vanbreda
RISK & BENEFITS

Cyber survey 2017

Inhoudstafel

1. Inleiding

Er gaat geen dag voorbij of cybercrime beheerst het nieuws. Gevoelige privacygegevens die gelekt worden, hackers die een bedrijf afpersen of een phishing-mail die leidt tot het uitvallen van een bedrijfskritisch systeem: het is geen science fiction, maar realiteit.

Hoe beschermen Belgische bedrijven zich tegen de snel toenemende cyberrisico's? En hoe bereiden ze zich voor op de komst van de General Data Protection Regulation, de nieuwe Europese richtlijn over het beschermen van persoonsgegevens? Dat waren de belangrijkste vragen die we aan onze respondenten in het kader van dit cyberrisico rapport 2017 hebben voorgelegd.

Op de volgende bladzijden presenteren we u de resultaten van ons onderzoek, waaraan in totaal meer dan honderd bedrijven deelnamen. De resultaten zijn opvallend, maar voor ons als cyberexperts niet verrassend.

De rode draad doorheen dit onderzoek is dat Belgische bedrijven de gevaren van cybercrime onderschatten - ondanks dat 11% van hen toegeeft het voorbije jaar slachtoffer te zijn geweest. Het updaten van de beveiligingssoftware, zoals anti-virusprogramma's, gebeurt bij meer dan een derde van de respondenten niet dagelijks. Hiermee zetten ze de deur wagenwijd open voor hackers die (zelfs) met oudere technieken probleemloos kunnen toeslaan.

Ook de nieuwe Europese datawetgeving is zeker niet de grootste bezorgdheid van de bedrijven die deelnamen aan dit onderzoek. En dit ondanks het feit dat de niet-naleving ervan kan leiden tot monsterboetes die oplopen tot 20 miljoen euro of 4% van de totale jaaromzet.

Als sensibilisator rond de gevaren van cybercrime, kunnen wij niet voldoende benadrukken dat dringende actie noodzakelijk is. Alleen door het nemen van de juiste voorzorgsmaatregelen, kan een vuist worden gemaakt tegen de steeds professionelere manier waarop cyberbendes tewerk gaan.

Maar dit is slechts het begin. Want zelfs met de beste voorzorgsmaatregelen bent u nooit helemaal ingedekt tegen de toenemende risico's van cybercrime. Een goede verzekeringsoplossing vormt daarom het sluitstuk van een goed cyberveiligheidsbeleid.

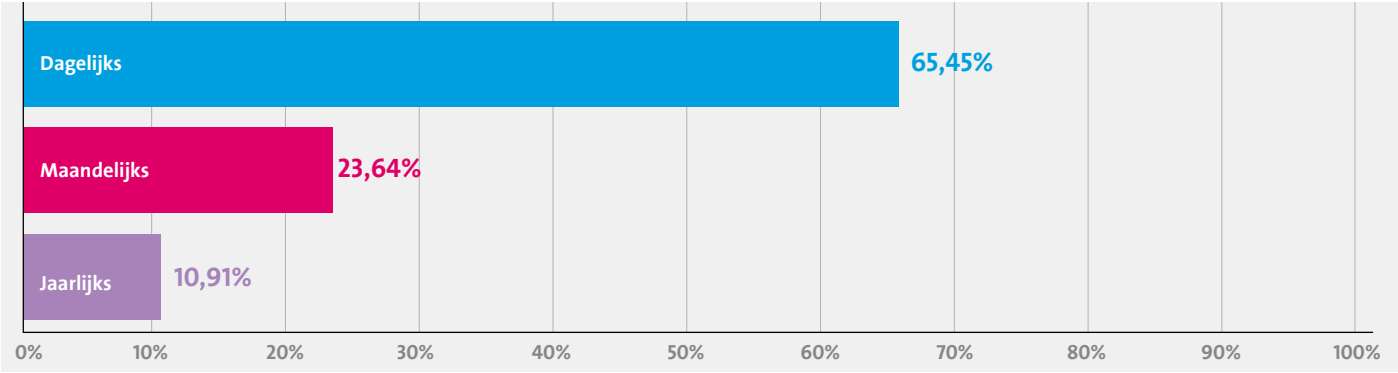
Tom Van Britsom
Cyberexpert Vanbreda Risk & Benefits

2. Onderzoeksresultaten

Het onderzoek spitst zich toe op 2 grote domeinen:

1. **Hoe beschermen Belgische bedrijven zich tegen cybercrime?**
2. **Hoe bereiden Belgische bedrijven zich voor op de komst van de nieuwe Europese privacywetgeving (GDPR), die op 25 mei 2018 in voege treedt?**

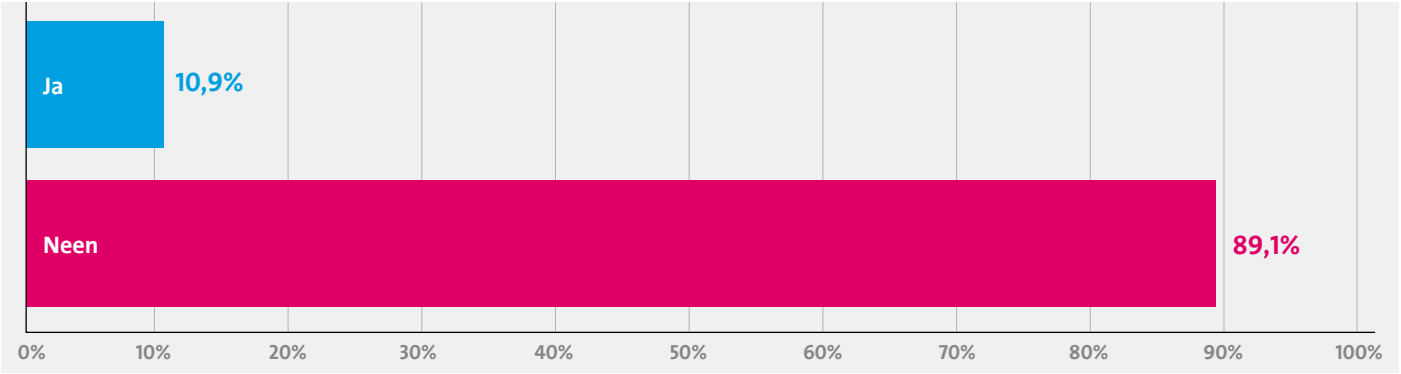
Hoe vaak worden beveiligingsproducten zoals anti-virusprogramma's bijgewerkt?



Het voortdurend bijwerken van beveiligingsproducten zoals anti-virusprogramma's is voor bedrijven cruciaal om zich te beschermen tegen de continue wijzigende aanvallen. Het is daarom opvallend dat 'slechts' 65,45% van de respondenten aangeeft dit dagelijks te doen. Dit betekent immers dat bijna een derde van hen dit ofwel maandelijks (23,64%) ofwel jaarlijks (10,91%) doet, wat volgens cyberexperts ruim onvoldoende is.

Het niet dagelijks bijwerken van beveiligingsprogramma's is een cruciale beveiligingsfout die aan de basis ligt van heel wat cyberonheil. De virussen (zoals cryptolockers of malware) waarmee cybercriminelen elke dag opnieuw grootscheepse aanvallen uitvoeren, worden dagelijks aangepast om antiviruspakketten te omzeilen. Deze nieuwe 'types' van virussen sluipen zo heel eenvoudig voorbij firewalls en andere beveiligingstoepassingen die niet dagelijks bijgewerkt worden.

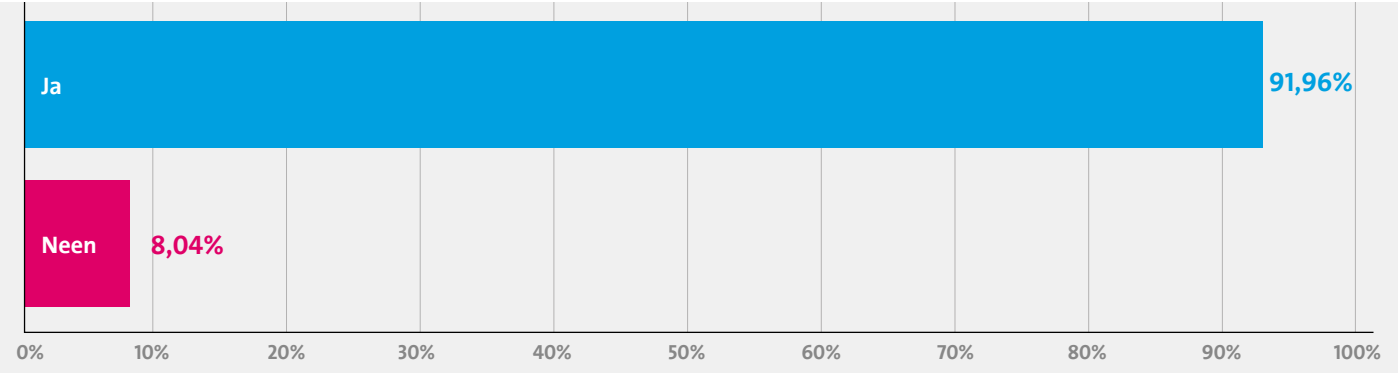
Bent u het afgelopen jaar getroffen door een vorm van cybercrime?



In onze Cyber survey 2017 vroegen we aan de deelnemers of zij het voorbije jaar het slachtoffer zijn geweest van cybercrime. Op die vraag antwoordde bijna 11% positief. Dit betekent dat één op de 10 ondervraagde bedrijven financiële schade heeft ondervonden als gevolg van cybercrime, wat het cyberrisico vandaag tot het meest waarschijnlijke bedrijfsrisico maakt.

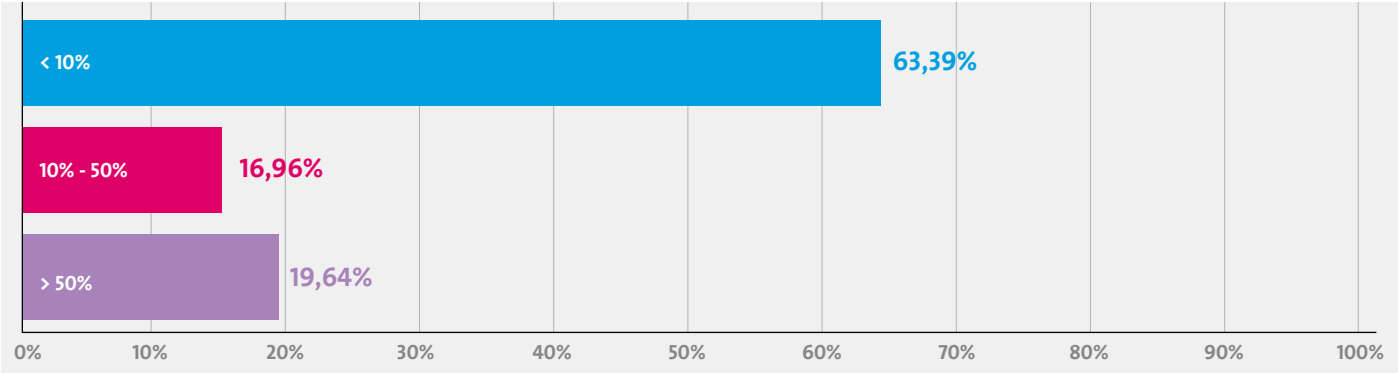
Van de bedrijven die getroffen werden, geeft de grote meerderheid aan dat het om een cryptolocker ging. Hierbij worden bepaalde bestanden of systemen van een bedrijf versleuteld, waarna de cybercrimineel losgeld vraagt in ruil voor het 'ontsleutelen'. Bij één van de respondenten werd het totale bedrijfssysteem gekraakt en bij nog een andere werd de bedrijfswebsite gehackt.

Beschikt u over back-up en recovery procedures voor kritische systemen, data en informatie?



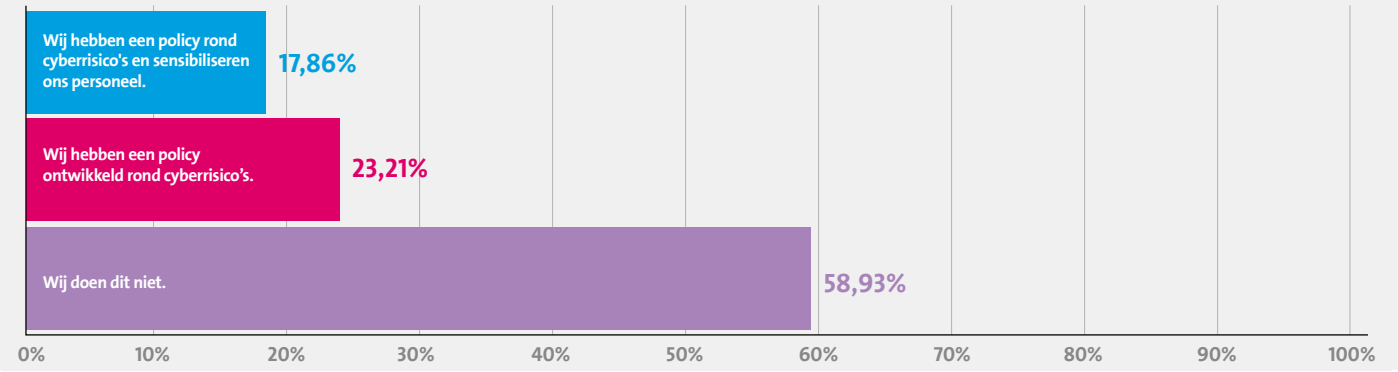
Meer dan 8% van de respondenten zegt niet over back-up en recovery procedures te beschikken voor kritische systemen, data en informatie. Hoewel dit een kleine minderheid is, blijft dit resultaat alarmerend. Het betekent immers dat een deel van de Belgische bedrijven na een cyberaanval alle gegevens voorgoed kwijt kan zijn: klantgegevens, boekhoudgegevens, gegevens die cruciaal zijn om bedrijfskritische processen uit te voeren, …. De impact hiervan voor het bedrijf in kwestie kan moeilijk overschat worden.

Hoeveel procent van uw data zit in de cloud?



Bijna een vijfde van de respondenten bewaart meer dan 50% van hun data in de cloud. Nog eens 17% van hen bewaart tussen de 10% en de 50% van hun data in de cloud. Dit vormt op zich geen groter veiligheidsrisico, maar vraagt wel voor een andere risicoanalyse. Door het online karakter van de cloud zijn er bijkomende risico's die afgedekt moeten worden. Zelfs wanneer hackers een datacenter viseren en gevoelige informatie te grabbel gooien, blijft de onderneming die klant is immers aansprakelijk. Informeer je daarom goed bij je service provider, lees je contracten goed na en voorkom een 'vals gevoel van veiligheid'.

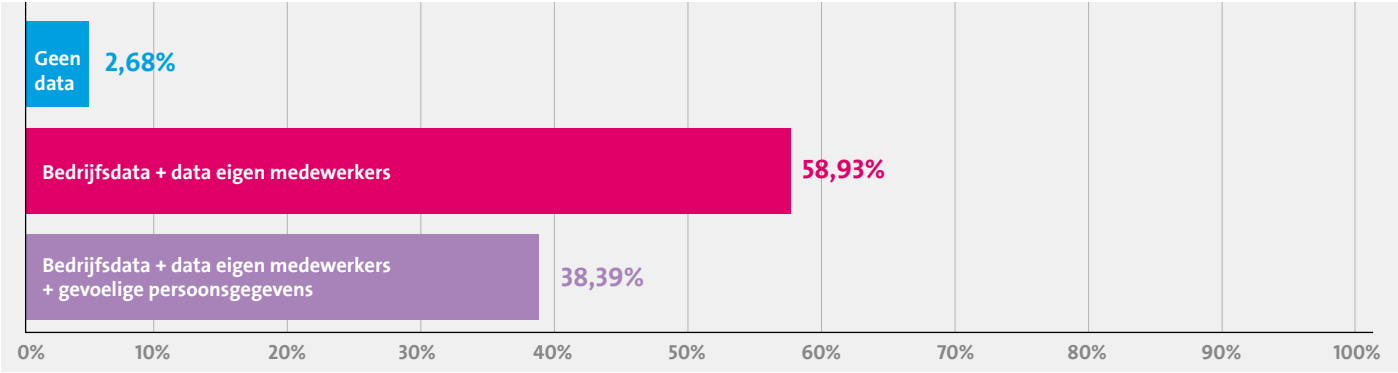
Hoe verhoogt u het bewustzijn van uw medewerkers rond cyberrisico's?



Cybercriminelen vallen bedrijven aan via het IT-netwerk, maar uit verschillende onderzoeken blijkt dat 'de mens' nog steeds de zwakke schakel is. Bij phishing is het vaak een van de medewerkers die een malafide mail opent en zo de IT-infrastructuur van zijn werkgever blootstelt aan virussen. Ook bij een datalek is het meer dan eens een van de medewerkers die – vaak onopzettelijk – onnauwkeurig omgaat met een bepaald bestand en zo een grote hoeveelheid gevoelige gegevens openbaar maakt.

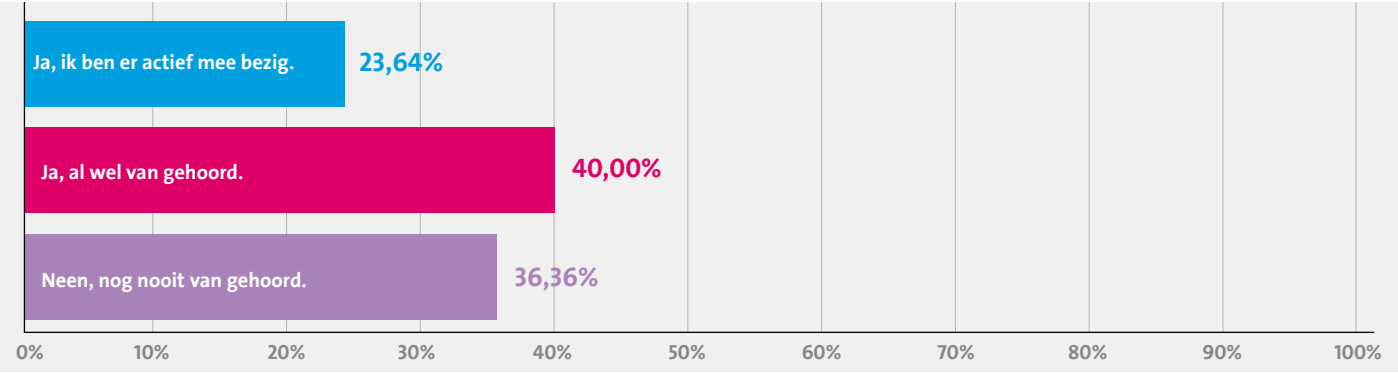
Het is daarom des te opvallender dat bijna 59% van de bedrijven in ons onderzoek aangeeft niet bezig te zijn met de verhoging van het bewustzijn van hun medewerkers rond cyberrisico's. Net zoals het ontbreken van dagelijkse updates van de beveiligingssoftware, vormt dit een ernstig veiligheidsrisico voor de betrokken bedrijven.

Over welk type data beschikt uw bedrijf?



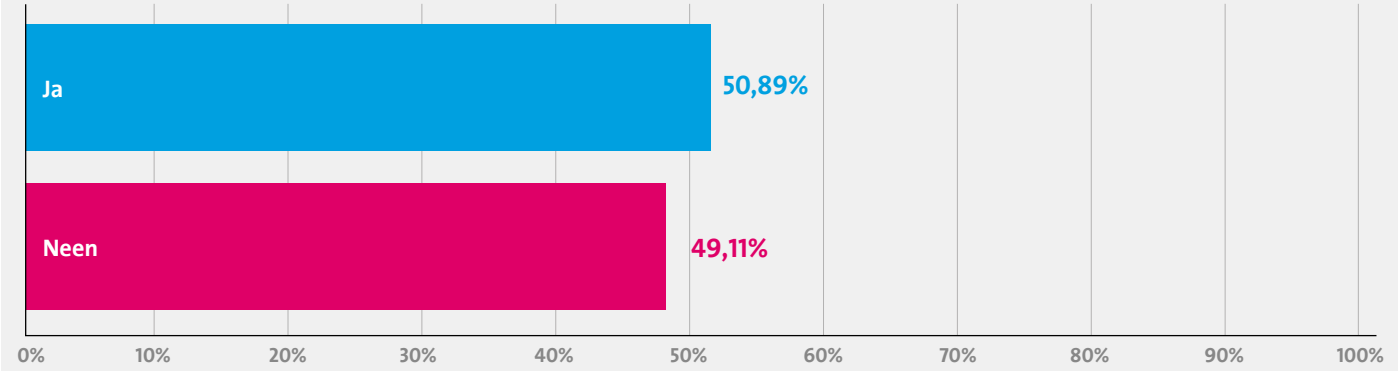
Van de ondervraagde bedrijven zegt bijna 39% over gevoelige persoonsdata te beschikken en zo goed als alle bedrijven beschikken ook over gegevens van de eigen medewerkers. Ondernemingen die persoonsgegevens verzamelen (zo goed als alle bedrijven dus), moeten vanaf 25 mei 2018 voldoen aan een nieuwe set regels die omschreven staan in de General Data Protection Regulation (GDPR).

Bent u op de hoogte van de General Data Protection Regulation (GDPR)?



Hoewel heel veel bedrijven over persoonsgebonden gegevens beschikken, zijn weinigen van hen al actief bezig met de nieuwe Europese privacywetgeving. Slechts 23,64% geeft aan dat ze actief stappen ondernemen om hun bedrijf in regel te brengen met de GDPR-wetgeving. Dit betekent dat meer dan 75% van hen dit niét doet, hoewel deze binnen een jaar voor alle Belgische bedrijven geldt. Dat 36,36% van de ondervraagde bedrijven zegt nog nooit gehoord te hebben van de GDPR, is in dit kader helemaal ontluisterend.

Hebt u een verantwoordelijke voor veiligheid en privacy?



De GDPR maakt het voor heel wat bedrijven (waaronder overheidsbedrijven of organisaties die strafrechtelijke data verwerken) verplicht om een Data Protection Officer aan te stellen. Deze moet erover waken dat het bedrijf in kwestie de data volgens de regels van de GDPR bewaart en verwerkt.

Om echter in regel te zijn met de nieuwe wetgeving, heeft elk bedrijf er belang bij om iemand aan te stellen die verantwoordelijk is voor veiligheid en iemand voor privacy. Deze medewerkers staan er immers voor garant dat het bedrijf de noodzakelijke stappen neemt om zich te beschermen tegen cybercrime, om datalekken te voorkomen en om – indien bepaalde gegevens toch openbaar zijn gemaakt – een eventueel lek meteen te melden aan de privacycommissie.

Opvallend is het daarom dat ongeveer de helft van de ondervraagden aangeeft niet over iemand te beschikken die zich bezighoudt met de verantwoordelijkheden op het vlak van veiligheid en privacy. Dit vormt opnieuw een ernstig veiligheidsrisico voor de organisaties in kwestie.

3. Conclusie: de GDPR als accelerator voor cyberveiligheid?

Zijn de Belgische bedrijven voldoende beschermd tegen cybercrime? En zijn ze voorbereid op de komst van de nieuwe Europese datawetgeving? Op basis van de resultaten uit deze survey, moeten we hierop genuanceerd antwoorden.

Een deel van de respondenten beseft vandaag duidelijk al welke gevolgen onvoldoende bescherming tegen cyberrisico's kan hebben. Ze werken dagelijks hun anti-virusprogramma's bij (65%), ze sensibiliseren hun personeel over de nieuwe cybergevaren (17,86%) en ze zijn actief bezig met de implementatie van processen in het kader van de Europese GDPR-wetgeving (23,64%).

Een ander deel echter, onderschat de gevaren sterk. Dat 11% van de bedrijven aangeeft het voorbije jaar slachtoffer te zijn geweest van cybercrime, bewijst dat het risico imminent is. Het feit dat 58,93% van de ondervraagde bedrijven z'n personeelsleden niet sensibiliseert rond de toenemende cyberdreigingen en dat 36,36% nog nooit van de GDPR-wetgeving heeft gehoord, geeft in dit opzicht op z'n minst te denken.

Als cyberexperts hopen we dat de nieuwe Europese datawetgeving kan gelden als een accelerator om Belgische bedrijven meer bewust te maken rond cyberrisico's en datalekken. Het kan vandaag niet meer zo zijn dat organisaties denken ongenaakbaar te zijn voor cybercriminelen. Daarvoor is het aantal cases van cryptolockers, data breaches en hackings te groot. Er is daarom meer dan ooit nood aan iemand die binnen zijn of haar bedrijf verantwoordelijk is voor veiligheid en privacy – ook indien het bedrijf in kwestie hiertoe niet wettelijk verplicht is. En niet alleen de bedrijfsleider, maar ook de medewerkers dragen in dit alles een grote verantwoordelijkheid.

Maar zoals in de inleiding reeds gezegd, zijn zelfs de beste voorzorgsmaatregelen niet voldoende voor een onderneming om zich 100% in te dekken tegen cybercrime. Ook bedrijven die dagelijks hun anti-virusprogramma's updaten, zijn de voorbije jaren ten prooi gevallen aan internetcriminelen. Een goede verzekering is de enige écht waterdichte garantie tegen financieel verlies als gevolg van een cyberaanval.

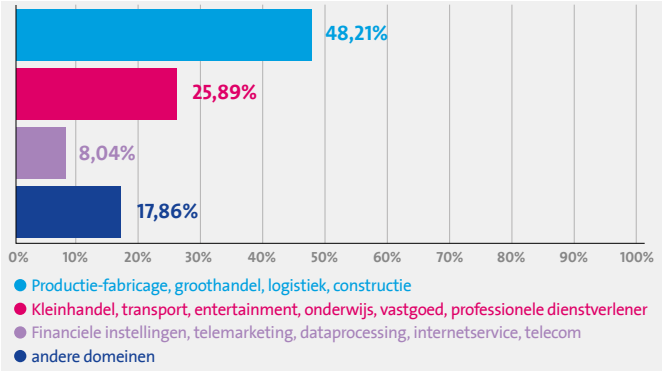
In het kader van de GDPR kan zo'n cyberverzekering bovendien ook redding brengen. De nieuwe Europese datarichtlijn legt monsterboetes op aan bedrijven die inbreuken doen op de GDPR-wetgeving. Aangezien het gaat over administratieve boetes, en niet over strafrechtelijke boetes, zijn deze boetes verzekerbaar via een cyberpolis. Dit is zonder meer goed nieuws voor bedrijven die zich honderd procent willen indekken tegen deze nieuwe risico's. Maar dit mag hen er uiteraard niet van weerhouden om zelf de nodige cruciale stappen te zetten om elk risico tot een minimum te herleiden.

4. Over het onderzoek

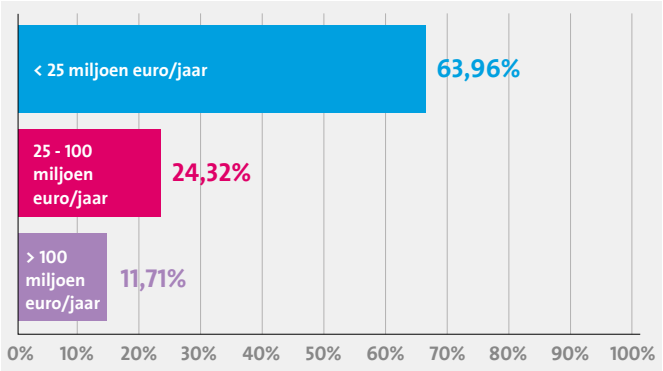
Aan het onderzoek van Vanbreda Risk & Benefits namen 110 Belgische bedrijven deel. Ze kregen een korte enquête voorgeschoteld waarin gepolst werd naar hun acties met betrekking tot cyberveiligheid en het in regel brengen van hun bedrijf met de Europese datawetgeving GDPR.

Onderstaande grafieken geven meer informatie over het profiel van onze respondenten.

In welk domein bent u actief?



Wat is uw omzet?



5. 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 als eServices 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.

cybersecure@vanbreda.be
T. + 32 3 292 00 13
www.vanbreda.be

Contactinfo
Vanbreda Risk & Benefits

Plantin en Moretuslei 297
2140 Antwerpen

cybersecure@vanbreda.be
T. + 32 3 292 00 13

www.vanbreda.be