

Cyber Risk Solutions

De continuïteit en digitale veiligheid van uw onderneming op maat verzekerd

Van Dessel
Insurance Brokers

In een digitale wereld zijn bedrijven meer dan ooit afhankelijk van technologie en internet. Ook al is uw onderneming goed beveiligd of bent u slechts beperkt afhankelijk van IT kan de impact van een cyberincident op uw bedrijf behoorlijk groot zijn.

Digitale aanvallen zijn dichterbij dan je denkt

Net zoals het beschermen van je onderneming tegen brand (kans 1/800), zou het beschermen tegen cyberrisico's (kans 1/5) vanzelfsprekend moeten zijn. Toch zien we dat niet iedereen een verzekering heeft om de hoogoplopende kosten voor herstel en omzetverlies bij een digitale aanval op te vangen.

Daar waar hackers zich vroeger voornamelijk richtten op grote bedrijven, zijn vandaag ook KMO's een doelwit geworden. Cybercriminelen weten immers dat kleinere bedrijven vaak minder uitgebreide beveiliging hebben en dus eenvoudiger binnen te dringen zijn.

Hackers surfen mee op de golf van digitalisering

Door de opmars van digitalisering, artificiële intelligentie en toenemende verbondenheid tussen bedrijven en programma's worden de risico's alleen maar groter. Hackers maken handig gebruik van deze technologische vooruitgang om hun aanvallen steeds slimmer en geraffineerder te maken. Phishingmails en aanvallen leunen alsmaar dichter bij de realiteit aan waardoor deze onderscheiden een moeilijke opdracht wordt.



2024 in cijfers

- Er waren 24% meer ransomware aanvallen dan het jaar voordien burgerlijke en beroepsaansprakelijkheid.
- Incidenten verschuiven zich meer en meer van grote ondernemingen naar KMO's.
- 73% van de incidenten vindt oorzaak bij eigen personeel (o.a. klikken op phishingmail, openen besmette bijlage)
- 69% meer incidenten bij Belgische bedrijven dan jaar voordien.
- 24 dagen is een bedrijf gemiddeld inactief na een cyberincident.
- €1.000.000 is het gemiddeld gevraagde bedrag (losgeld) geëist door hackers.

Bron: CCB Belgium

Een goede beveiliging is cruciaal maar ook dan blijft het risico bestaan...

Onderstaande preventiemaatregelen zijn vandaag de dag niet weg te denken en gaan hand in hand met het uitnemen van een cyberverzekering indien er toch iets misloopt.

- Netwerktoegangscontrole: o.a. sterke paswoorden (bv. minstens 14 tekens) en meervoudige authenticatie voor inloggen van op afstand.
- Training en bewustwording: o.a. verplichte opleiding en phishingtraining voor personeel.
- Bedrijfscontinuïteit: o.a. crisisplan en nemen van dagelijkse back-ups van kritische systemen.
- Beveiligingsmaatregelen: o.a. antivirus, encryptie van gevoelige data en regelmatige updates van software en systemen.

Recordpiek van cyberaanvallen op Belgische bedrijven...

Als Europese draaischijf is ons land een populair doelwit. Er waren nooit zoveel aanvallen op onze economie dan het afgelopen jaar. Ook in onze buurlanden zien we een gelijkaardige stijging. In België zijn er gemiddeld zo'n 1.231 aanvallen op organisaties per week.

Wereldwijd werd er afgeklokt op een gemiddelde toename van digitale aanvallen van zo'n 75%. Volgens recent onderzoek bij ondernemers worden cyberdreigingen dan ook als hoogste risico ingeschat hetwelk de continuïteit van zijn/haar onderneming kan aantasten.

Vandaag de dag is helaas elke onderneming blootgesteld aan het toenemende risico en niet enkel grote bedrijven die fel afhankelijk zijn van IT of een digitale infrastructuur.

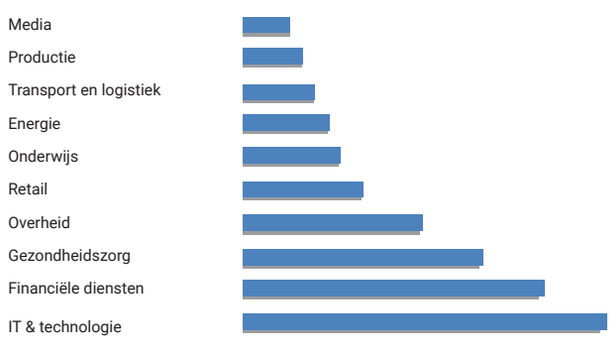
Vele bedrijven staan digitaal in verbinding met elkaar, niet enkel via computers of software maar ook slimme apparaten zijn vaak verbonden met internet o.a. slimme thermostaat, beveiligingscamera's, industriële machines, zonnepanelen.

Ook via deze weg kunnen hackers zich een weg naar binnen dringen.
In onderstaande grafiek kunnen we zien dat het speelveld van hackers al zeer uitgebreid is en cyberincidenten voorkomen in quasi alle sectoren.

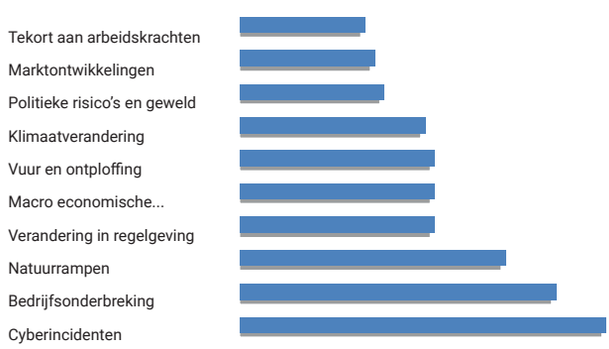
Veelgebruikte "hacking" methodes

- Phishing: slachtoffers worden misleid om gevoelige informatie of wachtwoorden te delen.
- Ransomsware: schadelijke software versleutelt systemen en losgeld wordt gevraagd om deze vrij te geven.
- Zero-day-aanval: aanval die gebruikt maakt van onbekende kwetsbaarheden waarvoor nog geen update beschikbaar is.
- Credential stuffing: aanval waarbij hackers gestolen gebruikersnamen en wachtwoorden van andere datalekken gebruiken om toegang te krijgen.
- DDOS-aanval: servers/websites worden onbereikbaar door bewust overvloedig digitaal verkeer.
- Brute force aanval: geautomatiseerd zoeken en invullen van wachtwoorden tot juiste communicatie gevonden wordt.
- Data lek: gevoelige data wordt gestolen of verwijderd.

Bron: CCB Belgium



Bron: Allianz Risk Barometer 2024



Welke tussenkomst mag je verwachten?

De cyberpolis komt tussen voor de financiële kosten t.g.v. ongeoorloofde toegang van een derde partij op het netwerk/systeem waaruit hack, virus, datalek, aansprakelijkheid, afpersing of bedrijfsonderbreking voortkomt.

Naast de terugbetaling van de eventuele financiële kosten biedt de polis ook 24/7 bijstand van een team van experten die helpen in het oplossen, beperken en herstellen van de cyberaanval om zo snel mogelijk de bedrijfsactiviteiten te hervatten.

Eigen schade

- 24/7 Hotline & crisis assistance
- Kosten voor herstel en wederopbouw IT-omgeving
- Forensische experts
- Kosten voor IT-experts

Cybercriminaliteit

- Losgeld bij cyberafpersing of ransomware
- Kosten in geval van cyberafpersing of ransomware
- Cyberfraude (sublimiet/ optionele waarborg)

Aansprakelijkheid

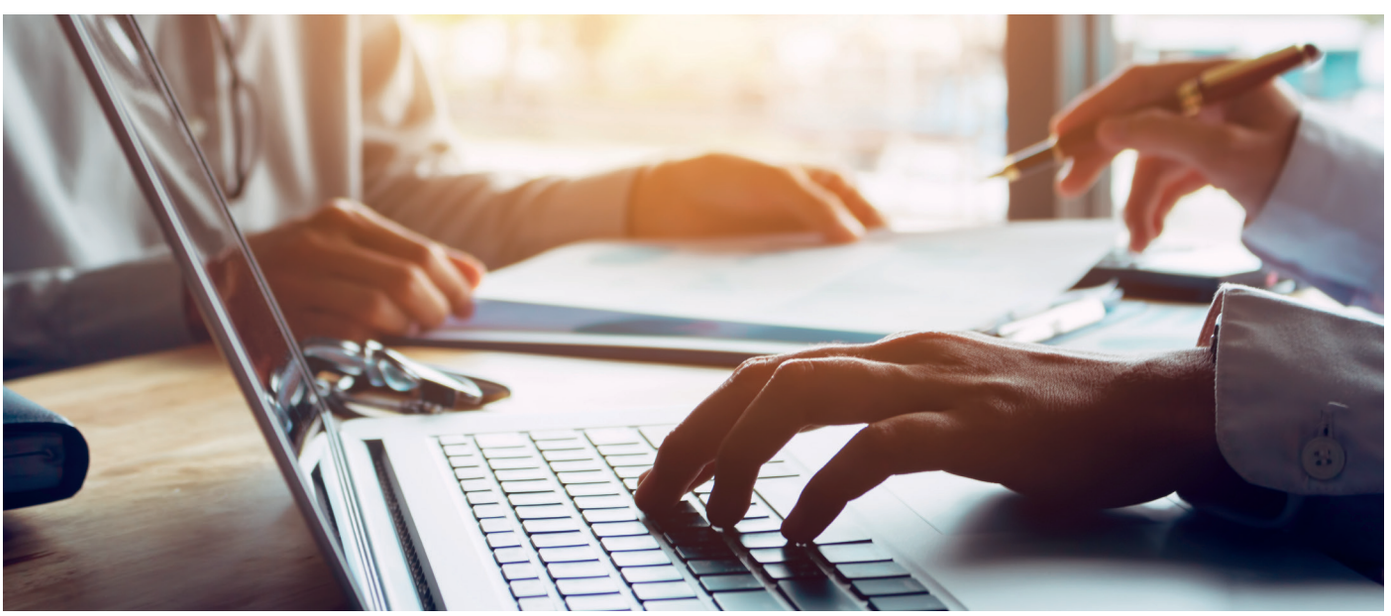
- Data-aansprakelijkheid
- Multimedia-aansprakelijkheid
- Netwerk-aansprakelijkheid (bv. virusoverdracht)
- Boetes (bv. GDPR)
- Juridische bijstand en verdedigingskosten

Bedrijfsschade

- Omzetverlies door cyberincident/systeem falen bij verzekerde
- Omzetverlies door cyberincident bij IT-provider

Gebruikelijke uitsluitingen in de polis:

- Uitval algemene infrastructuur (bv. stroom, internet, water)
- Traditionele fraude zonder inbreuk van een derde partij (interne fraude, identiteitsfraude, factuurfraude)
- Contractuele aansprakelijkheid
- Materiële en lichamelijke schade
- Lopende of gekende schades
- Oorlog en terrorisme vanuit en gericht aan landen in conflict



Tussenkomst aan de hand van actuele schadevoorbeelden

Ransomware-aanval bij een productiebedrijf met een omzetcijfer van €20.000.000

Door een phishingmail aan een werknemer krijgen hackers toegang tot het netwerk, ze versleutelen de systemen en vragen losgeld. Hierdoor is het IT-systeem niet toegankelijk en ligt de productielijn bijgevolg ook stil.

Mogelijke dekking in de polis:

- Hotline: verzekerde contacteert de 24/7 beschikbare incident response partner. Hierdoor wordt er kort op de bal gespeeld en wordt het incident meteen gecoördineerd en de nodige IT-experts ingeschakeld.
- Herstel: een gespecialiseerde IT-partner ontfermt zicht over de recuperatie en wederopbouw van data en netwerk.
- Losgeld: indien wederopbouw van IT-infrastructuur niet mogelijk is en/of kosten duurder uitvallen kan er overwogen worden om het losgeld uit te betalen om de systemen vrij te geven. De kosten van het losgeld en experten om te onderhandelen met hackers zijn gedekt.
- Forensische experts: een gespecialiseerd team onderzoekt wat de oorzaak was van het incident om hieruit de nodige lessen te trekken.
- Omzetverlies: verzekerde is enkele weken niet 100% operationeel, productiesystemen lagen ook stil. De vaste kosten blijven aanwezig. Het winstverlies wordt gedekt.

Mogelijke kosten:

- Hotline: kosten voor cyberincident manager €85.000
- Herstel van IT-omgeving: kosten voor ICT-consultants €375.000
- Losgeld: gevraagd losgeld in Bitcoins €1.000.000 (niet uitbetaald) en kosten voor onderhandelaar €5.500
- Forensische experts: professioneel onderzoek naar het in kaart brengen van incident €50.000
- Omzetverlies: verlies van winst door periode van inactiviteit €500.000
- Totale schadelast: €1.015.500

Data-lek bij een dienstverlenend bedrijf met een omzetcijfer van €100.000.000

Door een kwetsbaarheid in de systemen krijgen hackers toegang tot het netwerk. De hackers verwijderen een grote hoeveelheid aan medische data en andere gevoelige gegevens. Ze dreigen de data te verkopen wanneer er geen losgeld uitbetaald wordt.

Mogelijke dekking in de polis:

- Hotline: verzekerde contacteert de 24/7 beschikbare bijstand.
- Juridisch advies en verdedigingskosten: een juridische partner wordt aangesteld om de juiste stappen te nemen en de correcte partijen te informeren. Eventuele verdedigingskosten worden eveneens vergoed.
- Kennisgeving: kosten voor kennisgeving (melding van datalek) aan klanten/betrokken partijen wordt vergoed.
- Aansprakelijkheid: schadeclaims van derden t.g.v. van datalek en niet punitieve boetes (b.v. GDPR) worden vergoed.
- Forensische experts: een gespecialiseerd team onderzoekt welke data er concreet verloren is en achterhaalt de manier waarop hackers toegang kregen.

Mogelijke kosten:

- Hotline: kosten voor cyberincident manager €15.000
- Herstel van IT-omgeving: kosten voor ICT-consultants €75.000
- Juridisch advies en verdedigingskosten: kosten voor advocaten en consultants €75.500
- Kennisgeving: melding van datalek aan klanten/betrokken partijen €35.000
- Aansprakelijkheid: verweerkosten tegen aansprakelijkheidsclaims €5.000
- Losgeld: gevraagde losgeld in Bitcoins €350.000 (uitbetaald) en kosten voor onderhandelaar €5.000
- Forensische experts: professioneel onderzoek naar het in kaart brengen van incident €10.000
- Totale schadelast: €570.500

Verzekeringen zijn al meer dan 80 jaar onze expertise én onze passie. Met diepgaande kennis van uiteenlopende sectoren en hun specifieke risico's, bieden onze specialisten doordachte en op maat gemaakte verzekeringsoplossingen. Zo ondersteunen wij uw onderneming bij een veilige en zorgeloze groei, met de zekerheid van een betrokken en betrouwbare partner aan uw zijde.



Wenst u advies
of een kennismakend gesprek?

Neem vrijblijvend contact op met uw accountmanager of met onze expert Cyber, Robin Verlinden via **robin.verlinden@vandessel.be** of **03 482 15 30**.

Graag meer weten, scan deze QR code

Van Dessel
Insurance Brokers

Verzekeringskantoor Van Dessel NV
Misstraat 112, B-2590 Berlaar

+32 (0)3 482 15 30
info@vandessel.be

www.vandessel.be

Verzekeringsmakelaar erkend door FSMA met ondernemingsnummer 0446.433.491 - RPR Antwerpen, afdeling Mechelen
V.U.: Patrick Verlinden, Misstraat 112, B-2590 Berlaar - versie 06/2025