Zicht risico- en verzekeringsadviseurs

Staat u wel eens stil bij de datarisico's die u loopt?

VERZEKERING • BEDRIJFSRISICO • HYPOTHEEK • PENSIOEN

gelukkig geregeld!

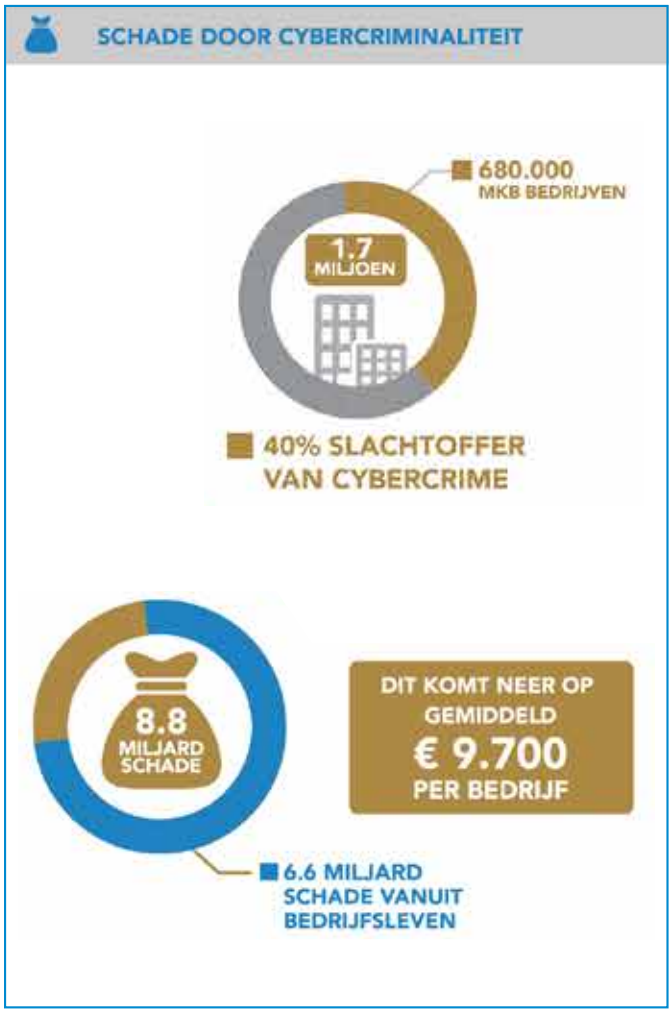
Kinderen van een jaar weten tegenwoordig al de weg op een tablet. De computer en het internet zijn niet meer weg te denken uit het hedendaagse leven. Bijna elk bedrijf werkt wel met een computer of laptop en smartphone die ook buiten kantoor gebruikt kunnen worden. En steeds vaker worden gegevens via internet (de cloud) opgeslagen. Ook zijn websites niet meer weg te denken als middel om te bestellen, betalen, gegevens te registreren en te wijzigen. De razendsnelle ontwikkeling van de computertechnologie heeft veel voordelen, maar kent ook een groot nadeel. Cyber- en datarisio's zoals cybercriminaliteit! Houdt uw onderneming rekening met deze risico's? Kan uw onderneming blijven draaien op het moment dat de ICT-omgeving niet meer functioneert vanwege een cyberaanval? Kan een datalek een faillissement van uw onderneming betekenen?

Criminaliteit

Cybercriminaliteit en datalekken zijn een vorm van criminaliteit met ICT als middel. Maar ook als doelwit. U kunt hier ook slachtoffer van worden als u geen computer of internetaansluiting heeft. Het kan bijvoorbeeld ook via de computerchips die in de meeste telefoons en bankpassen zitten of een USB-stick die u verliest. Maar ook bedrijfssystemen, moderne auto's en chipkaarten zijn vatbaar voor cybercriminaliteit. Cybercriminaliteit is strafbaar en wordt aangepakt door de politie en het Openbaar Ministerie.

Wist u dat

- *de schade door cybercriminaliteit jaarlijks 8,8 mld in Nederland is?*
- *90% van de bedrijven al is gehackt (maar weet dit vaak nog niet)?*
- *80% van de Android-toestellen besmet is?*
- *de zwakste schakel in de beveiliging de mens is?*
- *het oplossen van een hack weken kan kosten?*
- *iemand met zijn gegevens in honderden tot duizenden bestanden staan, zowel van bedrijven als de overheid?*

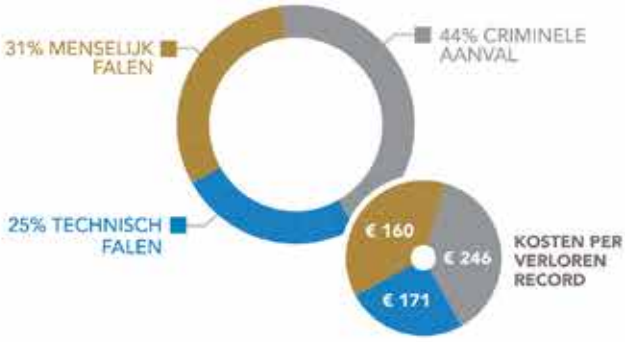


De risico's

Bij een cyberaanval loopt u verschillende risico's:

De oorzaken

Veel mensen denken dat door een goede ICT-beveiliging de kans op een cyberaanval minimaal is. In de praktijk blijkt alleen dat het falen van een IT-systeem het minst vaak de daadwerkelijke oorzaak is van een inbreuk op data. De drie voornaamste redenen waarop cyberrisico's ontstaan zijn:



Het niet goed beheren of beveiligen van ICT-infrastructuur of verlies van informatie en informatiedragers (zoals laptops, mobiele telefoons)

ICT-storingen en uitval van uw netwerk

Zoals hacken, phishing, malware en identiteitsfraude

Datalek

Slechte beveiliging kan leiden tot een datalek en dat kan weer misbruik van de gelekte gegevens tot gevolg hebben. We spreken van een datalek als er een inbreuk is op de beveiliging zoals bedoeld in artikel 13 van de Wet bescherming Persoonsgegevens. Met andere woorden: het gaat om de toegang tot persoonsgegevens of vernietiging, wijziging of vrijkomen van gegevens, zonder dat dat de bedoeling is van de betreffende organisatie. Het gaat dus niet alleen over het vrijkomen (lekken) van de gegevens, maar ook om de onrechtmatige verwerking van de gegevens.

Een voorbeeld

Een webshop wordt gehackt waardoor de website plat gaat. De gegevens van de klanten die een order hebben geplaatst zijn beschadigd. Hierdoor kan de webshop de bestellingen niet op de juiste manier afhandelen. De kosten voor het forensisch onderzoek en het herstel van de data zijn € 8.000,-. Omdat de website 14 dagen niet bereikbaar was, is de omzetverlies vastgesteld op € 45.000,-. De totale schade bedraagt dus € 53.000,-.

Meldplicht datalekken

De eerste kamer heeft op 26 mei 2015 een wetsvoorstel aangenomen dat een meldplicht datalekken regelt. Dit houdt in dat bedrijven en overheden vanaf 1 januari 2016 direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP), zodra zij een datalek met ogenschijnlijk ernstige gevolgen voor de bescherming van de persoonsgegevens hebben.
Als de datalek mogelijk schadelijk is voor de persoonlijke levenssfeer van de betrokkenen, dan moeten zij ook op de hoogte gebracht worden.
Als u dit niet of niet tijdig doet, riskeert u een boete van maximaal € 820.000,- of 10% van de omzet over het voorafgaande jaar. Met deze meldplicht wil de overheid de persoonsgegevens nog beter beschermen.

Tip:
Krijgt u een melding dat u een openstaande rekening of boete moet betalen om weer bij uw bestanden te kunnen? Niet doen! Het is namelijk helemaal niet zeker dat u na betaling weer overal toegang tot heeft. Bovendien beloont u daarmee de criminelen en wordt het probleem in de toekomst alleen maar erger.

Ons advies

Maak een risicoanalyse: Zicht op uw datarisico's.
Maak, in samenwerking met een ervaren online beveiligingsspecialist, een risicoanalyse:

- Welke onderdelen van uw bedrijfsvoering vormen een potentieel risico op ICT-gebied? Denk aan desktops, laptops, smartphones en tablets, e-mail, internettoegang en databases.
- Waar 'staat' de belangrijkste bedrijfsinformatie? Is deze informatie goed beveiligd? Laat de huidige beveiliging testen door een specialist.
- Welke software kan de risicovolle onderdelen optimaal beveiligen? Kijk, in plaats van alleen 'losse' producten, ook naar geïntegreerde oplossingen. Die zijn vaak voordeliger, overzichtelijker en veiliger. Vraag offertes aan en nodig de beste drie uit voor een demonstratie.
- Zijn uw medewerkers op de hoogte van de risico's van cybercriminaliteit en datalekken? Stimuleert u bijvoorbeeld het gebruik van sterke wachtwoorden?

Stap 1: Kies de juiste beveiliging

Kies voor een beveiligingsproduct dat goed bij uw bedrijf past én overzichtelijke en begrijpelijke rapportages geeft. Vergelijk verschillende producten en betrek een specialist bij uw uiteindelijke keuze. Evalueer regelmatig de gekozen beveiligingsoplossing; past die nog wel bij uw huidige én de toekomstige situatie?

Tip:
Via beschermjebedrijf.nl heeft u binnen enkele minuten inzicht hoe het zit met de beveiliging van uw informatie.

Stap 2: Geef uw medewerkers voorlichting

- Licht uw medewerkers in over potentiële risico's van bijvoorbeeld (eigen) laptops, smartphones en tablets die ze voor het werk gebruiken.
- Overweeg de aanschaf van een beveiligingsproduct voor mobiele apparaten waarmee bijvoorbeeld een verloren of gestolen laptop of smartphone op afstand buiten werking gesteld kan worden.
- Maak medewerkers duidelijk dat het 'zomaar' klikken op links in e-mails risicovol is. Bespreek de gevaren van bijvoorbeeld social engineering, waarbij de hacker de mens benadert om vertrouwelijke of geheime informatie los te krijgen.
- Zorg dat uw medewerkers regelmatig hun wachtwoorden wijzigen en stimuleer het gebruik van sterke wachtwoorden.
- Zorg voor een helder internet- en e-mailbeleid.

Tip:
U kunt uw bedrijf door uw eigen ICT-leverancier laten screenen, maar u kunt ook een risicoanalyse door ESET laten uitvoeren of het Hiscox selfassessment doen.
De adviseurs van Zicht leggen u graag uit wat de mogelijkheden zijn.

Stap 3: Sluit een passende cyber- en datarisicoverzekering af

Snel en doelgericht reageren op dataverlies, hackers of cyberaanvallen beperkt de schade. Een cyber- en datarisicoverzekering helpt u met de inzet van ervaren security-professionals, met wereldwijd bereik en met uitgebreide juridische kennis van gespecialiseerde advocaten. Als u een inbreuk meldt, staat er een team van ervaren professionals voor u klaar.
Zij helpen u databases en websites te repareren, belanghebbenden te informeren en het juridische traject op te starten. En uw eigen kosten? Die zijn gedekt.

Met een cyber- en datarisicoverzekering bent u verzekerd van de volgende dekkingen:

Systeeminbraak

De financiële gevolgen van inbreuk op uw systemen of (elektronische) data:

- Kosten van forensisch onderzoek
- Kosten van communicatie met providers, klanten, toezichthouders, justitie, creditmaatschappijen en andere belanghebbenden
- Kosten voor extra klantenondersteuning, bijvoorbeeld via een call center
- Kosten van crisismanagement, reputatieherstel en PR-campagnes

Privacy

De gevolgen van gestolen privacygevoelige gegevens:

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

Digitale aansprakelijkheid

Schade die ontstaat als uw website of e-mail onbedoeld het auteursrecht schendt, laster verspreidt of een virus bevat.

Hacking

Schade veroorzaakt door hackers:

- Reparatie, vervanging of herstel van websites, programma's of data
- Kosten van gestolen software of data
- Kosten van onderzoek en advies in systeembeveiliging
- Kosten van forensisch onderzoek naar de identiteit van de hacker
- Kosten van PR-advies voor reputatiebescherming

Afpersing

De schade door hackers die uw website of data gijzelen. U krijgt bijstand van een security-adviesbureau en eventueel betaald losgeld wordt vergoed.

Omzetverlies door cyberaanvallen

Omzetverlies in uw online verkoop, ontstaan door een DDoS-actie of andere aanval op de computersystemen van uw webwinkel.

Wilt u een cyber- en datarisicoverzekering afsluiten? Kijk dan op zichtadviseurs.nl/cybercrime

Kijk op zichtadviseurs.nl/cybercrime voor meer uitleg over de vormen van cybercriminaliteit, een checklist, de cyberrisicoverzekering en contact met onze adviseurs.

Zicht risico- en verzekeringsadviseurs

Over Zicht

Wij helpen u bij het maken van bewuste keuzes over financiële risico's. Bijvoorbeeld door samen goed vooruit te kijken. En door uw wensen en situatie in kaart te brengen. Maar ook door na te denken over verschillende oplossingen.

Dit doen we met persoonlijk advies en financiële producten die aansluiten bij de fase van uw (zakelijk) leven. Daardoor kunt u zich richten op de dingen waar het in uw leven écht om draait. **Dat is gelukkig geregeld!**

Zicht heeft meer dan 100 jaar ervaring met onafhankelijke advisering van bedrijven en particulieren. Vandaag de dag zijn we één van de toonaangevende adviesbedrijven van Nederland en onderdeel van NN Group. Vanuit 20 vestigingen adviseren onze 500 deskundige medewerkers u graag.

Z.DCR.0416