige informatie te grabbel gooien, blijft de onderneming die klant is immers aansprakelijk. De beveiliging in het datacenter is dan ook maar één van de vele onderdelen van 'information security', en absoluut niet allesomvattend. De externe host kent de risico's van uw onderneming niet en kan de potentiële gevaren dus ook niet inschatten.

Voorts kunnen er vraagtekens worden geplaatst bij de omgang met deze gegevens wanneer de klant zijn contract met het datacenter stopzet. Wordt deze vertrouwelijke informatie dan vernietigd? In hoeverre is dit mogelijk zonder dat er restanten achterblijven? Wat met de beveiliging van deze restanten? Ook hierin schuilt een verregaand cyberrisico.

Hoe werknemers en toplui dagelijks het cyberrisico vergroten

Zonder het te beseffen vergroten zowel werknemers als bedrijfsleiders dagelijks het cyberrisico dat een bedrijf loopt. Talrijk zijn de managers die bestanden door middel van een USB-stick of een Dropbox-account uitwisselen tussen kantoor en thuis. Of die om praktische redenen e-mailberichten doorsturen naar een privé-adres.

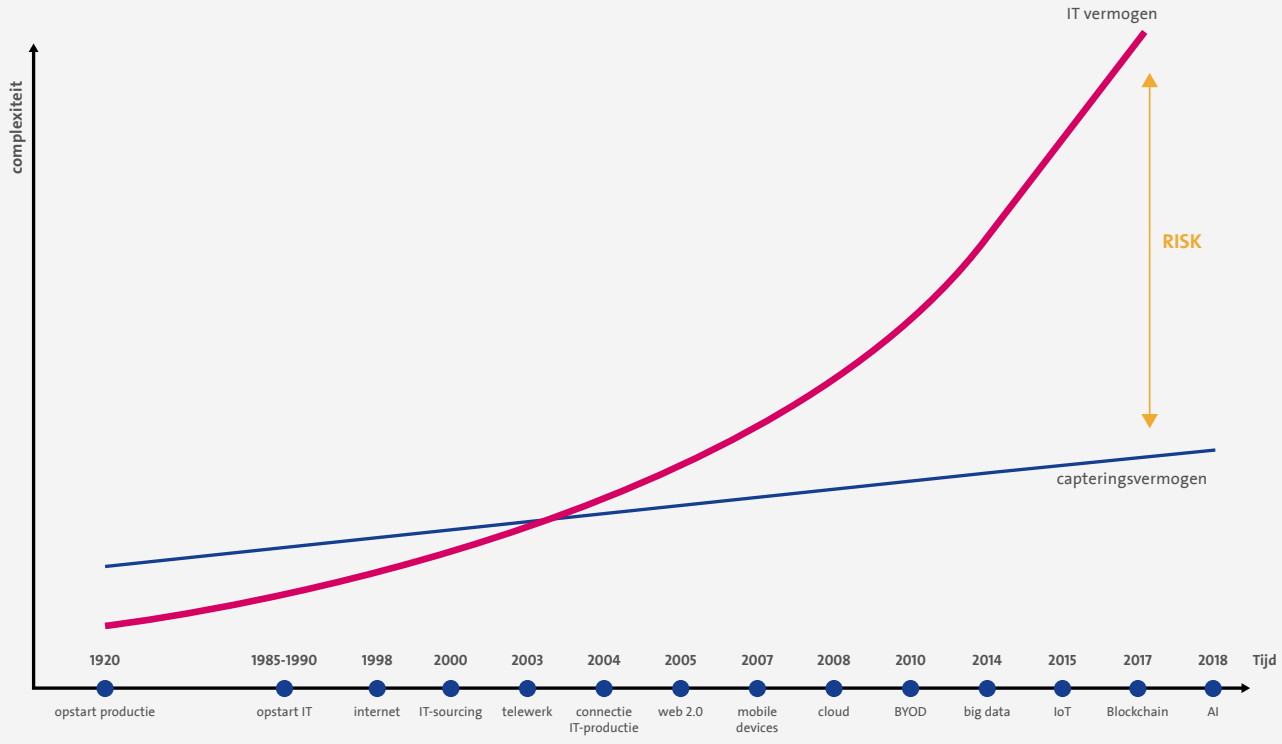
Het gaat om menselijke acties die achteloos worden gesteld, zonder stil te staan bij de ondermaats beveiligde omgeving waaraan deze vertrouwelijke data vervolgens worden blootgesteld.

Het IT-vermogen stijgt exponentieel

Sinds de jaren tachtig is de aanwezigheid van IT op de bedrijfsvloer enorm toegenomen. Wat begon met één pc om een aantal kerntaken uit te voeren, mondde uit in een digitale revolutie met ongekende mogelijkheden.

Het internet deed zijn introductie. Wat later ging thuiswerken tot de mogelijkheden behoren. De gsm groeide uit tot een mini-computer die niet hoefde onder te doen voor een desktop pc. Cloudtoepassingen maakten het vanzelfsprekend om bestanden online te bewaren. Vandaag blijkt big data meer dan ooit het nieuwe goud. En dan is er nog het Internet of Things. Welke gevolgen dat met zich meebrengt, zal in de nabije toekomst duidelijk worden.

IT-evolutie



Vast staat dat het voor de bedrijfsleider haast onmogelijk is om alle netwerken, toestellen en data te beveiligen tegen cyberaanvallen. De IT-omgeving is vandaag te sterk uitgedijd om nog beheersbaar te zijn. Risico's kunnen onmogelijk worden uitgesloten. Het is dan ook raadzaam om de nodige voorzorgsmaatregelen te treffen en uw onderneming in te dekken tegen mogelijk desastreuze gevolgen van cybercrime.

3. Bestaande versus nieuwe risico's

Ondernemen is niet vrij van risico. Tal van scenario's kunnen zich afspelen waarbij mogelijk de toekomst van uw onderneming in het gedrang komt. Met een bedrijfspolis en andere verzekeringsoplossingen op maat dekt u zich in.

Een ongeval, een blikseminslag of een noodlottige brand is het soort rampspoed waarmee u als ondernemer liever niet geconfronteerd wordt. En wat als een werknemer te kwader trouw handelt en uw onderneming schade tracht te berokkenen?

U hebt met uw onderneming een reputatie hoog te houden. Komt uw integriteit of uw confidentialiteit op de helling te staan, dan kan u dat zuur opbreken. Zakelijke deals worden opgeschort, bestellingen geannuleerd. Bent u het slachtoffer van een zware bedrijfsbrand, dan is het allicht niet langer mogelijk om goederen te leveren.

Deze risico's zijn voor uw onderneming niet nieuw. Vanbreda biedt verzekeringsoplossingen op maat zodat het voortbestaan van uw bedrijfsactiviteiten zeker is. Daarnaast zien we het ook als onze taak om u te wijzen op nieuwe risico's. Ten prooi vallen aan cybercrime is vandaag zonder twijfel het meest waarschijnlijke risico waaraan uw onderneming onderhevig is. Verderop leggen we u in detail uit hoe u zich hiertegen kunt beschermen.

GDPR, een nieuwe trigger

De roep naar privacy en de bescherming van privé- en andere belangrijke data klinkt steeds luider. Daarom is sinds 25 mei 2018 een nieuwe wet rond databescherming in voege. Ondernemingen die persoonsgegevens verzamelen, moeten voldoen aan een nieuwe set regels die omschreven staan in de General Data Protection Regulation (GDPR). Die regels moeten de gegevens van Europese burgers beter beschermen. In feite gaat het om een herziening van een Europese richtlijn uit 1995, al werd die door elke lidstaat op een andere manier geïnterpreteerd. In België bestond deze wet al in 1992.

Belangrijk voor u als ondernemer is dat de GDPR-wetgeving ook voorziet in een aanpassing van de Gegevens-beschermingsautoriteit. Die krijgt meer inspectiebevoegd-heden en ze kan grotere sancties opleggen. De boetes kunnen oplopen tot 20 miljoen euro of 4% van de totale wereldwijde jaaromzet van het voorafgaande boekjaar. Er zijn zowel in België als in de ons omringende landen al effectief boetes opgelegd.

Aangezien het tot op heden gaat om administratieve boetes en niet over strafrechtelijke boetes, zijn deze cfr. de huidige regelgeving verzekerbaar via een cyberpolis. Die komt tussen wanneer de verzekerde middels een van de triggers in de polis een inbreuk heeft gepleegd op de GDPR of een andere soortgelijke richtlijn, waarbij hem een boete wordt opgelegd. Om welke boetes gaat het precies? Iedere civielrechtelijke geldboete of sanctie opgelegd door een landelijke, provinciale, gemeentelijke of buitenlandse overheidsinstantie.

De GDPR-regels zijn opgebouwd rond vijf pijlers:

Transparantie
Ondernemingen moeten burgers op een begrijpelijke manier informeren over hoe data wordt verzameld en verwerkt.

Data-overdracht
Burgers kunnen hun gegevens overdragen van de ene dienstverlener naar de andere.

Het recht om vergeten te worden
Ondernemingen moeten persoonsgegevens kunnen wissen als de persoon in kwestie daarom vraagt en als er geen geldig tegenargument gegeven kan worden. Die plicht blijft overeind wanneer de data gedeeld werd met derde partijen.

Meldplicht bij datalekken
Ondernemingen zijn verplicht een datalek te melden binnen de 72 uur. Wanneer kan worden aangetoond dat het lek geen gevaar betekent voor de verzamelde persoonsgegevens, vervalt deze plicht.

Verantwoordelijkheid: Bedrijven zijn en blijven verantwoordelijk (ook na uitbesteding) en dienen te kunnen aantonen dat ze alle nodige maatregelen genomen hebben, afhankelijk van de geïdentificeerde risico's.

4. Verzekeringsoplossingen cybercrime

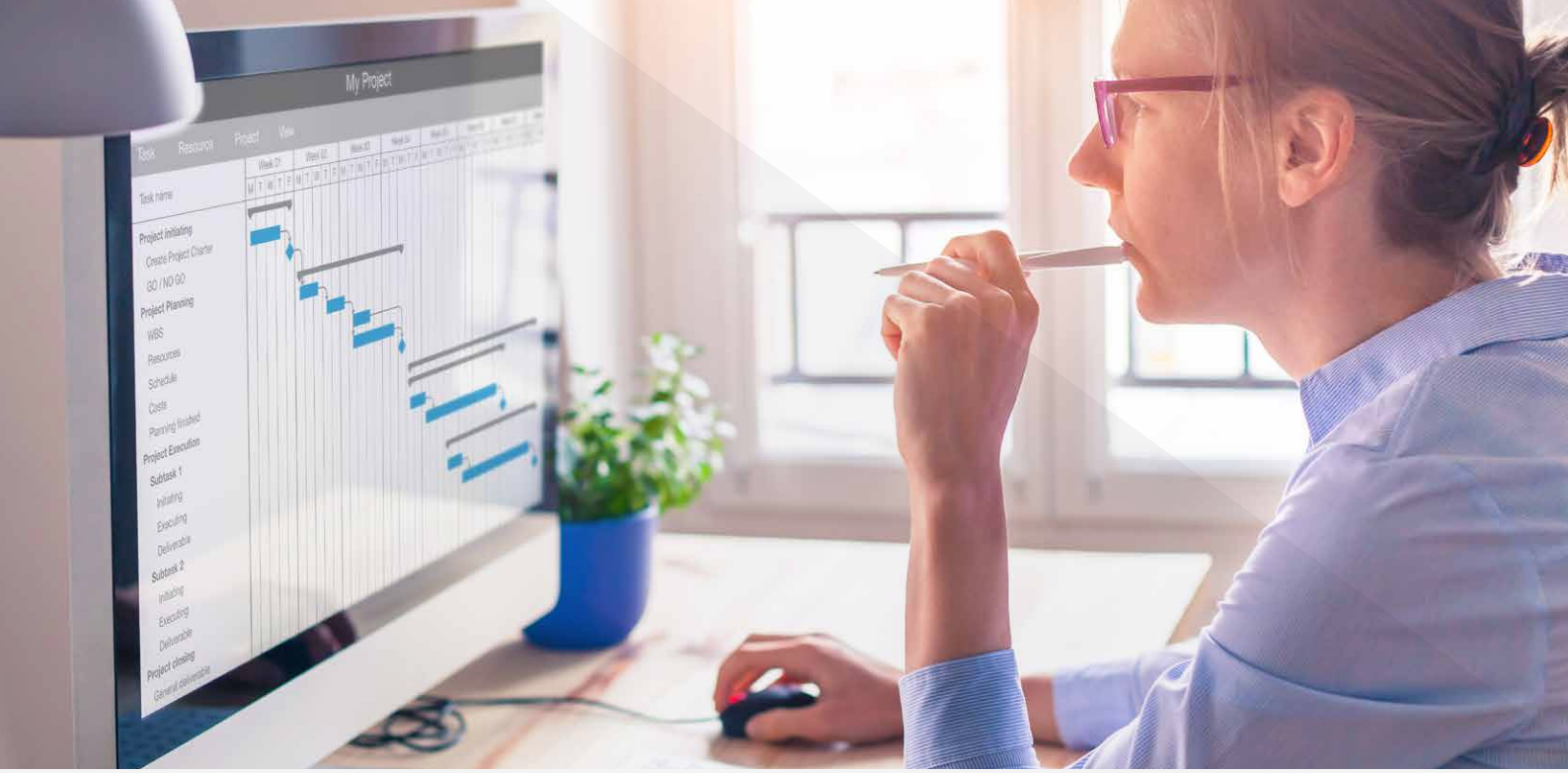
Traditionele verzekeringsoplossingen

Vandaag zijn er een aantal polissen die tot op zekere hoogte bescherming bieden bij een geval van cybercriminaliteit. Het gaat echter om bestaande polissen die niet geheel afgestemd zijn op deze nieuwe en complexe problematiek. De bescherming die ze bieden blijkt dan ook de geleden schade onvolledig te dekken, zoals onderstaande tabel aantoont.

	GL	PI	Crime	Property	Cyber
EIGEN SCHADE					
Een daad van kwaadwilligheid in informatica: intrusie van valse code					
Computervirus					
Onbevoegd gebruik of onbevoegde toegang van het computersysteem					
Menselijke fout, operationele fouten					
Een tekortkoming van een IT-dienstverlener voor outsourcing					
Een defect of een storing in de computerinstallaties en/of van de bijhorende installaties van infrastructuur					
Een stroomdefect, elektrostatische ontlading, elektromagnetische storing					
Een natuurlijke gebeurtenis, zoals het effect van de bliksem					
Een denial of service					
Een toezichtrechtelijke procedure aangaande een inbreuk op de bescherming van persoonsgegevens					
Cyber/privacy afpersing					
Hacking telefoonsysteem					
Cyber theft					
SCHADE AAN DERDE					
Inbreuk op persoonlijke en privacyrechten					
Schending van de integriteit van personen of onthulling van persoonsgegevens					
Schending van de geheimhoudingsplicht					
Laster					
Overdracht van een computervirus					
Denial of service					
Onbevoegd gebruik van het computersysteem					
Schade aan of vernietiging van data					
Multimedia aansprakelijkheid					
DEKKINGEN					
Managementhulp bij een verzekerde gebeurtenis (inclusief eerste hulp)					
Notificatie- en Communicatiekosten					
PR-kosten (Reputatiebescherming)					
Wedersamenstellingskosten van eigen en TP data					
Communicatiekosten					
Onderzoekskosten en opsporingskosten					
Bedrijfsschade + bijkomende kosten					
Bijstandskosten met een toezichthoudende instantie					
Verdediging + schadevergoeding (aansprakelijkheid)					
Verhaalskosten					
Losgeld in geval van afpersing					
Hacking telefooncentrale					

* PI : Beroepsaansprakelijkheid / GL : Algemene Aansprakelijkheid

Geen dekking | Gedeeltelijke dekking | Dekking



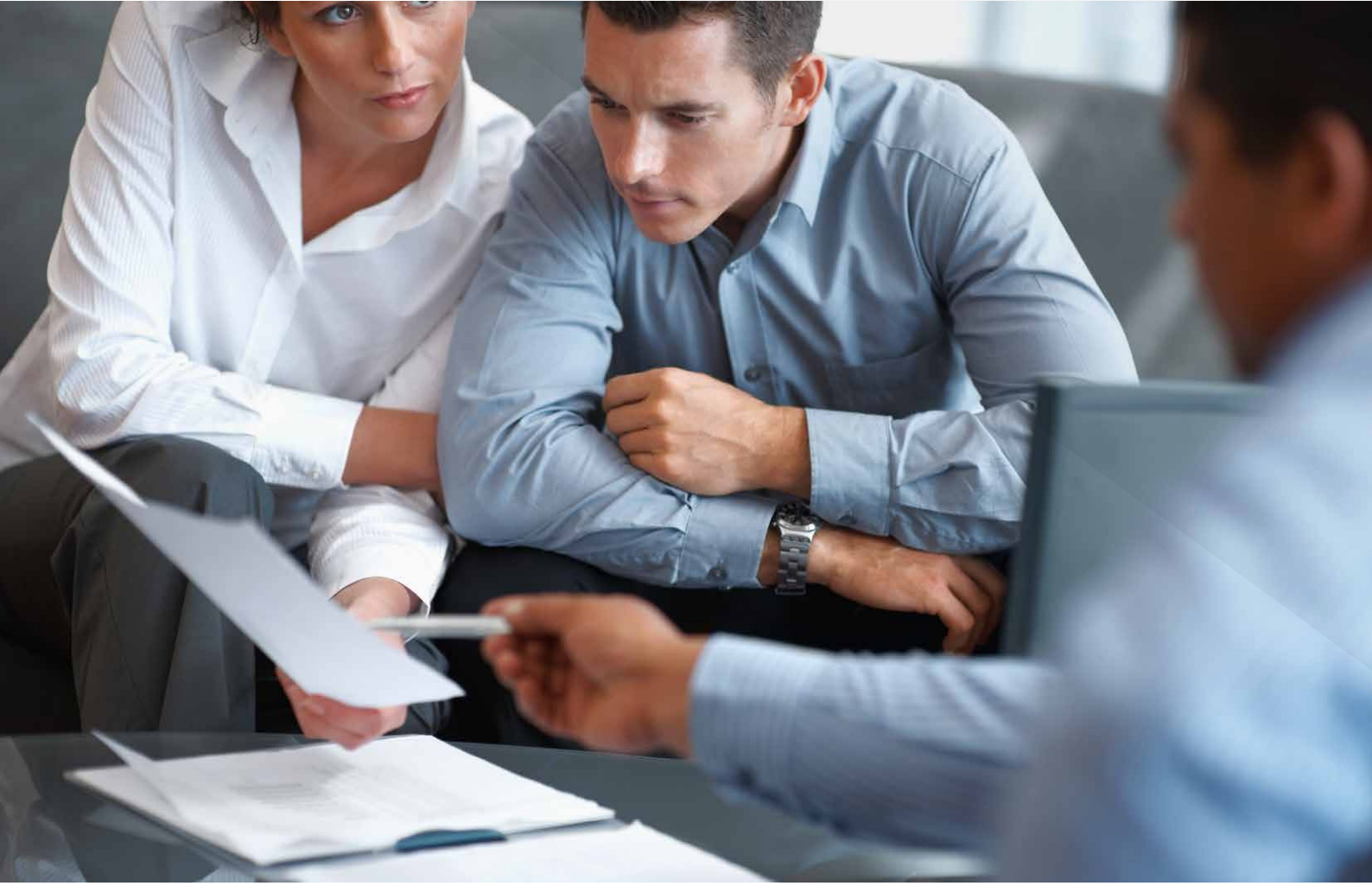
Brandverzekeringen in de zakelijke markt dekken enkel eigen schade. Ze bieden ofwel een all risk dekking, ofwel een dekking waarbij enkel specifieke schadeoorzaken verzekerd zijn. In beide gevallen is de overlapping met cyberverzekeringen doorgaans klein. Bij een all risk dekking is in principe alle materiële schade gedekt. Als een cyberincident dus ook materiële schade tot gevolg heeft, dan kan die materiële schade gedekt worden door de brandverzekering. Denk bijvoorbeeld aan de crimineel die via een computerverbinding een lopende band of machine hackt en daardoor schade aanbrengt.

Schade aan data beschouwen verzekeraars echter zelden als materiële schade. Vooral voor die schade is een cyberverzekering belangrijk. Bij brandverzekeringen zien we een tendens naar het uitsluiten van zogenaamde 'silent cyber risks' - risico's die gedekt zijn omdat ze niet zijn uitgesloten. Hetzelfde zien we in de polissen die de burgerlijke aansprakelijkheid van bedrijven dekken. Daarbij wordt de financiële schade na een cyberincident quasi volledig uitgesloten.

Er is dus duidelijk nood aan een polis die een ruime dekking op maat van cybercriminaliteit biedt.

Een fraudeverzekering verzekert de directe financiële gevolgen (eigen schade) van frauduleus handelen door werknemers en welomschreven soorten van frauduleus handelen door derden (o.a. afpersing, vervalsing van geld of documenten en computerfraude). De waarborg cyberdiefstal in de cyberpolis overlapt met de fraudeverzekering. Vandaar dat sommige cyberverzekeraars de waarborg cyberdiefstal niet aanbieden. Anderen bieden die dekking wel aan, maar met sublimieten en optioneel voor het geval de verzekerde geen afzonderlijke fraudeverzekering heeft afgesloten. De waarborg cyberafpersing binnen de cyberpolis heeft wel zin, ook al beschikt de verzekerde over een fraudeverzekering.

En wat als u als derde aansprakelijk wordt gesteld? In dat geval is er de liability polis waarmee uw aansprakelijkheid wordt gedekt. Dat is uitsluitend het geval wanneer uw fout bewezen kan worden, wat haast onmogelijk is bij een computervirus dat schade aanricht. Voorts worden uw eigen kosten die opduiken bij een cyberaanval – zoals de kosten voor de wedersamenstelling van data – niet gedekt door deze polis.



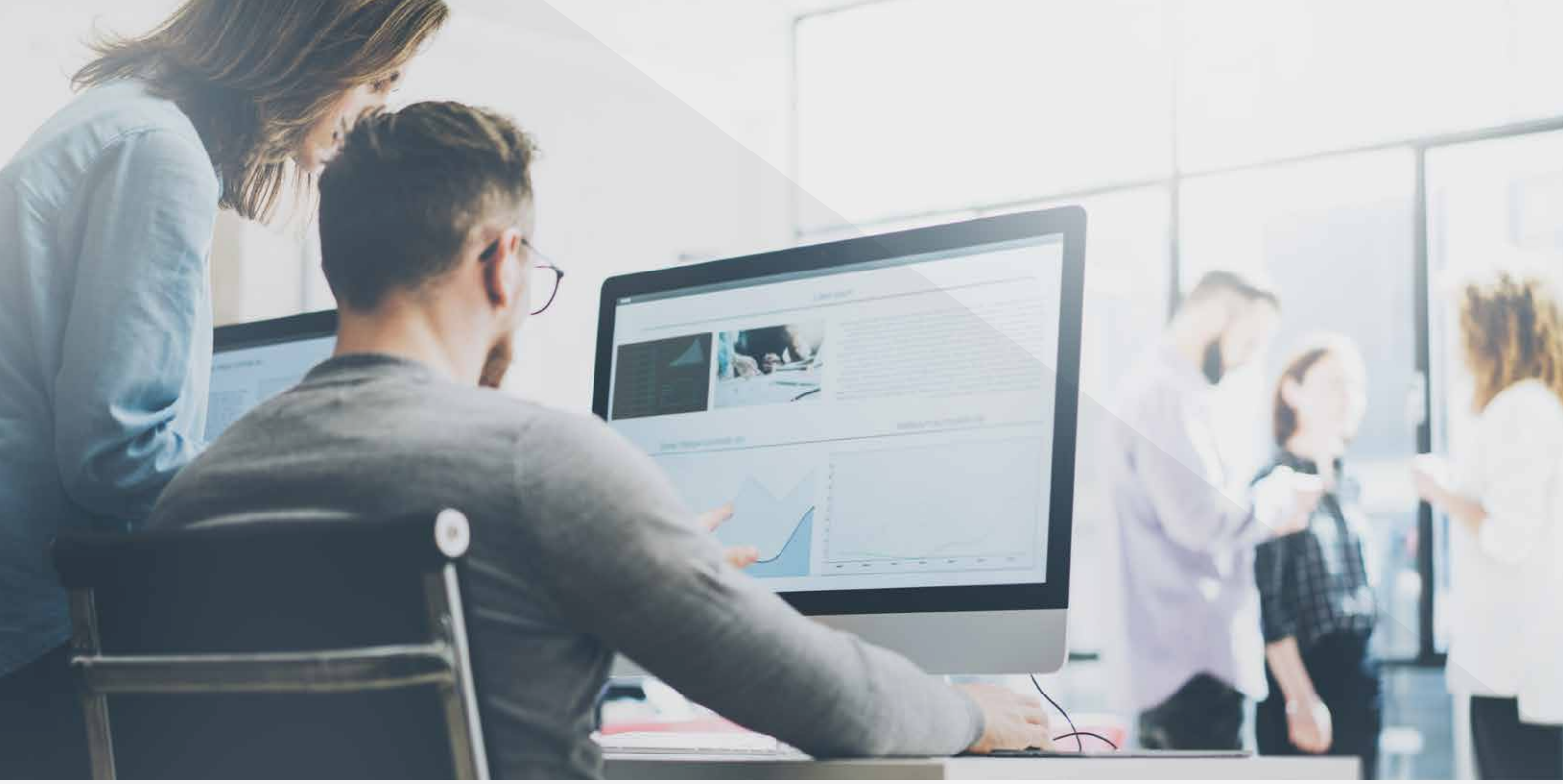
Nieuwe verzekeringsoplossing

Zogenaamde cyberpolissen zijn afgestemd op cyberincidenten: een computervirus legt uw netwerk lam, een hacker blokkeert de toegang tot uw online winkel, door phishing komen alle kredietkaartgegevens van uw grote klanten in het openbaar – de voorbeelden van wat mis kan gaan, zijn talrijk. Meer nog, cyberincidenten kunnen uw onderneming volledig ontregelen.

Een cyberincident valt echter niet altijd te herleiden tot een criminele daad. Ook menselijke fouten of bugs in een softwarepakket kunnen uw data en uw IT-systeem beschadigen. Zowel fouten, ongevallen als daden van kwaadwilligheid kunnen leiden tot een verlies van beschikbaarheid, integriteit en/of vertrouwelijkheid van data, zowel data van derden (onder bewaring van de verzekerde) als data die eigendom zijn van de verzekerde vennootschap zelf (die al dan niet bij derden bewaard of verwerkt worden).

In een bedrijfsomgeving die draait op computers en IT-procedures kan een klein incident immers grote gevolgen hebben. Extra kosten kunnen opduiken om te remediëren en te voorkomen dat het incident zich opnieuw stelt. De productie kan onderbroken of stopgezet worden – de gevolgen zijn dan niet te overzien. Eveneens kunnen juridische implicaties zich voordoen.

Voor al die risico's is een cyberpolis de optimale bescherming.



Cyberverzekering in detail

De oorzaken van het verlies van beschikbaarheid, integriteit of vertrouwelijkheid kunnen divers zijn: een fout van een werknemer; kwaad opzet (hacking, malware); of een ongeval dat gegevens aantast.

De meeste van deze oorzaken zoals kwaad opzet (denial of Service Attack, hacking, virus, targeted malware, enz...), fout van een werknemer en netwerksecurity problemen kunnen verzekerd worden onder een cyberpolis*.

***Noot:** *Sommige schadeoorzaken kunnen echter niet verzekerd worden, bijvoorbeeld een algemene panne van een "Internetprovider of een energieleverancier" (omdat in dergelijke gevallen bij de verzekeraars een cumul van schades ontstaat die verzekeraars niet in zijn geheel kunnen dragen). Een materieel risico zoals een brand is ook meestal uitgesloten omdat cyber verzekeraars van mening zijn dat dit zou moeten gedekt zijn onder de brandverzekering.*

Wat moet er fout gaan?

KWAADWILLIGHEID
- Onbevoegd gebruik
- Virus, worm, logical bomb, denial of service

FOUT
- Bewerkingsfout
- Onbedoeld wissen

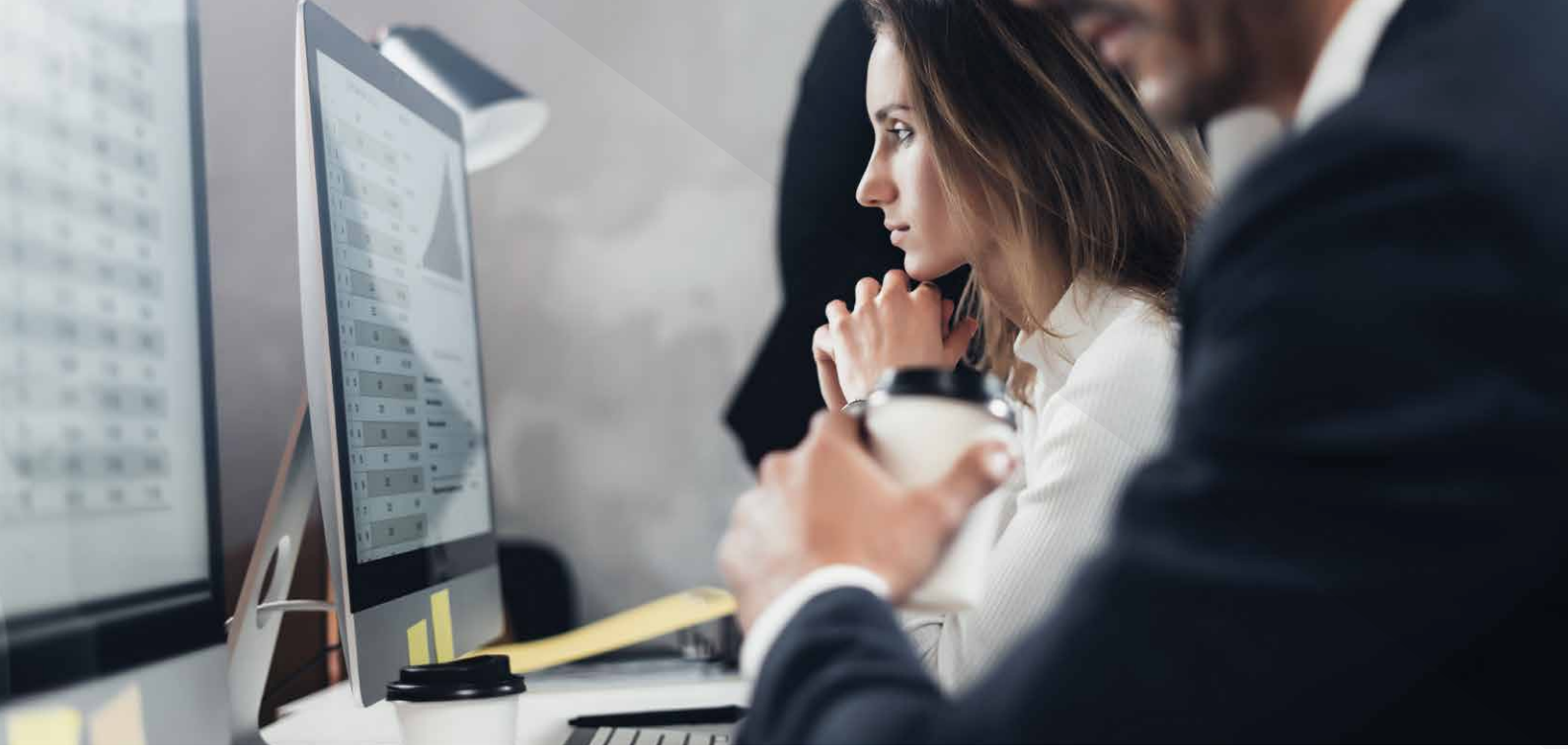
ONGEVAL
- Infrastructurele storing, bliksem
- Storing (over-/onderspanning, telecommunicatie)

VERLIES VAN ...

Beschikbaarheid

Integriteit

Vertrouwelijkheid



Welke risico's zijn verzekerbaar?

Vaak wordt gedacht dat cyberverzekeringen enkel relevant zijn voor bedrijven die in sterke mate afhankelijk zijn van IT-systemen of die veel gegevens beheren, zoals ziekenhuizen of webwinkels, banken, overheden en telecomproviders. Dit is echter een misvatting. Cyberrisico's zijn niet voorbehouden voor grote bedrijven.

Slechts weinig bedrijven zijn opgewassen tegen de financiële gevolgschade van zelfs maar een klein lek of incident. En tegelijk vormen cyberrisico's - zoals aangetoond - een enorm hiaat in de klassieke verzekeringen. Onderstaande figuur geeft nog eens weer tegen welke risico's een cyberpolis uw onderneming beschermt:

RISICO'S

IMPACT OP ACTIVITEITEN

- Onderbreking van activiteiten op productie
- Omzetdaling
- Verlies van contracten, klanten of patiënten
- Reputatieschade
- ✖ Daling van de waarde van de onderneming (beurskoers)

EXTRA KOSTEN, REMEDIËRING

- Onderzoekskosten
- Juridisch advies
- Crisismanagement
- Notificatie
- Systeem- en databeheer
- Herstel IT-systeem
- Afpersingsgelden

JURIDISCHE GEVOLGEN

- Verdedigingskosten
- Schadevergoedingen
- Administratie boetes
- ✖ Strafrechtelijke boetes

Met een cyberpolis beschermt uw onderneming zich tegen de financiële gevolgen van dit verlies. Cyberverzekeringen dekken zowel uw eigen schade als uw burgerlijke aansprakelijkheid tegenover derden. Een goede polis is onmisbaar voor de gezonde werking van een bedrijf. De verschillende polissen op de markt bieden verschillende dekkingen aan.

Daarnaast voorziet de cyberpolis ook in een hulplijn. Bij een schadegeval, of vermoeden van schade, kunt u onmiddellijk contact opnemen met deze hulplijn.

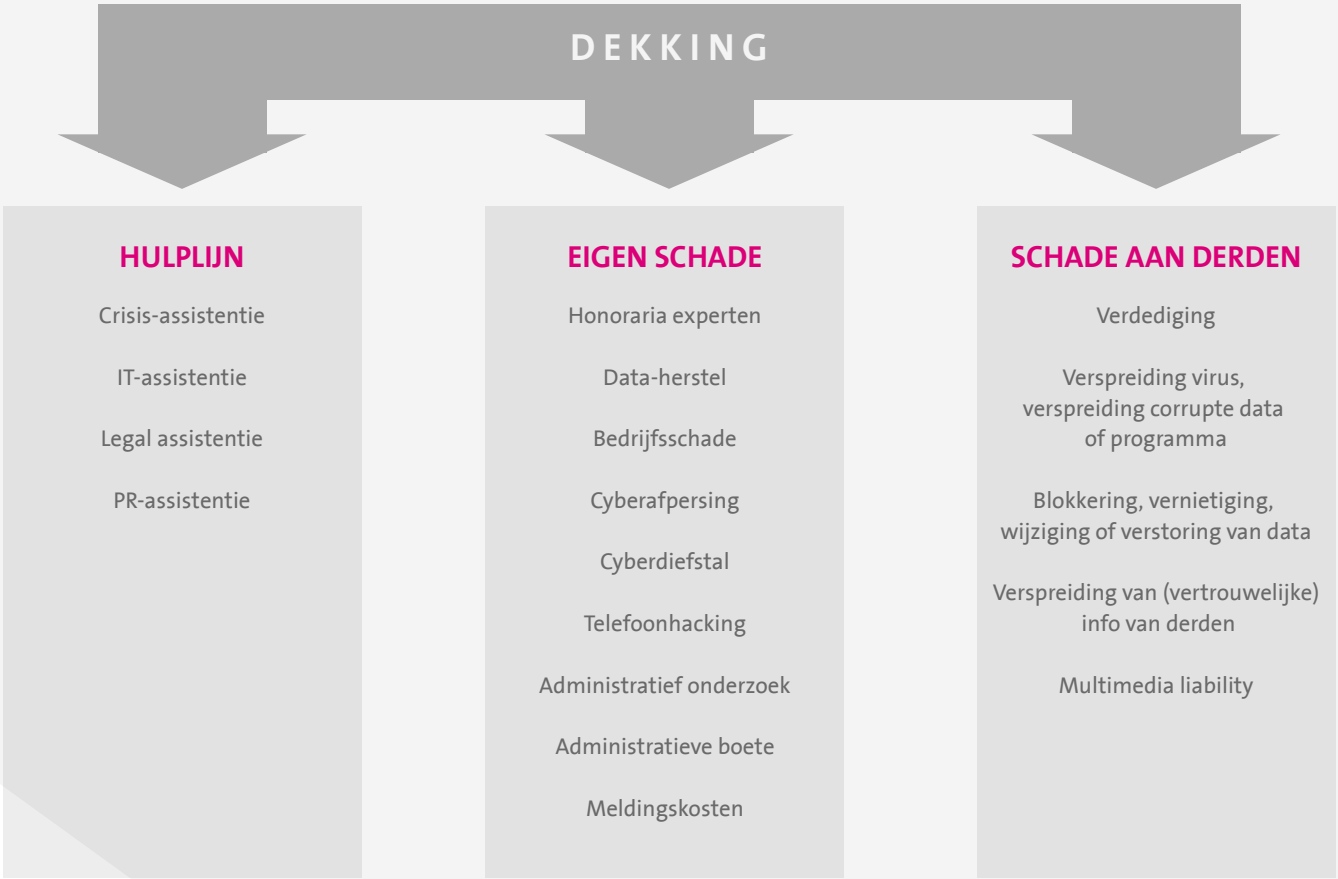
Kosteloos – al dan niet beperkt in tijd – ontvangt u via deze weg verschillende diensten:

Crisisassistentie: een centraal team dat de crisis beheert. Wat is er gelekt? Moet er gemeld worden? Wat is de IT-impact? Wat zijn de te maken IT-keuzes? Alle info wordt voor u als klant samengebracht, zodat de juiste keuzes gemaakt kunnen worden.

IT-assistentie: detectie, herstel en mogelijk ook advies tot verbetering.

Juridische assistentie: specialisten schatten de juridische gevolgen in.

PR-assistentie: communicatie naar de buitenwereld toe.



5. Meer dan alleen verzekeringen

Het afsluiten van een cyberpolis is meer dan alleen het ondertekenen van een contract. De voorbije jaren hebben veel verzekeraars extra diensten ontwikkeld, waardoor bedrijven nog beter in staat zijn het risico op een cyberincident te verkleinen.

Vaak hebben de verzekeraar en de verzekerde in het bijzijn van hun IT-dienstverleners eerst een uitgebreide meeting waarbij ze de belangrijkste toepassingen én de beveiligingsaspecten van de computersystemen bespreken. Dat gebeurt al dan niet op basis van een voorafgaandelijk overgemaakte vragenlijst en gebeurlijke verificatie of nazicht van de systemen.

Sommige verzekeraars geven de verzekerde de mogelijkheid om een kwetsbaarhedenscan uit te voeren. Dit houdt in dat via een scan op de openstaande poorten van het computersysteem en van het netwerk van de verzekerde de online verbindingen worden geanalyseerd en gecontroleerd op kwetsbaarheden.

De verzekerde kan de IT-dienstverlener van de verzekeraar bovendien vragen om bepaalde onderdelen van het netwerk specifiek op kwetsbaarheden te onderzoeken. Nadien ontvangt de verzekerde een rapport met de gevonden kwetsbaarheden per risiconiveau, bovenop adviezen om deze kwetsbaarheden verder te beperken.

De verzekerde heeft in sommige gevallen de mogelijkheid om een toestel te laten installeren dat het inkomende en/of uitgaande dataverkeer voortdurend controleert of tegenhoudt. Het maakt meldingen van zodra er buiten het medeweten van de verzekerde data naar specifieke verdachte IP-adressen wordt gestuurd. Eveneens wordt er door deze toestellen malware opgespoord op de verschillende hardware en netwerken van de verzekerde.

Als door de aanwezigheid van malware data wordt verzonden naar onbetrouwbare IP-adressen zal de transfer hiervan tegengehouden worden en ontvangt de verzekerde onmiddellijk een verwittiging.

Risicoplanning

De verzekeraars bieden de verzekerde ook de mogelijkheid om aan risicoplanning of -preventie te doen door afspraken te maken op het vlak van:

Legal: gedurende 2 uren worden de to-do's besproken in geval van een privacy-breach, kan er een privé-training plaatsvinden, etc...

Forensisch: gedurende 1 uur bespreekt een forensisch expert met de verzekerde de nodige stappen die men dient te ondernemen bij een cyberincident.

Public Relations: gedurende 1 uur bespreekt een pr-expert met de verzekerde de verschillende scenario's van een cyberincident.

Preventie: een kwetsbaarhedenanalyse uitvoeren, naast de mogelijkheid om een draaiboek op te stellen voor het geval een incident zich voordoet.

Contractscreening: een gespecialiseerd bureau screent de overeenkomst(en) tussen de verzekerde en een clouddienst.

Bovenstaande maatregelen verschillen van verzekeraar tot verzekeraar, al bieden ze allemaal preventieve maatregelen om de verzekerde zoveel mogelijk voor schade te behoeden.

6. Meest voorkomende cyberrisico's

Databreach

Een databreach of datalek is het al dan niet opzettelijk vrijgeven van beveiligde informatie. Die vrijgekomen data kan dan gebruikt worden voor uiteenlopende doeleinden. Zo kunnen persoonsgegevens door privé-bedrijven worden gebruikt voor direct marketing. Bij dergelijke datalekken kan ook informatie verspreid worden over betaalwijzen of betaalmiddelen, wat een risico inhoudt voor frauduleuze bankverrichtingen.

Cryptolocker

Cryptoware of cryptolocker is ransomware waarbij computerbestanden verloren kunnen gaan. Cryptoware versleutelt computerbestanden. Het virus zelf wordt verspreid via bijlagen in e-mails en links. Slachtoffers laten zich hier vaak door misleiden. Om weer toegang te krijgen tot de computerbestanden is een geheime sleutel nodig waarover alleen de cybercriminelen beschikken. Ze vragen losgeld om de bestanden te herstellen, al gebeurt dat zelfs na betaling doorgaans niet of slechts/enkel gedeeltelijk.

Telefoonhacking

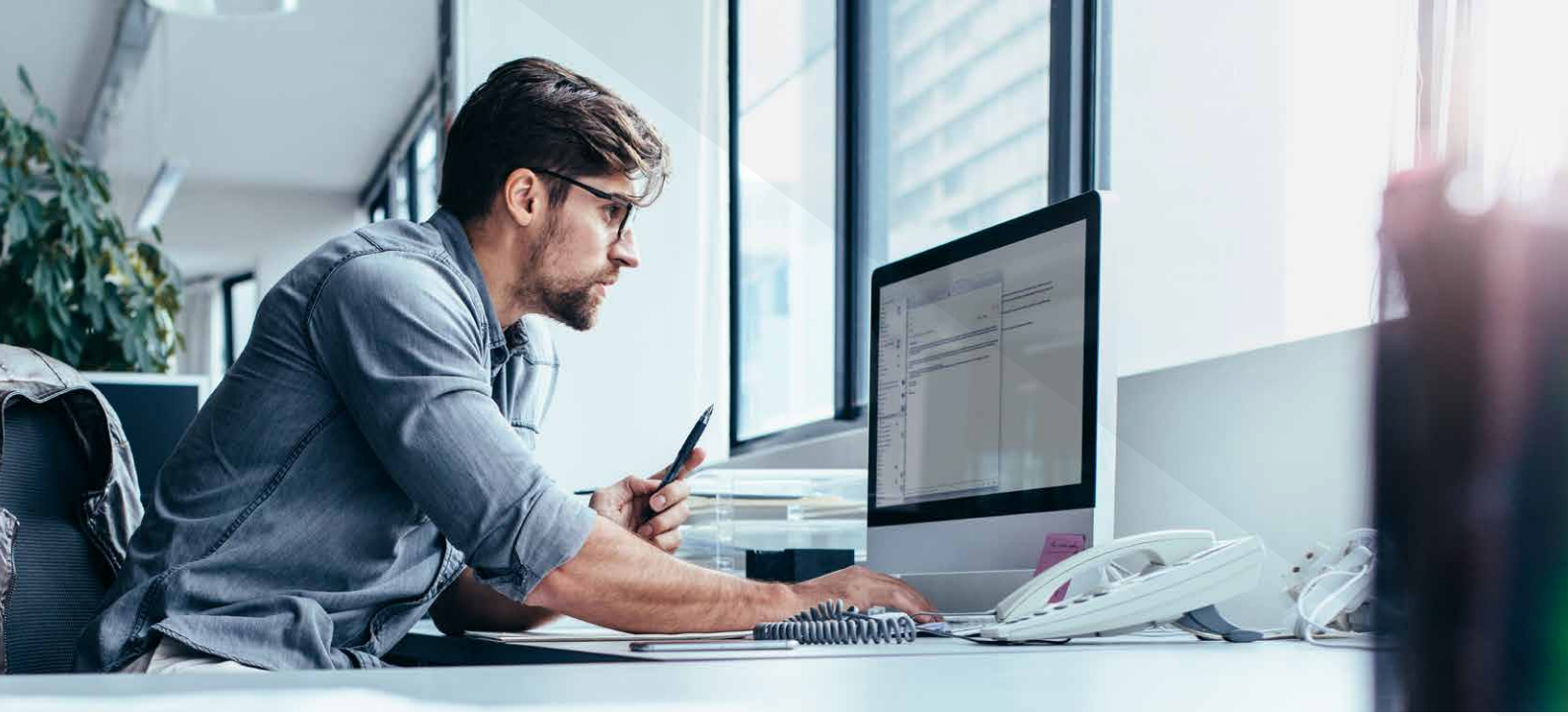
Door binnen te breken in het systeem of zich op een andere manier toegang te verschaffen, kan een aanvaller bellen op kosten van uw bedrijf. Dit soort hacks zijn steeds van korte duur, aangezien ze bij een volgende factuur onmiddellijk aan het licht komen. Schadegevallen lopen bijgevolg niet hoger op dan 100.000 euro.

Cyberdiefstal

Het per mail en telefoon hengelen naar informatie over uw geldzaken is de snelst groeiende tak van digitale criminaliteit. Het is een vorm van oplichting waarbij criminelen zich voordoen als werknemers van betrouwbare instanties zoals een bank of creditcardmaatschappij. Zij vragen uw inloggegevens, creditcardinformatie, pincode of andere persoonlijke informatie. Criminelen proberen uw vertrouwen te winnen om persoonlijke gegevens te ontfutselen om toegang te krijgen tot een bankrekening of om producten te kopen op uw kosten.

Netwerkonderbreking

Een DDOS-attack, een netwerk outage door een menselijke fout, een gehackte firewall,... Allen kunnen ze een netwerkonderbreking veroorzaken. Systeemherstelkosten omvatten ook systeemupdates om verdere incidenten te voorkomen. Deze actie brengt doorgaans een boel kosten met zich mee. Ook herstelkosten om het netwerk of de gegevens te herstellen en onderzoek te voeren naar de oorzaak van het probleem (forensisch onderzoek en wedersamenstellingskosten voor herstel van gegevens) vallen hieronder.



7. Evoluties

In schadegevallen

Als ondernemer stelt u zich mogelijk de vraag naar het waarom van een cyberverzekering. Uw IT-systeem is immers op het ergste voorbereid – of daarvan bent u overtuigd. Er zijn tal van firewalls en virusscanners actief, geregeld worden veiligheidsupdates en ontelbare andere maatregelen uitgevoerd. Bovendien houdt uw IT-manager een oogje in het zeil. Wat kan er dan alsnog misgaan?

Dezelfde vraag kan gesteld worden wanneer het gaat over het nut van een brandverzekering. U hebt immers talloze rookmelders en branddetectoren geïnstalleerd. Uw bedrijfspand is uitgerust met branddeuren en sprinklers die aanspringen bij brand. Kortom, op het vlak van brandpreventie heeft u kosten noch moeite gespaard. Waarom dan een brandverzekering afsluiten?
De reden is eenvoudig: omdat er nog steeds een restrisico bestaat. Hoeveel maatregelen u ook treft, het is onmogelijk om het risico tot nul te herleiden. Daarom vindt u het verstandig om een brandverzekering af te sluiten. En om diezelfde reden dekt u zich best ook in tegen cybercrime.

Die nieuwe vorm van criminaliteit wint immers almaar meer terrein. Steeds talrijker zijn de feiten die plaatsvinden, steeds driester gaan deze criminelen tewerk. Enkele jaren geleden leefde nog het idee dat een cyberpolis een veeleer overbodige veiligheidsmaatregel was. Maar door de talloze, verbazingwekkende feiten die steeds vaker de pers halen, stellen weinig experts de wenselijkheid van dit nieuw type verzekering nog in vraag.

In de verzekeringswereld

De wereld is voortdurend in verandering. Wat vandaag gangbaar is, behoort morgen misschien alweer tot het verleden. Het betekent dat ook de context waarin ondernemers zakendoen steeds wijzigt, en die gewijzigde context brengt nieuwe risico's met zich mee. Dan is het aan de verzekeringswereld om met gepaste oplossingen te komen. Dat ging zo in het verleden, en dat zal ook in de toekomst zo blijven gaan.

Wie enkele stappen terug in de tijd zet, ontdekt algauw dat ruwweg elk nieuw decennium een nieuw type verzekering het levenslicht zag.

Verzekeringsevolutie

Zo werd in de jaren tachtig duidelijk dat onder impuls van een bloeiend economisch klimaat bedrijven steeds groter werden. Enorme kapitaalconcentraties gingen hiermee gemoeid. Het was echter diezelfde omvang die hen parten speelde wanneer ze na een forse brand opnieuw overeind trachten te krabbelen. Natuurlijk waren ze verzekerd voor de materiële schade die ze hadden geleden. Maar voorts werd er geen rekening mee gehouden dat het tijd vergde om nieuwe bedrijfsgebouwen op te richten. Tegen de tijd dat ze zover waren en de productie konden hervatten, had hun vroegere clienteel elders onderdak gevonden. Het bankroet liet dan ook niet lang op zich wachten.

Vanbreda reageerde door - naast de klassieke brand-verzekering - een verzekering voor bedrijfsschade te lanceren. Dit type verzekering ging als een levens-verzekering voor bedrijven fungeren. Het hielp hen om die periode na een brand door te komen. Lang niet elke ondernemer zag hier meteen de meerwaarde van in, maar de tijd wees uit dat bedrijven die hierop intekenden sterker uit zo'n ongemeen harde tegenslag kwamen.

In de jaren negentig was het de polis bestuurders-aansprakelijkheid die de aandacht trok en voor snoeiharde kritiek zorgde. Met deze polis konden bestuurders zich voortaan indekken tegen de gevolgen van beleidsfouten. De eerste reacties waren echter weinig enthousiast. Klanten zagen het als een polis op maat van de grote multinationals, het was geen verzekeringsproduct waar zij baat bij hadden.

Maar in diezelfde periode wijzigde de wetgeving grondig en zo ontstonden steeds meer rechtsgronden op basis waarvan een bestuurder aansprakelijk kon worden gesteld. Als koploper op de Belgische markt zag Vanbreda dit nieuwe risico opdoemen. Vandaag is deze polis bestuurdersaansprakelijkheid uitgegroeid tot een standaardverzekering die zijn meerwaarde ettelijke malen heeft bewezen.

Het was dan weer de dioxinecrisis die in de jaren 2000 aantoonde dat de klassieke polis voor product-aansprakelijkheid voor een voedingsbedrijf onvoldoende was. De overheid sprong deze bedrijven destijds ter hulp en voorkwam dat de Belgische voedingssector gedecimeerd werd.

In de verzekeringswereld reageerde Vanbreda met een verzekering recall en contaminatie. Voedingsbedrijven konden zich zo indekken voor de schade die geleden werd wanneer producten dienden teruggeroepen te worden. In de jaren die volgden deed de ene voedingscrisis na de andere zich voor. Gelukkig konden voedingsbedrijven zich voortaan met deze polis beschermen tegen de gevolgen van contaminatie. De polis groeide zo uit tot een standaardverzekering in de sector.

Wat dan te denken van een cyberverzekering? Het staat vast dat de mening van vele experts nu reeds grondig gewijzigd is. Terwijl enkele jaren geleden een cyberverzekering nog afgeschreven werd als een polis op maat van enkelingen, wordt het bestaan van dit nieuw type verzekering vandaag steeds breder gedragen. Ook bij de bedrijven zelf.

8. Besluit

De wereld is steeds in verandering. Geen enkele ondernemer die daarvan opkijkt. Het ligt voor de hand dat uw verzekeringsprogramma steeds afgestemd is op de heersende context. Zoals er polissen verdwijnen – zal de zelfrijdende auto straks de verzekering burgerlijke aansprakelijkheid overbodig maken? – zien ook nieuwe polissen het levenslicht.

Als professioneel makelaar ziet Vanbreda het als zijn plicht om continu de wereld te scannen op nieuwe risico's. Wij stellen alles in het werk om die te vertalen in verzekeringsoplossingen die de financiële impact van deze risico's maximaal opvangen. In die context is de cyberpolis een product waarvan de noodzaak steeds duidelijker wordt.

Indien u hierover meer informatie wenst, dan staan wij u graag te woord.

Gerrit Mets
Cyberexpert
Vanbreda Risk & Benefits
Gerrit.Mets@vanbreda.be

Tom Van Britsom
Cyberexpert
Vanbreda Risk & Benefits
Tom.VanBritsom@vanbreda.be

Christophe Liekens
Cyberexpert
Vanbreda Risk & Benefits
Christophe.Liekens@vanbreda.be

9. Over Vanbreda Risk & Benefits

Vanbreda Risk & Benefits is de grootste onafhankelijke Belgische verzekeringsmakelaar en risicoconsultant, en de toonaangevende verzekeringspartner in de Benelux. Sinds 1937 formuleert Vanbreda antwoorden op de risicovragen van bedrijven, publieke en sociale instellingen en ondernemers.

Bij Vanbreda adviseren meer dan 600 medewerkers ruim 60.000 cliënten op vlak van verzekeringen, risicobeheer en employee benefits. Een grondige kennis van de activiteiten en risico's van onze cliënten en een doorgedreven technische knowhow en dienstverlening zijn de hoekstenen van ons succes, wat weerspiegeld wordt in een cliëntenretentie van meer dan 95%.

Als marktleider hebben we als geen ander zicht op nieuwe tendensen in de snel evoluerende verzekeringswereld. Onze experten spelen kort op de bal door innovatieve producten te ontwikkelen die beantwoorden aan uw meest recente verzekeringsnoden. Bescherming tegen cyberrisico's is hiervan een voorbeeld. Met vooruitstrevende technologieën en bedrijfseigen online tools verbeteren we onze efficiëntie en vereenvoudigen we de communicatie voor onze cliënten.

Via het Europese partnership EOS RISQ en het internationale partnership Lockton Global bieden we wereldwijd dezelfde kwalitatief hoogstaande dienstverlening aan.

www.vanbreda.be
cybersecure@vanbreda.be
03 292 00 13

Laatste update 03/2021

Verantwoordelijke uitgever: Vanbreda Risk & Benefits NV
Plantin en Moretuslei 297, 2140 Antwerpen
RPR Antwerpen, afdeling Antwerpen - BTW BE0404.055.676