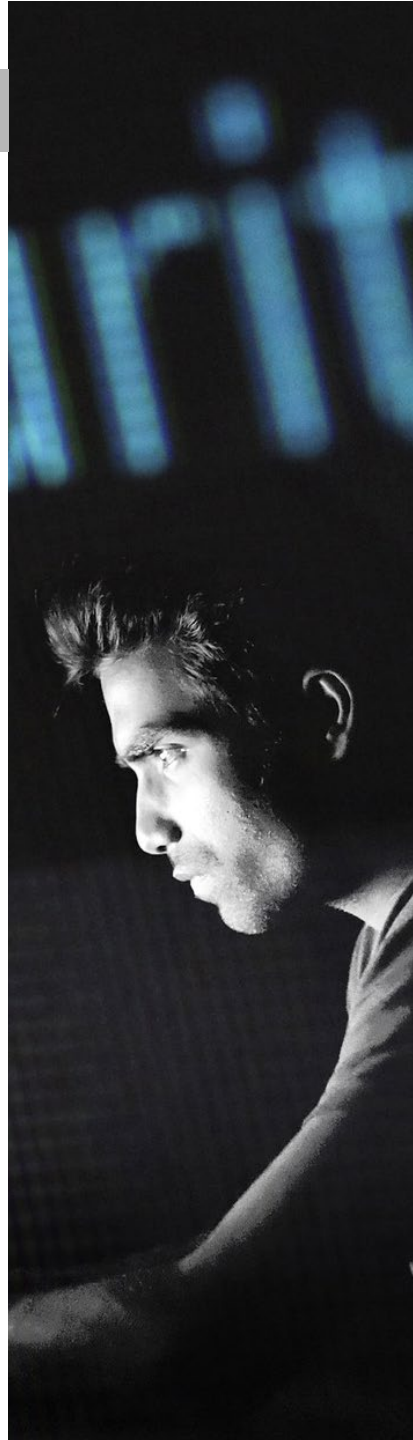
Cyber en Data Risks

DE REGT ADVIESGROEP

1. Inhoudsopgave



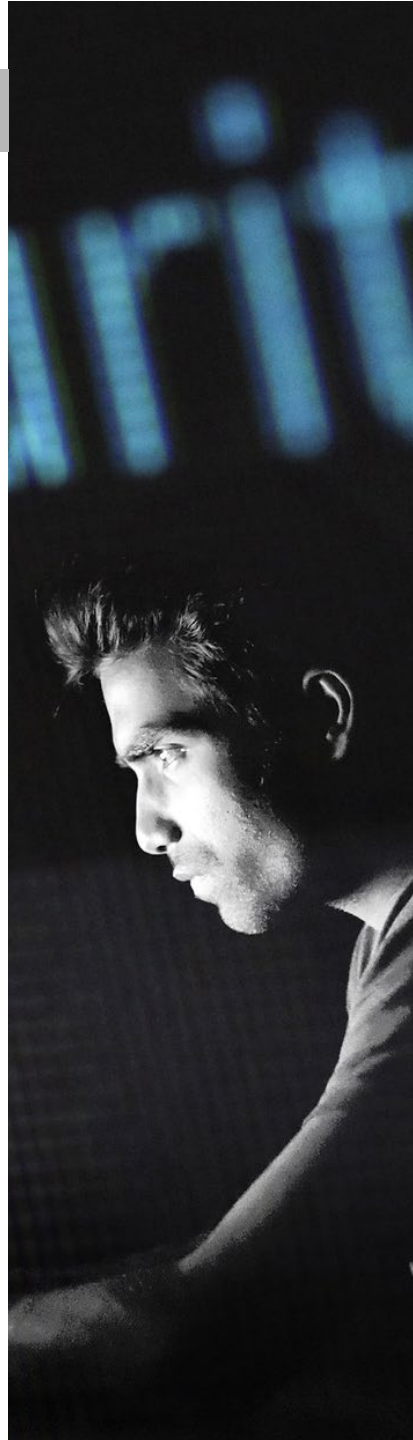
2. U wilt weten ‘waarom?’

“Het overkomt mij toch niet!”, is een veelvoorkomende uitspraak in de markt. Helaas is de realiteit dat het iedereen kan overkomen! 98% van alle bedrijven zijn het slachtoffer van een datahack of een poging daar toe. De Norton Symantec Security Survey toont aan dat:

- ✓ 29% op frequente basis onderhevig zijn aan een cyber aanval;
- ✓ 24% van de bedrijven schade en dataverlies oplopen;
- ✓ 20% van de aangevallen bedrijven hierna een inkomsten- of reputatieverlies ondervindt.

Waarom is het MKB juist een aantrekkelijke prooi voor cybercriminelen?

- ✓ Er valt bij het MKB meer te halen dan bij de gemiddelde consument, en de meeste ondernemers hebben hun cybersecurity niet beter geregeld dan de gemiddelde consument.
- ✓ Wanneer een kleinere organisatie bestolen of gehackt wordt, haalt dit niet vaak het nieuws, waardoor hackers rustig verder kunnen gaan zonder al te veel media-aandacht.



3. Belangrijkste redenen om een cyber- en datarisks verzekering af te sluiten

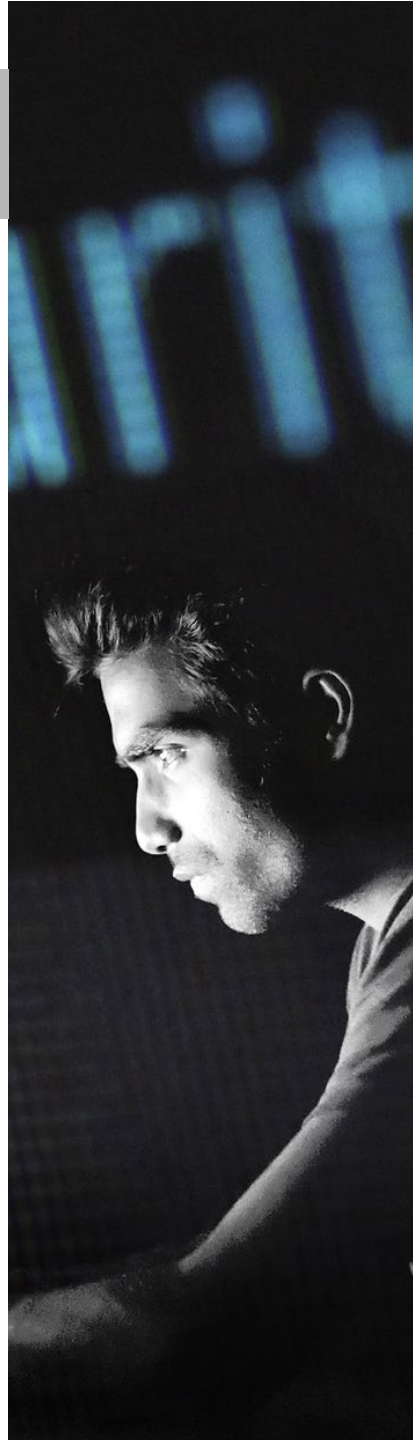
De vier belangrijkste redenen om een Cyber en Data Risks verzekering af te sluiten:

1. Cybercrime

Cybercrime is de snelst groeiende vorm van misdaad van de laatste jaren. Omdat ons leven zich meer en meer digitaal afspeelt, neemt ook de kans op online criminaliteit toe. Verlies van data en hacking zijn een paar voorbeelden en deze risico's zijn niet of maar voor een deel gedekt onder traditionele verzekeringen. De Cyber en Data Risks verzekering van Turien & Co. biedt wel een uitgebreide dekking tegen deze risico's.

2. Afhankelijkheid van systemen

Systemen zijn cruciaal voor het bedienen van klanten, maar hun downtime is niet gedekt door de standaard verzekeringen. Alle bedrijven vertrouwen op systemen om hun core business te kunnen verrichten. Een hackaanval, computervirus of (kwaadaardige) handeling van een werknemer kan voor onderbreking van business zorgen. Online en/of offline omzetderving wordt door de Cyber en Data Risks verzekering van Turien & Co. vergoed.



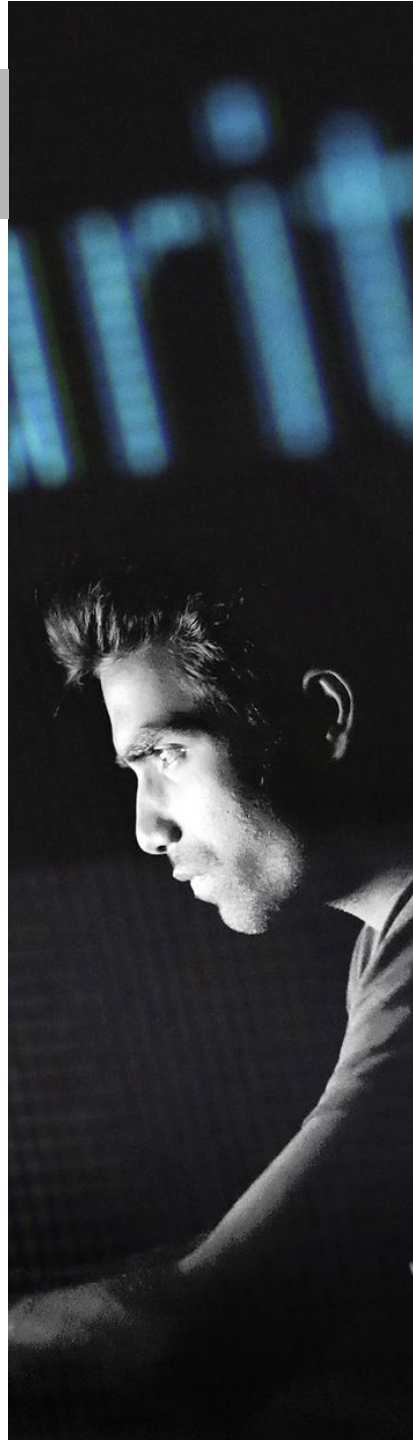
3. Belangrijkste redenen om een cyber- en datarisks verzekering af te sluiten

3. Draagbare apparaten

De komst van draagbare apparaten en de mogelijkheid om thuis te werken heeft het leven een stuk makkelijker gemaakt voor velen van ons. Echter, deze nieuwe manier van werken betekent ook dat belangrijke en vertrouwelijke gegevens kunnen worden gestolen of gemakkelijker verloren worden. Een laptop achtergelaten in een trein, een gestolen iPad in een restaurant of een verloren USB-stick zijn allemaal goede voorbeelden. Bovendien zijn de apparaten zelf het doelwit met een groeiend aantal virussen. De Cyber en Data Risks verzekering dekt de kosten die gepaard gaan met een data-inbreuk via draagbare apparaten.

4. Data zijn waardevol

We hebben meer data dan ooit tevoren en vaak zijn deze gegevens van onze klanten en leveranciers. Non-disclosure overeenkomsten en commerciële contracten, garanties en vrijwaringen besteden steeds meer aandacht aan beveiliging van data. Gegevens van derden zijn waardevol. U kunt aansprakelijk worden gesteld als u deze gegevens verliest ongeacht de oorzaak. Met de juiste Cyber en Data Risks verzekering worden de eigen kosten en de schade van derden als gevolg van verlies van data en/of inbreuk op privacy vergoed.



4. Niet goed gedekt binnen traditionele verzekeringen

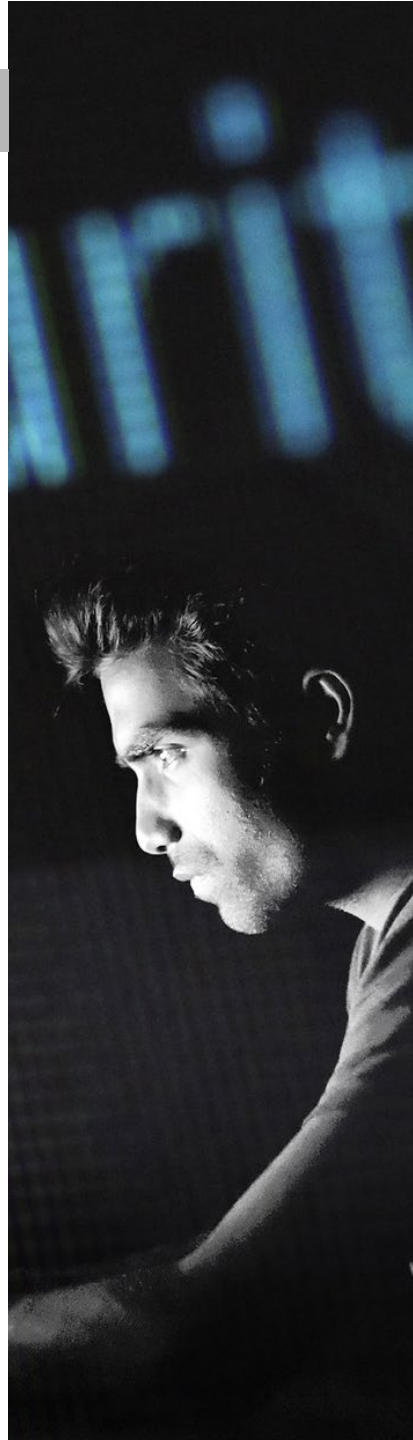
Verhouding tot traditionele verzekeringen

De indruk bestaat dat sommige cyberrisico's al gedekt zijn op enkele traditionele verzekeringen. Zo kan een bestaande bedrijfsschadeverzekering een deel van de gevolgschade dekken die door een cyberincident ontstaat.

Brand- en technische verzekeringen

De belangrijkste bestaande verzekeringen die dit al dekken, zijn de brand- en technische verzekeringen (machinebreuk/computer), de aansprakelijkheidsverzekering en de fraudeverzekering.

Brand- en technische verzekeringen in de zakelijke markt bieden ofwel een allrisk dekking ofwel een dekking waarbij alleen specifieke schadeoorzaken verzekerd zijn. De allrisk dekkingen komen veel voor in de grootzakelijke markt, de specifieke oorzaken variant komt veel voor in de MKB-markt. In beide gevallen zal de overlap met de Cyber en Data Risks verzekering doorgaans klein zijn. Bij een allrisk dekking is in principe alle materiële schade gedekt. In het geval dat een cyberincident dus ook materiële schade tot gevolg heeft, dan kan voor die materiële schade dekking worden gevonden bij de brandverzekering. Denk bijvoorbeeld aan de hacker die via een computerverbinding een lopende band of machine hackt, waardoor deze in elkaar draait. Verzekeraars beschouwen schade aan data echter zelden als materiële schade. Voor de schade aan data is dan ook een Cyber en Data Risks verzekering van belang. Bij een verzekering die alleen specifieke schadeoorzaken verzekert, wordt tot op heden cyberschade zelden meeverzekerd. De overlap is daarom in beide dekkingsvarianten minimaal.



5. Meldplicht datalekken

Bent u al geïnformeerd over de Meldplicht datalekken? Deze nieuwe wet zegt in vogelvlucht:

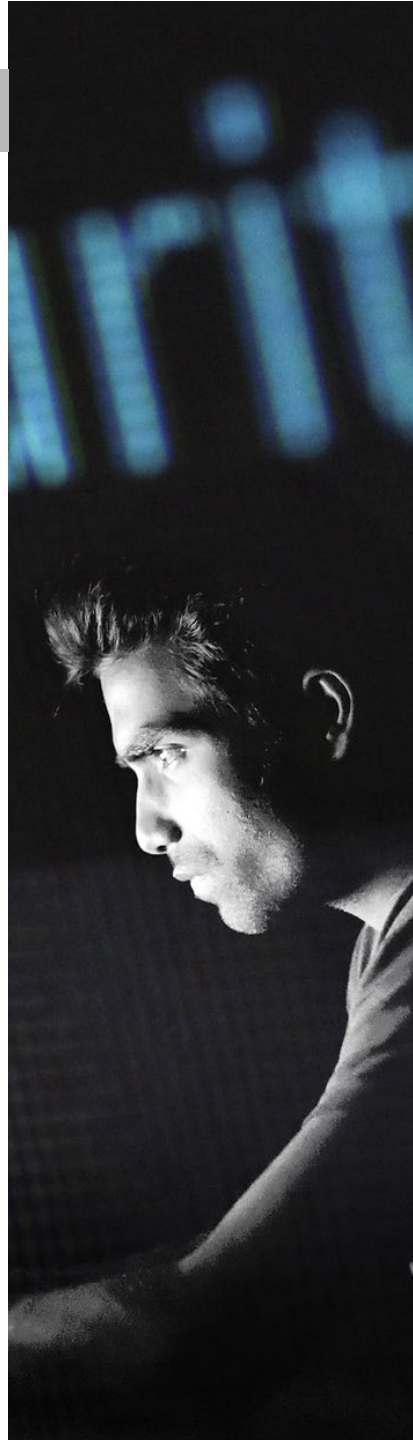
- ✓ Boete van maximaal €820.000 of 10% van de jaaromzet; *
- ✓ Voor commerciële instellingen en (semi-) overheid;
- ✓ Binnen 48 uur melden bij falen van technische en organisatorische beveiliging met kans op verlies of onrechtmatige verwerking van persoonsgegevens;
- ✓ Inspanningen om de schade te herstellen;
- ✓ Raadgevingen aan publiek en klanten.

** Let op: vanaf 25 mei 2018 kunnen onder de privacyverordening (AVG) boetes worden opgelegd tot € 20 miljoen (of 4% van de wereldwijde jaaromzet, als dat hoger is).*

Hier vindt u de Beleidsregels Meldplicht Datalekken

Hoe kunt u bepalen of er een datalek is?

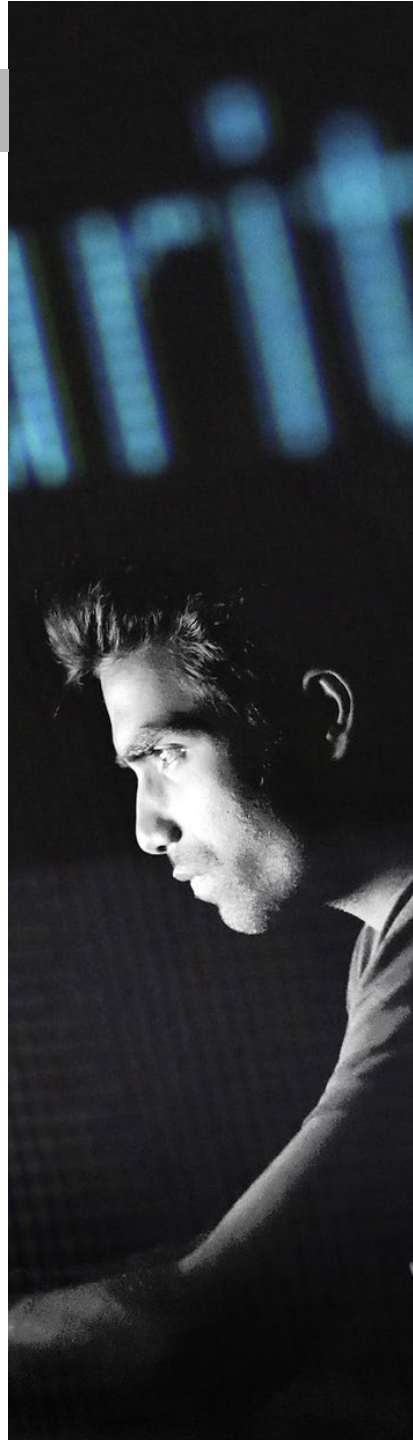
Kennedy Van der Laan heeft hiervoor een Datalek Quickscan ontwikkeld. Deze scan helpt om na te gaan of er sprake is van een datalek en zo ja, wat u moet doen om er zeker van te zijn dat u tijdig de juiste acties onderneemt richting de Autoriteit Persoonsgegevens en de betrokkenen. Een mooie kosteloze tool om aan uw favorieten toe te voegen!



6. De risico’s

Waar moet u zoal aan denken bij cyberrisico’s voor uw onderneming? Onderstaand de meest voorkomende risico’s in het MKB:

- ✓ Gehackte telefooncentrale;
- ✓ Phishing e-mails;
- ✓ Politievirus / Locky ransomware;
- ✓ DDOS- aanval;
- ✓ Kwijtraken laptop of USB-stick;
- ✓ Datadiefstal.

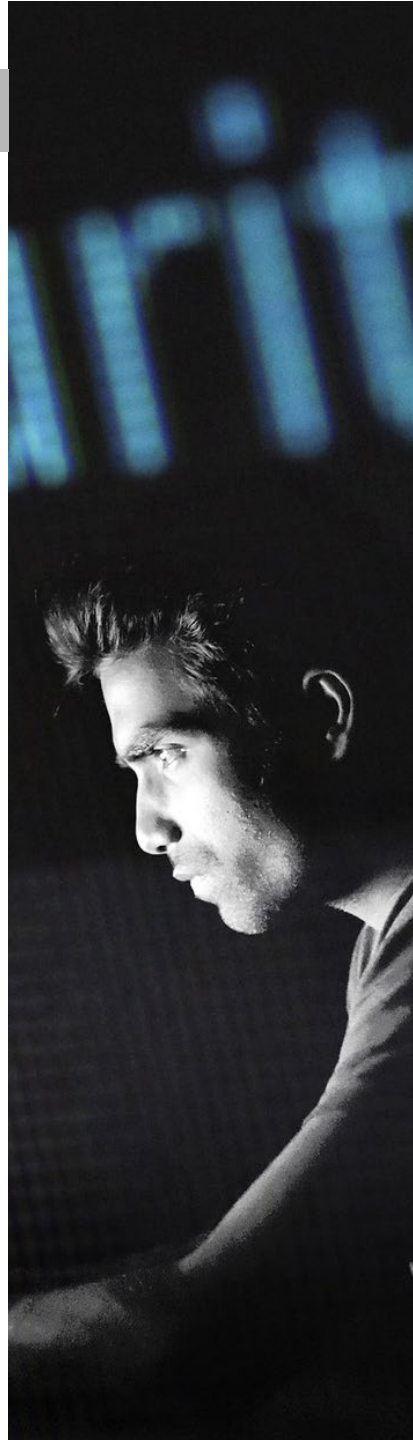


7. Welke gegevens zijn blootgesteld aan risico's?

- ✓ Persoonsgegevens;
- ✓ Beschermde (gezondheid/zorg) gegevens;
- ✓ Betaalkaart gegevens.

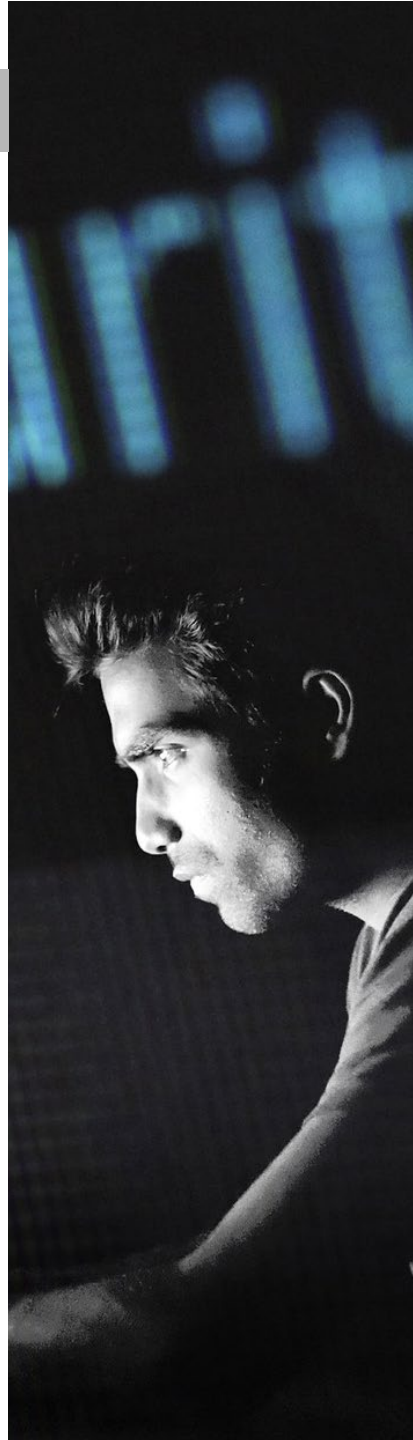
Waarom worden persoonsgegevens gestolen?
Persoonsgegevens zijn simpelweg veel geld waard. Criminelen kunnen gestolen persoonsgegevens en vertrouwelijke informatie eenvoudig te gelde maken, bijvoorbeeld door fraude te plegen of door vertrouwelijke informatie te koop aan te bieden.

Ter bescherming van persoonsgegevens zijn strenge regels opgelegd aan het bedrijfsleven; bedrijven die een fout maken of gehackt worden, moeten de kosten van de inbreuk betalen.



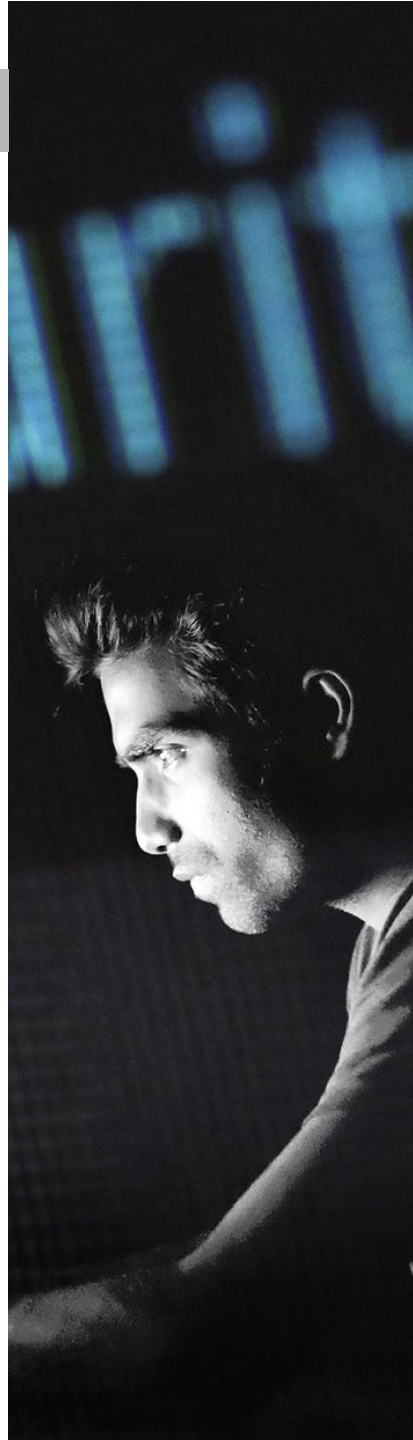
8. Mogelijke oorzaken

- ✓ Schadelijke of criminele aanvallen veroorzaken 44% van de inbreuken (grootste financiële schade);
- ✓ 31% van de inbreuken zijn te wijten aan de nalatigheid van personeel. Hieronder vallen ook gestolen, verloren, mobiele toestellen en fouten gemaakt door derden;
- ✓ 25% van de inbreuken worden veroorzaakt door een het falen van een IT-systeem.



9. Mogelijke kosten

- ✓ Bedrijfsschade;
- ✓ Kosten van digitaal forensisch onderzoek;
- ✓ Melden en inlichten van gedupeerden (kosten lopen uiteen van € 1,25 tot € 5 p.p.);
- ✓ Kosten voor PR en crisismanagement;
- ✓ Ransomware, betaling voor cyberafpersing;
- ✓ Kosten voor herstel van ICT-systemen.



10. Dekking door Cyber en Data Risks verzekering

Systeeminbraak: Deze dekking dekt eigen kosten als gevolg van inbraak op systemen of data:

- ✓ Kosten van forensisch onderzoek;
- ✓ Kosten van communicatie met klanten, toezichthouders, justitie, creditcard-maatschappijen en andere belanghebbenden;
- ✓ Kosten voor extra klantenondersteuning, bijvoorbeeld via een callcenter;
- ✓ Kosten van crisismanagement, reputatieherstel en pr-campagnes.

Privacy: Deze dekking dekt gevolgen van gestolen privacygevoelige gegevens:

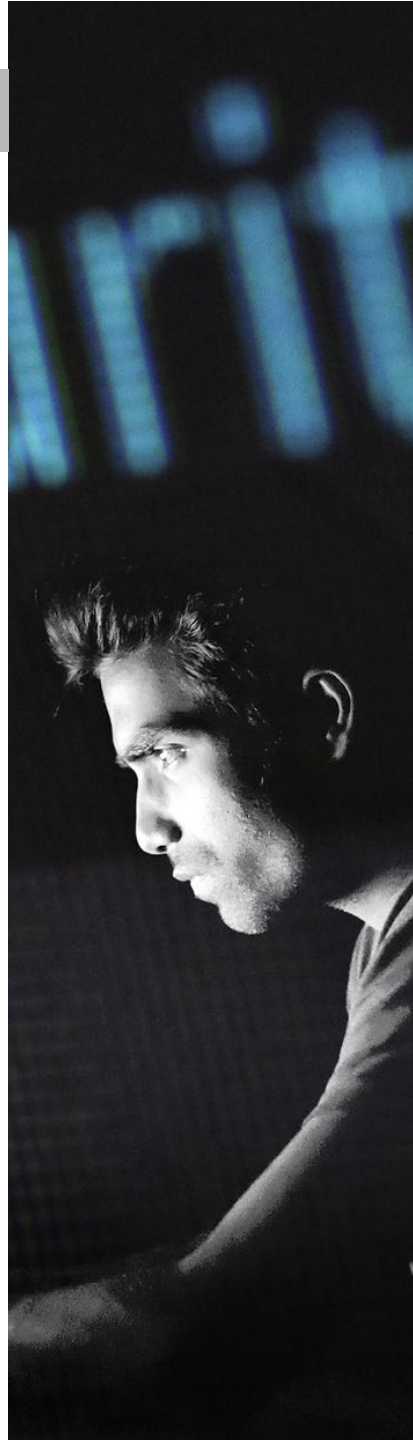
- ✓ Kosten van onderzoek door bijvoorbeeld justitie of creditcardmaatschappijen;
- ✓ Claims van individuele personen;
- ✓ Boetes opgelegd door toezichthouders, of andere verplichte vergoedingen.

Digitale aansprakelijkheid:

- ✓ Deze dekking dekt voortvloeiende schade als bijvoorbeeld de website of e-mail __ onbedoeld het auteursrecht schendt, laster verspreidt of een virus bevat.

Hacking: Deze dekking dekt de 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 oorzaak van een hacking.

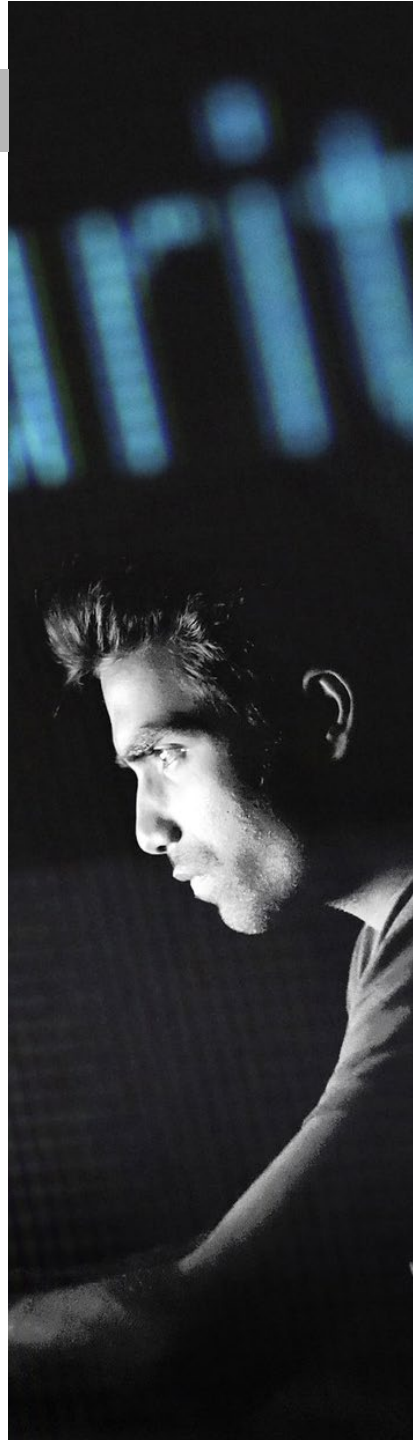


10. Dekking door Cyber en Data Risks verzekering

Afpersing: Deze dekking beschermt
Beschermt tegen de schade van hackers die de website of data gijzelen. U krijgt bijstand van security-adviesbureau NetDiligence en eventueel betaald losgeld wordt vergoed.

Omzetverlies door cyberaanvallen: Deze dekking dekt omzetverlies
Dekt omzetverlies door bijvoorbeeld een DDos-actie of andere aanval op de computersystemen wanneer deze leidt tot omzetverlies, bijvoorbeeld door uitval van een webwinkel.

Alle onderdelen zijn in één pakket verzekerd. Het is niet mogelijk om de onderdelen los van elkaar te verzekeren.



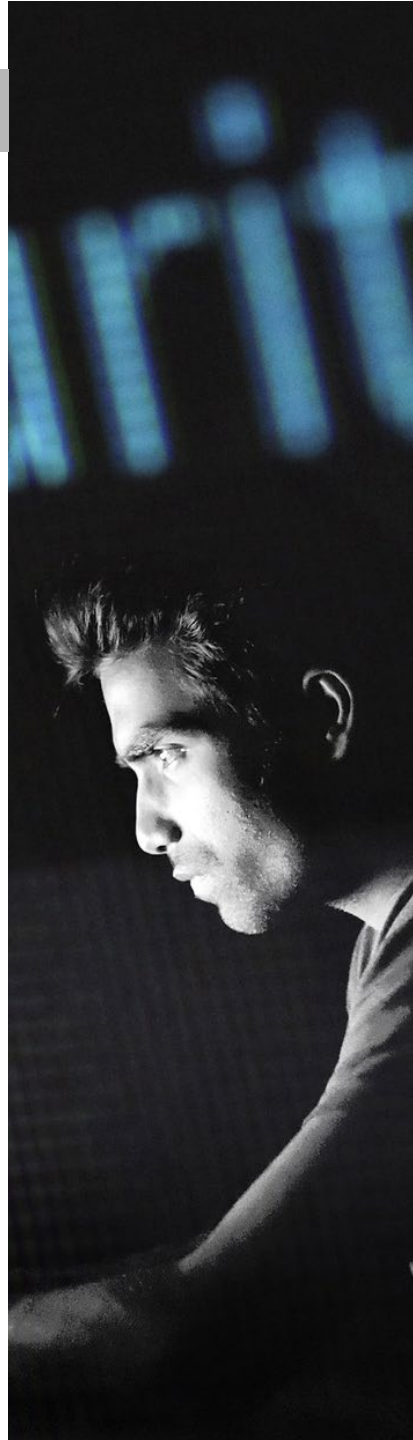
11. ESET kwetsbaarhedenscan

Kwetsbaarhedenscan op alle bereikbare adressen

Uw online verbindingen worden met behulp van een scan op openstaande poorten geanalyseerd en op kwetsbaarheden gecontroleerd. Deze scan geeft inzicht in externe risico's die de cybercrimineel mogelijk zou kunnen gebruiken als toegangspunt tot uw bedrijfsgegevens.

Rapportage en advies

Na afloop van de scan stelt de ESET Cyber Security Engineer een overzichtelijk rapport op met de gevonden kwetsbaarheden en het risiconiveau per kwetsbaarheid, geclassificeerd van laag tot kritiek niveau. Op basis van deze informatie worden adviezen uitgebracht om de gevonden kwetsbaarheden of risico's te verkleinen of te verzekeren.



12. Over ons

Meer dan deskundig advies alleen

Kijk op mensen, organisaties en ambities
De Regt adviesgroep is al meer dan 20 jaar dé specialist op het gebied van Verzekeringen, Pensioenen, Verzuim & Inkomen, Bedrijfsrisico's en (werknemers)communicatie. Wij zetten onze kennis en ervaring graag in om onze relaties proactief te adviseren over de risico's die ze als particulier, ondernemer of werkgever lopen. En daarin gaan we graag een stap verder.

Ambities waarmaken
Onze ervaren adviseurs geven een actueel inzicht in de situatie van uw organisatie, van uw medewerkers en van uzelf. Zodat u bewuste keuzes kunt maken waarmee u uw ambities waar kunt maken. Wij volgen voortdurend de nieuwste ontwikkelingen, beheren uw verzekeringen en communiceren met uw medewerkers. Zo houden we samen met u uw arbeidsvoorwaarden betaalbaar en overzichtelijk.

Doen waar u goed in bent
Wij kennen uw organisatie, uw mensen en uw doelstellingen. Ons streven is een langetermijnrelatie, gebaseerd op vertrouwen, transparantie en wederzijds respect. Hierdoor kunt u zich concentreren op uw kernactiviteiten. In de wetenschap dat u uw zaken goed geregeld heeft en aan alle geldende wetgeving voldoet.

De Regt adviesgroep
Larenseweg 60 A
7241 CN Lochem

T: 0573-255300
E: info@deregt.nl
KvK: 08071612