Cyberrisico's in de transport- en logistieke sector

vanbreda
RISK & BENEFITS

Bent u goed verzekerd tegen cybercriminaliteit?

Door de toenemende digitalisering en automatisering van de **transport- en logistieke sector** is ook deze industrie een mogelijk **doelwit van cybercriminaliteit** geworden. De vele schakels in de logistieke keten en het grote aantal kleine spelers die goederen van derden behandelen, maken de sector zelfs extra kwetsbaar.

Bij een cyberaanval in de transport- en logistieke 'supply chain'-sector wordt in de eerste plaats gedacht aan het verlies van producten, cargo, lading en de mogelijke directe gevolgen voor de afnemer.

De **impact van een cyberaanval** is echter veel diverser en omvangrijker: ongeoorloofd gebruik van het systeem waarmee de expediteur zijn logistieke planning doet, misbruik van het trackingsysteem van goederen, een virusinplanting in de registratie-applicaties van radarsystemen of zelfs het verstoren van de navigatiesystemen van schepen kunnen enorme financiële gevolgen hebben voor de klanten of leveranciers, maar ook voor het gehackte bedrijf zelf.

Denk maar aan alle kosten die noodzakelijk zijn om het probleem op te sporen en te herstellen, de eigen bedrijfsonderbreking, de kosten om een imagoschade te vermijden of in te perken, kosten verbonden aan verlies of encryptie van al dan niet gevoelige gegevens enzovoort.

Klassieke verzekeringen, zoals de brand- en bedrijfsschadeverzekering, bieden de klant financiële zekerheid in geval van materiële schade aan het eigen patrimonium. Met aansprakelijkheidsverzekeringen kan schade aan derden worden vergoed die in oorzakelijk verband staat met een fout van de verzekeringsnemer.

Die klassieke polissen dateren echter van het 'pre-digitale' tijdperk en focussen op materiële en lichamelijke schade. De financiële verliezen die gepaard gaan met het verlies van data- of netwerkverbindingen worden dus niet (of niet volledig) gedekt door deze klassieke verzekeringspolissen.

De **nood aan een sluitende verzekeringsoplossing** dringt zich dan ook op.

NYE-630042-16-01

Informatiebeveiliging van goede kwaliteit

Cyberrisico's zijn onlosmakelijk verbonden met de **beschikbaarheid (B)**, de **integriteit (I)** en/of de **vertrouwelijkheid (V)** van data, de zogenaamde "BIV-driehoek".

De BIV-driehoek geeft de verschillende criteria van kwalitatieve informatiebeveiliging weer:

- De opgeslagen gegevens moeten **beschikbaar** zijn op het gewenste moment.
- De **integriteit** van data is verzekerd als de juiste data aan de juiste records gelinkt zijn.
- De **vertrouwelijkheid** van de informatie zorgt ervoor dat enkel de personen voor wie de informatie bedoeld is, er toegang toe hebben.

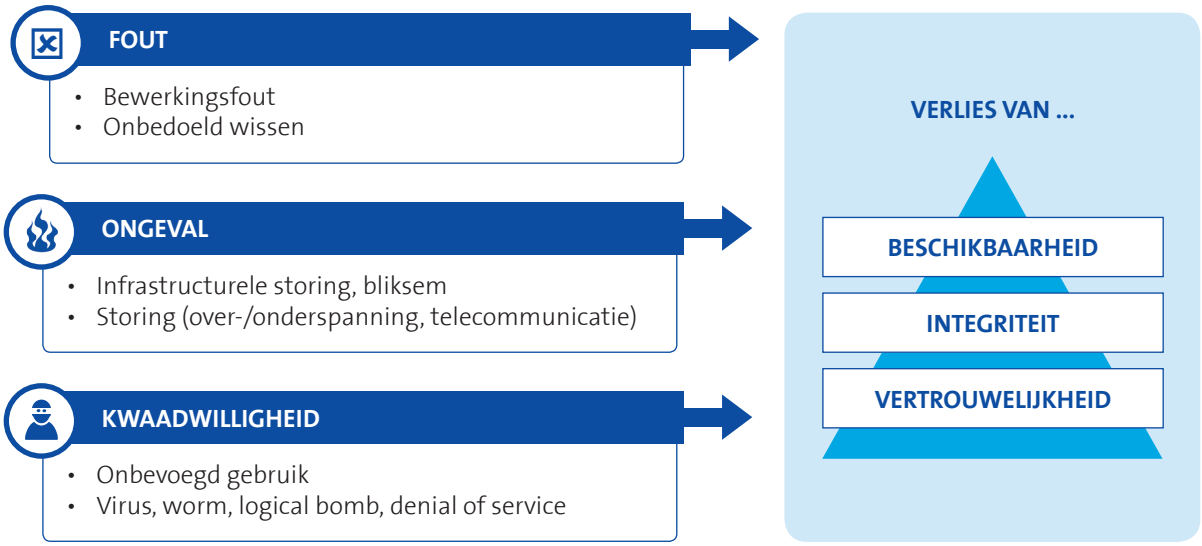
Het beheren en beheersen van deze BIV- driehoek wordt o.a. mogelijk gemaakt door de **Wet op de Privacy** (8 December 1992) ter bescherming van de persoonlijke levenssfeer i.k.v. verwerking van de persoonsgegevens, maar wordt sinds december 2015 verder gesteund door de **nieuwe Europese regelgeving: de "General Data Protection Regulation Act"** welke op Europees niveau dataverwerking regelt, samen met de daaraan verbonden plichten en boetes in geval van datalekken.

Een cyberpolis verzekert de **financiële gevolgen** van het verlies van of een inbreuk op die 'BIV' van data.

Oorzaken van schade

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 kunnen verzekerd worden via een cyberpolis.

Net zoals elke andere polis kent de cyberverzekering ook enkele uitsluitingen, zoals bv. een algemene panne van een internetprovider of een energieleverancier (in dergelijke gevallen kan immers een cumul van schades ontstaan die verzekeraars niet in zijn geheel kunnen dragen).



Gevolgen van een cyberincident

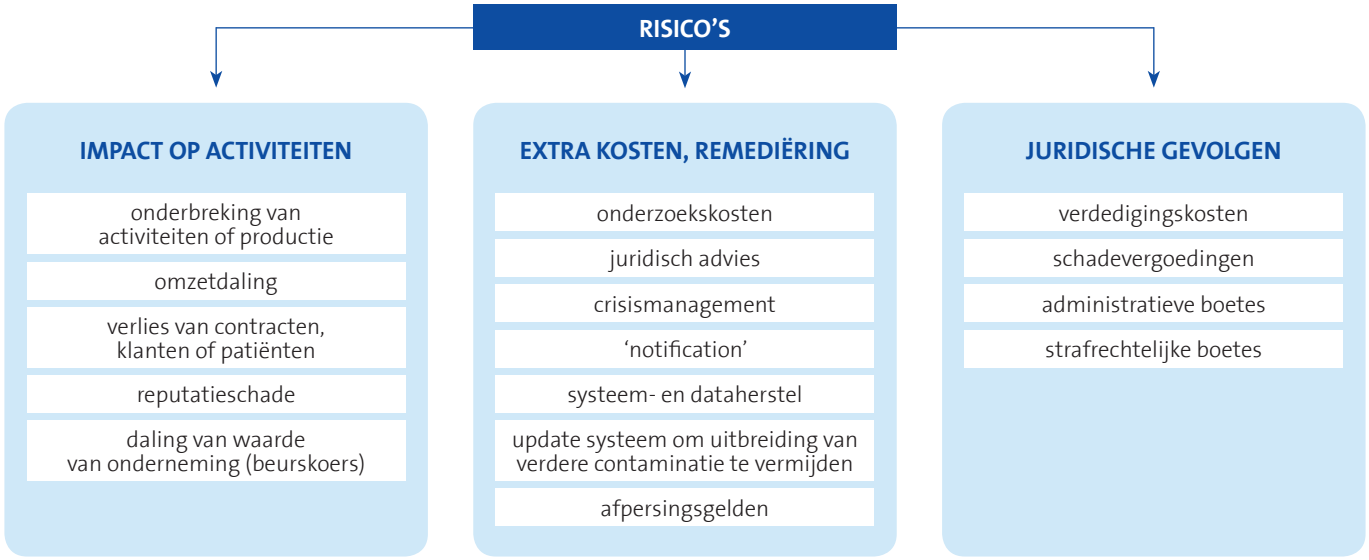
We kunnen de financiële gevolgen van een cyberincident in drie grote domeinen sorteren:

- impact op activiteiten;
- extra kosten, remediëring;
- juridische gevolgen.

Afhankelijk van het soort incident wordt een ander domein van risico's getriggerd.

Het publiceren van een database met persoonsgegevens op het internet kan aanleiding geven tot juridische kosten terwijl er ook extra kosten zullen moeten gedaan worden om de betrokken slachtoffers persoonlijk te verwittigen.

Een 'denial of service'-aanval die een bedrijf een hele week stil legt, zal vooral een grote impact op de bedrijfsactiviteit zelf hebben.



Voorbeelden van cyberaanvallen

Voorbeelden van en redenen voor cyberaanvallen in de transport- en logistieke sector zijn legio:

- cyber hacking in twee overslagbedrijven in de haven van Antwerpen om containers vol drugs afhandig te maken vooraleer de rechtmatige eigenaar ze kan ophalen;
- hacking van het systeem van de expediteur om loggegevens te stelen en door te verkopen aan de hoogste bieder of om ongeoorloofd inzicht te verwerven van waar en wanneer bepaalde transporten ingepland zijn;
- een DDOS (Distributed Denial of Service)-aanval legt een bedrijf 'plat' om een ideologisch of politiek-economisch statement te maken;
- installatie van ransomware (gegevens worden versleuteld en dus onbruikbaar) om het bedrijf af te persen;
- 'portables' (bv. gsm's, tablets, ...) vallen in verkeerde handen met het oog op het verkrijgen van toegang tot de bedrijfssystemen;
- spionage, concurrentie: een aanval op de systemen die de lading, lossing en opslag beheersen, zorgt voor vertraging in verscheping/levering van een nieuw model van producten met imagoschade en financiële verliezen tot gevolg;
- AIS (Automatic Identification System)-hack: de coördinaten van de locatie van een schip worden niet meer doorgezonden, waardoor het schip officieel van de radar verdwijnt. De hackers kunnen het schip echter wel blijven tracken en kunnen het schip zelfs een andere koers laten innemen (bv. schip dat in Somalische wateren wordt gekaapt); ...

Cyberrisico's verzekerd

Een grondige analyse van uw huidige verzekeringen is van belang om te weten welke risico's al of niet gedekt zijn. In onderstaande tabel vindt u een overzicht van de dekkingen die in een cyberpolis voorzien zijn. U kunt zelf de vergelijking maken met een klassieke polis brand of burgerlijke aansprakelijkheid.

Dekkingen	PI / GL*	Crime	Property	Cyber
managementhulp bij een verzekerde gebeurtenis (incl. eerste hulp)	■	■	■	■
notificatie- en communicatiekosten	■	■	■	■
PR-kosten (reputatiebescherming)	■	■	■	■
wedersamenstellingskosten van eigen en TP-data	■	■	■	■
onderzoekskosten en opsporingskosten	■	■	■	■
bedrijfsschade + bijkomende kosten	■	■	■	■
bijstandskosten met een toezichthoudende instantie	■	■	■	■
verdediging + schadevergoeding (aansprakelijkheid)	■	■	■	■
verhaalskosten	■	■	■	■
losgeld in geval van afpersing	■	■	■	■
cyber theft	■	■	■	■
hacking telefooncentrale	■	■	■	■

■ geen dekking ■ gedeeltelijke dekking ■ dekking

*PI: beroepsaansprakelijkheid / GL: algemene aansprakelijkheid

Ook voor polissen toegespitst op de transport- en logistieke sector raden we aan een aparte analyse te maken. Hou alvast rekening met volgende aandachtspunten:

- **Cargoverzekering**: dit is een zogenaamde 'alle risico'-polis (schade aan of verlies van cargo zal via deze polis verzekerd worden). Diefstal van cargo valt hier ook onder, maar de BVT (Koninklijke Belgische Verening van Transportverzekeraars) voorziet in hun standaard (algemeen gangbare) polissen een uitsluiting 'cybernetische aanvallen': alle verlies of schade die rechtstreeks of onrechtstreeks veroorzaakt wordt door een computer, virus, ... is dus niet gedekt.

- **CMR-polis**: dit is een niet verplichte aansprakelijkheids-polis waarin tot een maximum van ongeveer 10 euro per kilo vracht wordt vergoed. Daar dit echter ook een aansprakelijkheidspolis is, zal in geval van een hacking of cyberaanval zonder aangetoonde/bewezen fout van de verzekerde geen dekking worden verleend.

Volgende stappen

1. Stel orde op zaken

- Stel uw algemene en specifieke IT-gerelateerde beveiligingsprocessen op punt via audits en systematische updates of controles.
- Verwerf inzicht in welke data door uw bedrijf verwerkt worden of waarmee uw bedrijf in aanraking komt, en welke processen er op de data worden voltrokken.
- Analyseer uw eigen contractuele aansprakelijkheden t.o.v. leveranciers en afnemers, en eis van uw partners dat ook zij hiervoor de nodige stappen ondernemen. U bent maar zo sterk als uw zwakste schakel!
- Breng mogelijke probleemgebieden binnen uw bedrijf in kaart.
- Maak cyber bespreekbaar binnen uw bedrijf en beperk dit niet tot uw IT-departement. De resources komen immers van hogeraf en sensibilisering van alle werknemers is essentieel om dit hele proces te doen slagen.

2. Zorg voor een business continuity plan

Als er zich een probleem voordoet, moet u uiterst efficiënt kunnen voortwerken en weten wie verantwoordelijk is voor het opvolgen van de schade (IT, legal, communicatie, ingenieurs, ...). Weet dus welke maatregelen er dienen genomen te worden in geval van een crisis.

3. Analyseer uw huidige verzekeringsportefeuille

Laat u hierbij begeleiden door experts. Misschien bent u toch al goed verzekerd?

Meer informatie?

Annelies Helsen
Product Manager
Tel. + 32 3 217 54 13
annelies.helsen@vanbreda.be

Cécile Vassart
Product Manager
Tel. + 32 3 217 55 20
cecile.vassart@vanbreda.be

Verantwoordelijke uitgever: Pedro Matthynssens
Vanbreda Risk & Benefits NV • Plantin en Moretuslei 297 • 2140 Antwerpen
RPR Antwerpen, afdeling Antwerpen • BTW BE 0404 055 676 • FSMA 13718 A-R