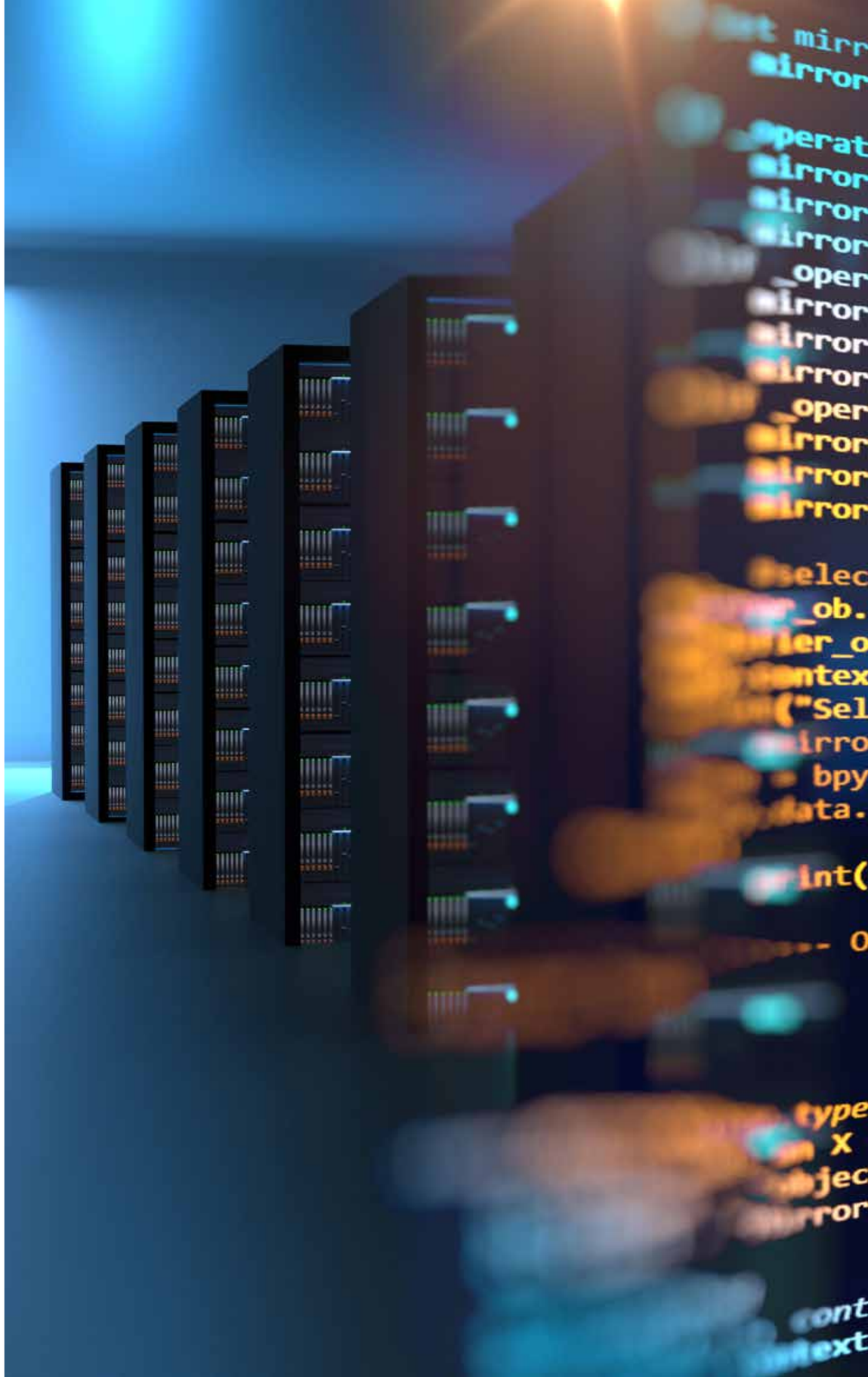
1768
Raetsheren

Cyberrisico’s: mijden helpt niet, managen wel

INHOUDSOPGAVE



INTRODUCTIE RAETSHEREN

Verandering is een kans

Onder invloed van globalisering en digitalisering verandert onze samenleving. Wet- en regelgeving wordt complexer, transparantie wordt belangrijker en het risicoprofiel van organisaties en ondernemingen beweegt mee. Verandering brengt ook nieuwe kansen met zich mee. Het bedrijfsleven en de publieke sector willen inspelen op deze kansen om klantwaarde te creëren. Ook dit brengt weer nieuwe risico's met zich mee.

Raetsheren helpt zijn partners ***risico's te managen*** zodat zij de rust en ruimte krijgen nieuwe uitdagingen aan te gaan, ***zelfverzekerd te handelen*** en daardoor ***kansen te benutten.***

Raetsheren is een zelfstandige en onafhankelijke, internationaal opererende assurantiemakelaar zonder eigendomsverhoudingen tot banken en verzekeraars. De assurantiemakelaars en adviseurs van Raetsheren kennen de opdrachtgevers, de markten en het vakgebied van risico's en verzekeringen. Met die kennis, ervaring en deskundigheid ondersteunen zij de opdrachtgevers met segmentspecifieke oplossingen. Bij voorkeur door risico's weg te nemen en daarnaast door risico's te managen en processen te beheersen.

Werken in een wereld van cyberrisico's

2018

Aantal meldingen

20.881

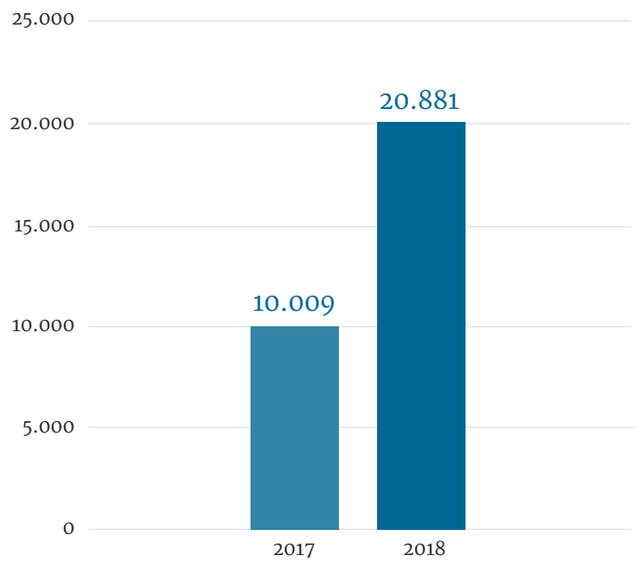
Type datalekken

63%
persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger

Meest gelekte gegevens

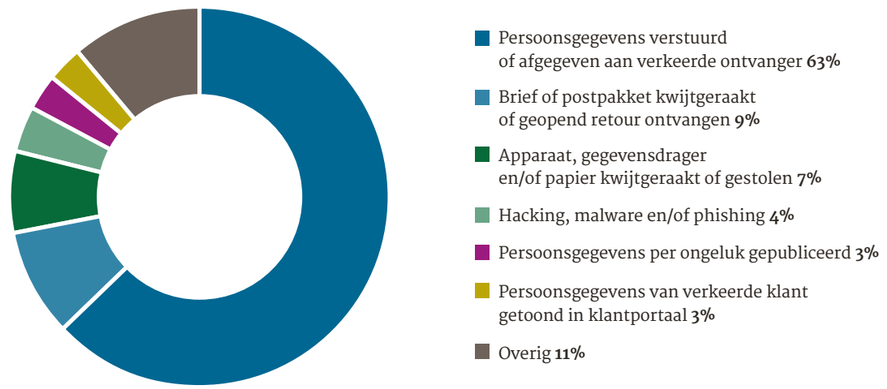
NAW, geslacht, geboortedatum en leeftijd, BSN

Aantal meldingen 2017 vs. 2018



Bron: Autoriteit Persoonsgegevens.

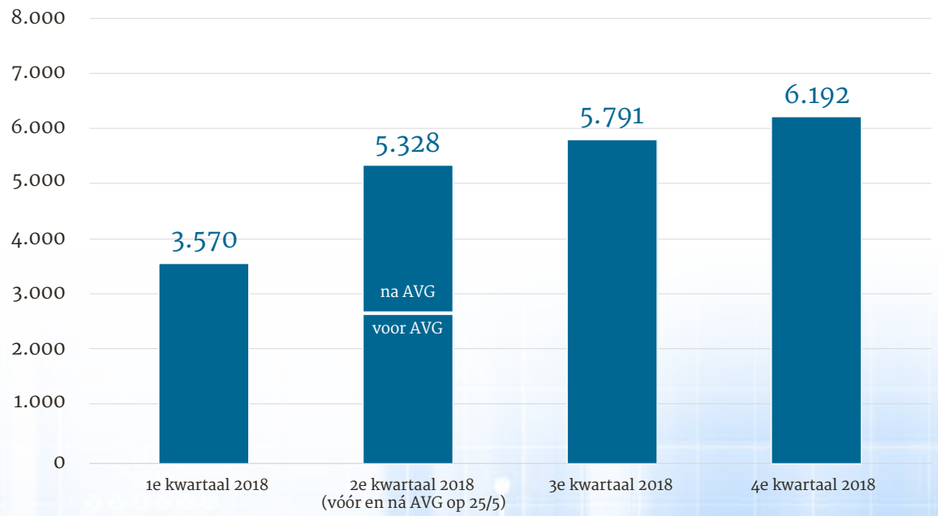
Meldingen datalekken per sector



Bron: Autoriteit Persoonsgegevens.

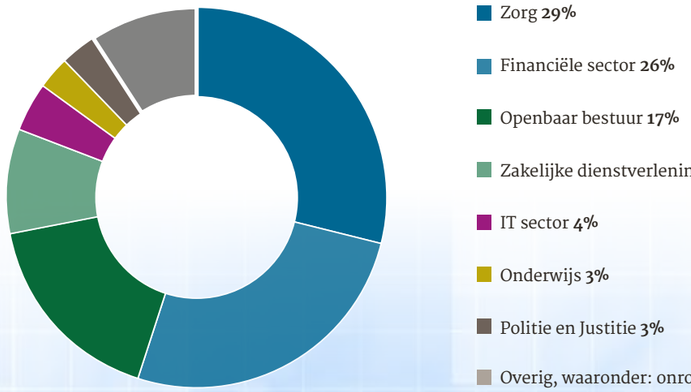
2. FEITEN EN CIJFERS

Aantal meldingen in 2018



Bron: Autoriteit Persoonsgegevens.

Meldingen datalekken per sector



Bron: Autoriteit Persoonsgegevens.

3. CYBERINCIDENTEN IN NEDERLAND

Hoe groot is de dreiging?

Recente gegevens van het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Justitie en Veiligheid tonen aan dat de omvang en ernst van de digitale dreiging in Nederland toenemen. Cyberaanvallen zijn immers profijtelijk, laagdrempelig en weinig riskant voor aanvallers. Die aanvallers kunnen criminelen zijn. Maar er zijn ook staten die digitale aanvallen inzetten en op steeds grotere schaal toepassen.

Geen doelwit, toch schade

Ook als uw bedrijf geen doelwit van een dergelijke aanval is, loopt u het risico getroffen te worden door nevenschade. Bekend voorbeeld is de aanval met de NotPetya-malware waarbij tal van Europese bedrijven schade opliepen. Zo waren de containerterminals van APM, dochterbedrijf van logistiek bedrijf Maersk, dagenlang buiten werking.

Houd digitale ramen en deuren gesloten

Een cyberaanval kan niet altijd voorkomen worden. Maar u kunt het de aanvallers wel zo moeilijk mogelijk maken. Een goede verdediging maakt minder kwetsbaar en kan incidenten voorkomen of beperken. Oftewel: houd digitale ramen en deuren gesloten. Denk daarbij aan het tijdig installeren van updates of het voorkomen van tekortkomingen in configuraties. De ervaring leert dat veel incidenten voorkomen hadden kunnen worden als organisaties hun basisveiligheid op orde hadden gehad.

Cybersecuritybeeld Nederland 2018

Aanvallen leiden ook in andere landen tot schade

Grote incidenten laten zien dat aanvallers het risico van nevenschade niet voorzien of mogelijk zelfs accepteren.
In andere landen heeft nevenschade geleid tot maatschappelijke verstoring, in Nederland tot economische schade. De kwetsbaarheid voor spionage, verstoring en sabotage groeit door de afhankelijkheid van buitenlandse partijen.

Sabotage en verstoring vormen grootste dreiging

Landen voeren steeds meer digitale aanvallen uit. Sabotage en verstoring zijn grootste dreiging voor de nationale veiligheid.
Het doel is om strategische informatie te verwerven via spionage. Om de publieke opinie of democratische processen te beïnvloeden, of om vitale systemen te verstoren of zelfs te saboteren.

Basismaatregelen zijn vaak niet op orde

Overheid, bedrijven en burgers zijn afhankelijk van cybersecurity. De gevolgen van aanvallen kunnen groot zijn.
Omdat organisaties basismaatregelen niet op orde hebben, blijven aanvallers succesvol. Onveilige producten en diensten maken het de aanvaller nog makkelijker.

Digitale dreiging is permanent

Voor een aanvaller is een cyberaanval veelal profijtelijk, laagdrempelig en weinig riskant.
De gevolgen van aanvallen en van uitval van vitale systemen kunnen maatschappijontwrichtend zijn. Diefstal van waardevolle informatie kan het vertrouwen in de Nederlandse economie aantasten.

Dreiging van beroepscriminelen groeit

Beroepscriminelen blijven zich ontwikkelen op digitaal vlak. Daardoor neemt de dreiging verder toe.
Vanuit een professionele criminele dienstensector worden hulpmiddelen geleverd waarmee aanvallers op eenvoudige wijze digitale aanvallen kunnen uitvoeren. De laagdrempelige toegankelijkheid van aanvals-middelen zorgt voor vergroting van de dreiging.

Bron: Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Justitie en Veiligheid.

Cyberrisico en de nieuwe wet voor databescherming

Sinds 25 mei 2018 is er een nieuwe Europese wet voor databescherming, voluit genaamd de Algemene Verordening Gegevensbescherming (AVG). De nieuwe privacywetgeving geldt voor alle ondernemers, instellingen en overheden die persoonsgegevens verwerken in de Europese Unie.

Onder de AVG is het begrip ‘persoonsgegevens’ aanzienlijk verruimd. Ook voor het opslaan van een naam of kenteken, online nickname of een IP-adres zijn in de AVG regels opgesteld.

Bij Raetsheren hebben we voor en met onze klanten inmiddels de nodige ervaring opgedaan bij het implementeren van de AVG. Zo zijn onze klanten ervan verzekerd dat ze voldoen aan de nieuwe wet- en regelgeving. Maar we zorgen er ook voor dat datastromen binnen de organisatie in kaart worden gebracht zodat eventuele risico’s zichtbaar worden.

De AVG in een notendop

De nieuwe privacywetgeving vanaf 25 mei 2018

Op basis hiervan mag je persoonsgegevens verzamelen
De grondslag

- Toestemming van de gebruiker
- Vitale belangen
- Wettelijke verplichting
- Overeenkomst
- Algemeen belang
- Gerechtvaardigd belang

Het begint aan de keukentafel
Zorgvuldigheid

- Functionaris gegevensbescherming
- Privacy by design
- Impact assessment

Technische en organisatorische maatregelen
Verplichtingen

- Register met alle verwerkingen
- Gegevens-beschermingsbeleid
- (Digitale) beveiliging

Mensen moeten controle kunnen uitoefenen
Rechten van de betrokkenen

- Recht om in te zien
- Recht om te wijzigen
- Recht om vergeten te worden
- Recht om gegevens over te dragen
- Recht op informatie

4. DE NIEUWE PRIVACYWETGEVING

“ *De AVG in vier stappen*

1. Wanneer mag u persoonsgegevens verzamelen?

Persoonsgegevens mogen alleen voor een bepaald, uitdrukkelijk omschreven doel worden verwerkt. De AVG noemt zes redenen waarom u gegevens van personen mag verzamelen. U kunt de gegevens nodig hebben voor een wettelijke verplichting of overeenkomst. Of er moet sprake zijn van vitaal belang, een algemeen belang of een gerechtvaardigd belang.

Let op: het tot in het oneindige bewaren van gegevens mag niet meer. Als identificatie niet meer noodzakelijk is voor het doel, dan moeten de persoonsgegevens worden verwijderd of geanonimiseerd. Ook moeten de gegevens worden beveiligd door middel van technische en organisatorische maatregelen.

2. Wat heeft u nodig om gegevens te mogen verzamelen?

Bovenal heeft u toestemming nodig van de gebruiker. Belangrijk is dat de gebruiker actief toestemming geeft en het hem of haar duidelijk moet zijn wat er wordt gevraagd. Een vooraf aangevinkt hokje is niet meer voldoende. Ook heeft de betrokkene te allen tijde het recht de toestemming in te trekken. Dat vereist extra inspanning bij het vastleggen van de gegevens.

3. Hoe en wat moet u vastleggen?

Persoonsgegevens moeten op behoorlijke, rechtmatige en transparante wijze worden verwerkt. In het geval van een discussie met de betrokkene moet bewezen kunnen worden dat deze ondubbelzinnig de toestemming heeft gegeven. En als u het in uw eigen organisatie op orde heeft, bent u er nog niet. Want u bent ook verplicht erop toe te zien dat eventuele externe partijen die voor u gegevens verwerken, de regels naleven.

Ook dit dient te worden vastgelegd in een overeenkomst die een aantal verplichte onderdelen moet bevatten. Daartoe behoren onder meer het doel van de verwerking, het soort persoonsgegevens dat wordt verwerkt en de categorieën van betrokkenen. Andere onderdelen betreffen de verplichting tot passende beveiligingsmaatregelen, het meewerken van de verwerker aan audits om te controleren of de verwerker zich aan alle verplichtingen houdt en het teruggeven of vernietigen van de gegevens na afloop. Tot slot mag de verwerker geen derde partij inschakelen zonder de voorafgaande schriftelijke toestemming van de verantwoordelijke.

4. Wat moet u aan wie melden?

Transparantie brengt met zich mee dat u de betrokkene moet melden wat er met zijn persoonsgegevens gebeurt. Alles moet in eenvoudige en duidelijke taal worden gecommuniceerd. Naast het bekende recht op verzet, inzage en rectificatie, heeft de betrokkene onder de AVG ook het recht om vergeten te worden, het recht op overdraagbaarheid van zijn data, het recht de verwerking te beperken en het recht bezwaar te maken tegen bepaalde verwerkingen.

Als organisatie moet u kunnen aantonen dat u voldoet aan alle verplichtingen uit de AVG. Denk hierbij aan de toestemming, gegeven informatie, rechten van betrokkenen, beveiliging van gegevens, minimalisatie van de verwerkingen en afspraken met verwerkers.

Voor veel organisaties brengt de invoering van de AVG een enorme belasting met zich mee. Reden waarom het aanstellen van een Data Privacy Officer niet alleen verplicht maar ook onontbeerlijk is. Het is belangrijk een goed systeem te hebben waarin de gegevens worden vastgelegd en op basis waarvan bij een eventueel geschil altijd bewezen kan worden dat de organisatie aan de verplichtingen heeft voldaan en de beginselen van de AVG niet heeft geschonden.

5. CYBERRISICO-STRATEGO

Een spel zonder einde

Van virtueel vandalisme tot cybercrime, van burst-aanvallen tot updates van het digitale afweergeschut: in de wereld van de cyberrisico's volgen de ontwikkelingen elkaar in razend tempo op. De ene DDoS-aanval is nog niet afgeslagen of de andere staat alweer aan de virtuele voordeur te bonken.

Houdt u het allemaal nog bij? Wij bij Raetsheren wel.

En omdat we kennis graag delen, hebben onze specialisten voor u een aantal opmerkelijke cyberrisico-weetjes op een rijtje gezet.

PDF

PDF is het bestandstype waarop interne bedreigingen het meest zijn gericht.

53%

53% van de verdedigers beheert meer dan de helft van hun infrastructuur in de cloud.

34%

34% van de beveiligings-professionals vertrouwt op machine learning.

1

Mobiele apparaten staan op nummer 1.

1 miljoen

Nyetya is op meer dan 1 miljoen computers geïnstalleerd.

72%

72% van de verdedigers geeft nog steeds de voorkeur aan superieure producten.

> *'Burst-aanvallen' vinden steeds vaker plaats, worden steeds complexer en duren steeds langer. Uit een onderzoek bleek dat 42% van de organisaties in 2017 met deze vorm van DDoS-aanvallen te maken heeft gehad. In de meeste gevallen duurden deze terugkerende bursts slechts enkele minuten.*

> *Interne bedreigingen: een paar 'onbetrouwbare' gebruikers kunnen een grote impact hebben. Bij slechts 0,5% van de gebruikers werd bepaald dat zij verdachte downloads uitvoerden. Deze verdachte gebruikers waren elk verantwoordelijk voor het downloaden van gemiddeld 5.200 documenten.*

> *Beveiliging wordt beschouwd als een belangrijk voordeel van het hosten van netwerken in de cloud.*

> *Het gebruik van infrastructuren op locatie en in de openbare cloud neemt toe. Volgens beveiligingspersoneel dat aan het onderzoek deelnam, vormt beveiliging het belangrijkste voordeel van het hosten van netwerken in de cloud.*

> *Een omgeving met meerdere leveranciers verhoogt het risico. Bijna de helft van de beveiligingsrisico's waarmee organisaties te maken hebben, is het gevolg van het gebruik van meerdere beveiligingsleveranciers en -producten.*

6. CYBERVERZEKERING RAETSHEREN

Cyberrisico's: mijden helpt niet, managen wel

Digitale ontwikkelingen gaan snel en het ziet er niet naar uit dat hier verandering in gaat komen. Integendeel.

De verwachting is dat de digitale ontwikkelingen alleen maar sneller zullen gaan. Dit vergroot de kans op een cyberincident. Ook zal de impact van een incident alleen maar groter worden.

Een verzekering biedt geen bescherming tegen cybercriminelen op zichzelf, maar verzekert wel de gevolgen van een aanval. Die gevolgen kunnen groot zijn. Denk bijvoorbeeld aan verlies van data, hacking en ransomware-aanvallen.

Een door Raetsheren afgesloten cyberverzekering stelt u in staat op een zo adequaat mogelijke wijze te reageren op een cyberincident. Zo waarborgt u de bedrijfscontinuïteit. De cyberverzekering biedt dekking voor kosten van crisismanagement, waaronder de inzet van IT-specialisten, advocaten en communicatie-adviseurs.

> *"Cyberincidenten blijven toenemen en vormen het tweede belangrijkste bedrijfsrisico (40%). Vijf jaar geleden stond het op de vijftiende plaats.*

> *"Net zoals een natuurramp kan een aanval mogelijk honderden bedrijven beïnvloeden.*

Wat dekt een cyberverzekering van Raetsheren?

1. **De kosten van crisismanagement:** IT-diensten, advocaten, PR, forensisch onderzoek, kredietbewaking, notificatiekosten.
2. **Aansprakelijkheid:** schadevergoeding en juridische bijstand in geval van aanspraken van derden als gevolg van verlies van persoonsgegevens en/of bedrijfsinformatie, ook als deze gerelateerd is aan multimedia-activiteiten (zoals smaad en laster) en de aanschaf van nieuwe creditcards.
3. **Boetes:** kosten voor onderzoek door toezichthouders, juridische bijstand en de boetes zelf (voor zover juridisch toegestaan).
4. **Kosten gerelateerd aan cyber-/privacyafpersing**, bijvoorbeeld door het gebruikmaken van ransomware.
5. **Eigen schade**, zoals bedrijfsschade.

6. CYBERVERZEKERING RAETSHEREN

Waarom Raetsheren?

Het gemak van een partner die alles voor u regelt en zorgt voor adequaat crisismanagement. In geval van een incident zijn wij 24/7 bereikbaar. Zo kunnen wij direct actie ondernemen. Daardoor kunnen wij schades, zoals reputatieschade beperken.

Omdat wij onafhankelijk zijn maar door onze eeuwenlange ervaring alle marktpartijen kennen, weten onze klanten zich verzekerd van:

- een uitgebreide dekking;
- lage premies en eigen risico's.

"De manier waarop een bedrijf een datalek beheert, heeft een directe impact op de uiteindelijke kosten.

"Zogenaamde 'cyber-orkaan'-evenementen, waarbij hackers grote aantallen bedrijven verstoren, nemen toe.

"Bewustwording van de cyberdreiging stijgt onder het midden- en kleinbedrijf.

"Reputatieschade is onvermijdelijk wanneer het antwoord op een cyberincident ontoereikend is.

"Ondertussen betekent de introductie van de Algemene Verordening Gegevensbescherming (AVG) in mei 2018 in heel Europa het vooruitzicht van meer en hogere boetes voor bedrijven die zich niet aan de regels houden.

“

Meer dan een partner op het gebied van risico's en verzekeringen.

Rianne Baumann
Manager Sluiting
Aansprakelijkheid
06 - 511 193 54

Imco Struiksma
Commercieel directeur
06 - 502 664 54

1768
Raetsheren

Raetsheren van Orden Groep B.V.
Arcadialaan 36a
Postbus 1015
1810 KA Alkmaar
www.raetsheren.nl