CYBERVERZEKERING

NUTTIG OF OVERBODIG

HEILBRON

Voorwoord

Weet je hoe groot **jaarlijks de schade is van cybercriminaliteit in Nederland? 10 miljard euro!** Cybercrime is de snelst groeiende vorm van misdaad. Steeds meer bedrijven en burgers worden slachtoffer. We horen daar relatief weinig over, omdat het bijna een soort taboe is om te vertellen dat je gehackt bent of om te vertellen dat je in de praatjes van online oplichters bent getrapt. Burgers raken soms enorme bedragen kwijt en **bij bedrijven is de ellende helemaal groot**, vooral als hun volledige computersysteem gegijzeld wordt door hackers. Inclusief de back-ups.

Toen ik me voor het eerst in het onderwerp cybercrime verdiepte om het boek *'Komt een vrouw bij de h@cker'* te schrijven, was ik verbaasd dat het zo simpel is geworden om volledige identiteiten te stelen. Ik dacht dat het vooral mensen overkwam die niet voorzichtig genoeg waren. Maar de verhalen van de slachtoffers in mijn boek laten één ding zien: **het kan iedereen overkomen.** Niet echt een geruststellende gedachte als je ziet hoe groot de gevolgen zijn: **ik sprak met mensen die door identiteitsfraude hun werk, hun huis, hun relaties en ook hun bedrijf kwijtgeraakt zijn.** Ze dachten allemaal: 'Dit kan niet waar zijn in een land als Nederland, ik ben in een slechte film beland'. Vaak duurde het jaren om de gevolgen terug te draaien, maar niet alles kon teruggedraaid worden.

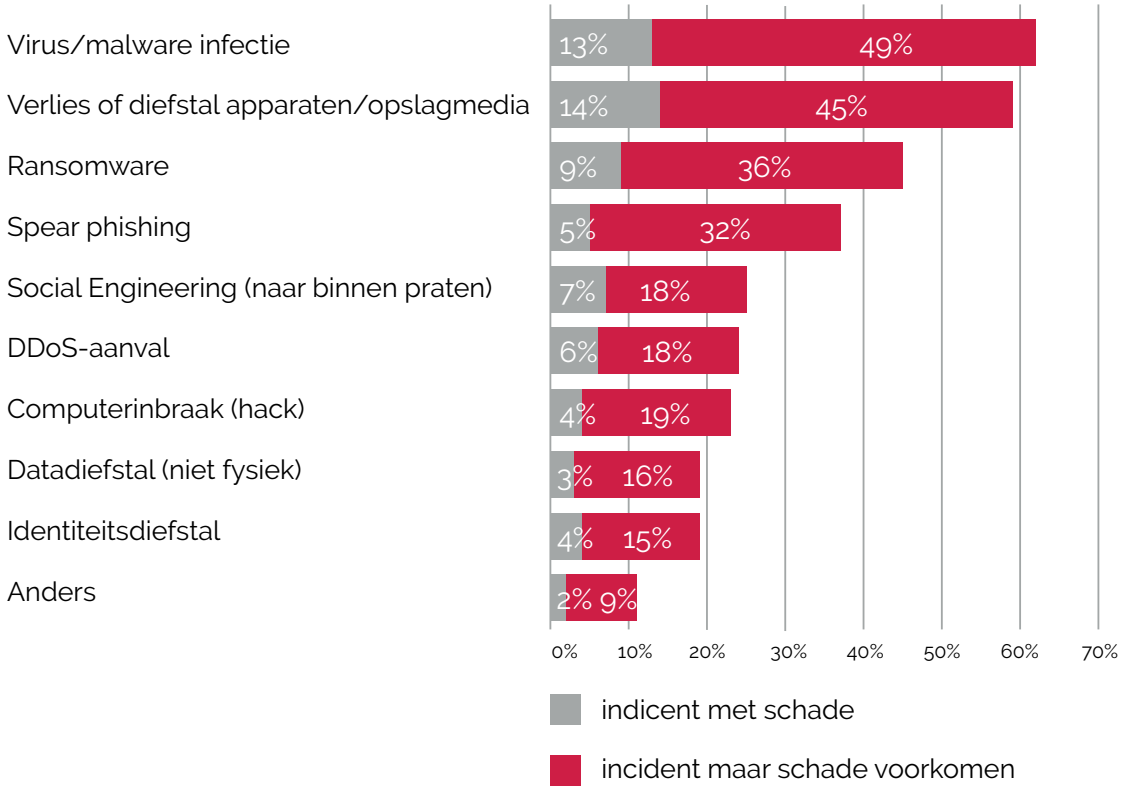
Het gebeurt steeds vaker dat bedrijven, webshops en overheidsorganisaties gehackt worden en al onze persoonlijke gegevens lekken. Je kunt je eigen computer en mobiel beschermen, maar tegen dat soort datalekken kun je jezelf nauwelijks beschermen. Sinds het verschijnen van *'Komt een vrouw bij de h@cker'* geef ik zo'n twintig lezingen per maand om bedrijven en overheidsorganisaties wakker te schudden hoe belangrijk het is geworden om onze persoonlijke gegevens goed te beschermen. Het **kennisniveau over privacy en cybercrime** van de meeste mensen laat te wensen over. Daarom heb ik een quiz gemaakt om uw **cyberkennis te vergroten**. Wilt u de **quiz ontvangen**? Stuur me een berichtje via www.mariagenova.nl en u ontvangt de quiz kosteloos binnen drie dagen. Laten we het de cybercriminelen niet te makkelijk maken!

Maria Genova,
schrijfster en cybercrime-expert

Inhoudsopgave

De kans dat uw bedrijf door cybercrime wordt getroffen is niet heel klein

Met welke van de volgende incidenten heeft uw organisatie de afgelopen 12 maanden te maken gehad?



Een Kaspersky onderzoek uitgevoerd in 2018.
302 organisaties zijn ondervraagd met behulp van een webgebaseerde panel survey.

Cyberverzekering: nuttig of overbodig?

Criminelen zijn inventief, zij bedenken steeds weer nieuwe, geavanceerde methoden om bedrijven en consumenten geld afhandig te maken. Bovendien testen zij hun **kwaadaardige programma's (malware)** uitvoerig voordat zij het gaan toepassen.

Bij deze tests kijken ze wat er nodig is om ongezien langs de firewall en de antivirussoftware te komen. Als dat lukt, kan de malware worden verspreid. De malware kan in het begin dus ongezien zijn gang gaan.

Pas als de nieuwe malware wordt ontdekt, kunnen er door de leveranciers van de firewall en de antivirussoftware maatregelen tegen genomen worden. Vaak zijn dan al vele slachtoffers gemaakt.

Het duurt dus altijd een poosje voordat de antivirussoftware de nieuwe malware herkent en tegenhoudt.

"Wij hebben een firewall én antivirussoftware geïnstalleerd. Wij hebben dus geen cyberverzekering nodig."

Cyberverzekering: nuttig of overbodig?

Wist u dat **minder dan 5% van alle ICT-bedrijven thuis is in cyber security**? Grote kans dus dat uw ICT'er onvoldoende kennis heeft van cyberrisico's. Hij zal best bereid zijn om, tegen betaling, ICT-problemen op te lossen, maar: betaalt het ICT-bedrijf ook de bedrijfsschade als uw bedrijf drie dagen stil ligt na een cyberincident? Betaalt het ICT-bedrijf ook het losgeld als u niet meer bij uw bestanden kunt? Regelt het ICT-bedrijf ook aanspraken van derden, bijvoorbeeld na diefstal van persoonsgegevens?

Cybercrime vindt altijd plaats met behulp van internet, maar veelal **draagt een menselijke factor bij aan het succes van een crimineel**, veelal via een onbewuste actie. Bijvoorbeeld het openen van een bijlage bij een e-mail waarin malware zit of het klikken op een link van een valse (bank)website. Ook als alles technisch gezien voor goed elkaar is, of als de administratie in de cloud staat, bent u niet 100% veilig.

"Wij hebben een ICT-bedrijf dat alles regelt. Waarom zouden wij dan een cyberverzekering nodig hebben?"

Cyberverzekering: nuttig of overbodig?

"Mijn bedrijf is niet interessant voor criminelen. Een cyberverzekering vind ik overbodig."

Het klopt dat uw bedrijf waarschijnlijk geen doelwit is van criminelen. Maar (**cyber)criminelen worden door slechts één ding gedreven, geld.** En een geldstroom is aanwezig in elke onderneming. Indirect kunnen **klantgegevens en vertrouwelijk bedrijfsgegevens** ook geld opleveren. Als criminelen in het bezit van deze informatie komen, kunnen zij u afpersen.

Het verdienmodel van criminelen is gebaseerd op schaalgrootte. **Feitelijk 'schieten' zij met hagel:** als zij aan 150.000 e-mailadressen een bericht sturen en slechts één procent opent de "besmette" bijlage, raken 1.500 systemen geïnfecteerd. Dat zijn in de ogen van criminelen 1.500 kansen om geld te verdienen.

Vergelijk het met de traditionele inbreker. Wanneer hij een wijk inspecteert check hij op zwakke sloten en openstaande ramen. Wellicht ziet het huis er niet heel kostbaar uit, maar **als het raam openstaat gaat hij naar binnen** en weet altijd wel iets van waarde te bemachtigen.

Cybercrime binnen het MKB blijft onder de radar

Er gaat geen dag voorbij zonder dat de media berichten over cybercriminaliteit. Toch hebben nog veel MKB'ers zoiets van 'ons overkomt het toch niet'. Vaak ingegeven doordat ze het niet om zich heen zien gebeuren. Voorbeelden bij grote bedrijven zijn er legio. Binnen het MKB zijn ze minder zichtbaar. Toch hebben al veel MKB'ers in meer of mindere mate schade door cybercriminaliteit gehad. De schadelast in Nederland per jaar voor het MKB bedraagt € 1.000.000.000.

Jaarlijkse schadelast cybercrime voor het MKB: € 1.000.000.000 (1 miljard)

Dat de incidenten en schades niet bekend worden gemaakt, komt veelal door het **taboe** dat rond dit nieuwe risico hangt. Ondernemingen zijn gebaat bij een betrouwbaar en professioneel imago en kiezen er meestal voor cyberincidenten binnenskamers te houden. **Bedrijven vrezen voor reputatieschade en de gevolgen** die dit heeft voor het krijgen en behouden van klanten.

"Een brand of inbraak is vaak snel bekend, cybercrime blijft vooralsnog onder de radar."

Wat kost cybercrime?

Vanwege de serieuze en mogelijk verstrekkende gevolgen van cybercriminaliteit is het belangrijk een goede overweging te maken om wel of niet te verzekeren.

Met een verzekering bent u snel in staat te reageren, om zo de materiële en immateriële schade te beperken.

Dit zijn voorbeelden van verzekerbare schadeposten die veroorzaakt kunnen worden door een cyberincident:

- Bedrijfsschade:
  - Uurtarieven medewerkers * aantal uren stilstand.
  - Webshop: aantal uren stilstand * gebruikelijke online omzet per uur.
- Forensisch onderzoek voor opsporen en bepalen omvang hack/lek: € 4.000 per dag.
- Betalen losgeld.
- Herstel ICT-systemen: verwijderen malware, herstel en testen. Uurtarief ICT-expert: € 120.
- Kosten PR en crisismanagement – als een cyberaanval publiekelijk bekend wordt zal uw organisatie kosten moeten maken voor het informeren van alle betrokkenen. Uurtarief PR adviesbureau: € 100.
- Boete Autoriteit Persoonsgevens: maximaal € 10 miljoen of 2% van de (wereldwijde) omzet.
- Inhuren juridisch expert (€ 240 per uur).
- Datalek: kosten van gestolen of verloren bestand: gemiddeld € 185 per bestand.
- Reputatieschade.
- Aansprakelijkheidskosten en kosten van verweer.

Preventiemaatregelen

1. Maak uw werknemers bewust van de cyberrisico's.
2. Gebruik een virusscanner, firewall, anti-spyware, advertentieblockers en veilige websites.
3. Houd systemen up-to-date. Download en installeer de benodigde updates.
4. Maak regelmatig een back-up van al je data.
5. Gebruik sterke wachtwoorden en update ze regelmatig.
6. Beveilig mobiele apparaten en draadloos internet
7. Klik niet zomaar op alle links, afbeeldingen of video's. Kijk eerst naar de website of het bestand waar de link je naartoe stuurt door met je muis over de link te 'hooveren'.
8. Blijf weg van toegestuurde of gedownloade bestanden met de extensie '.exe', '.vbs' en '.scr' als u niet voor 100% zeker bent over de herkomst van deze bestanden.
9. Bij twijfel googel altijd eerst of er iets bekend is over de mail of site.
10. Als je een onbetrouwbaar of onbekend proces tegenkomt op je computer, verbreek dan onmiddellijk de verbinding met het internet of andere netwerkconnecties. Dit voorkomt verspreiding van de infectie.

Wat is gedekt door de cyberverzekering

EEN CYBERVERZEKERING OMVAT VEELAL DE VOLGENDE DEKKINGEN:

SYSTEEMINBRAAK

Dekking voor eigen kosten als gevolg van inbraak op systemen of data. Bijvoorbeeld kosten van forensisch onderzoek, kosten van communicatie met klanten, kosten van crisismanagement en reputatieherstel.

PRIVACY

Dekking voor de gevolgen van gestolen privacygevoelige gegevens. Bijvoorbeeld claims van individuele getroffen personen en boetes die zijn opgelegd door de Autoriteit Persoonsgegevens.

DIGITALE AANSPRAKELIJKHEID

Deze dekking dekt schade als bijvoorbeeld de website en een e-mail onbedoeld een virus verspreidt.

HACKING

De schade veroorzaakt door hackers is verzekerd. Bijvoorbeeld reparatie of vervanging van websites en data, kosten van forensisch onderzoek naar de oorzaak van een hacking en advies in systeembe-veiliging.

AFPERSING

Beschermt wanneer een afperser de website, het netwerk e.d. gijzelt en dreigt deze te beschadigen of te vernietigen of informatie openbaar te maken (ransomware). U krijgt bijstand en eventueel betaald losgeld wordt vergoed

OMZETVERLIES DOOR CYBERAANVALLEN

Dekt omzetverlies. Bijvoorbeeld wanneer door een DDos-aanval de webwinkel niet bereikbaar is.

Dit is een samenvatting van de geboden dekking. Hieraan kunnen geen rechten worden ontleend. De exacte dekking leest u in de polisvoorwaarden. Deze kunt u downloaden via www.turien.nl/voorwaarden-documenten.

Misschien wel de belangrijkste reden om een cyberverzekering af te sluiten

Een essentieel aspect, en volgens veel verzekerden zelfs hét belangrijkste aspect, van de cyberverzekering is de **hulpverlening**. Hiervan maakt u **gratis** gebruik wanneer u een cyberverzekering afsluit.

De hulpverlening is erop gericht om schade te beperken en bedrijfsactiviteiten snel te kunnen hervatten.

De hulpverlening bestaat uit:

- Een 24/7 helpdesk.
- Forensisch experts (voor het onderzoeken van de toedracht en de omvang en het herstel).
- De tijdige melding aan de Autoriteit Persoonsgegevens (AP) wordt gecoördineerd.
- Juridische bijstand.
- PR-bureau voor communicatie-advies.

De kosten voor forensisch **onderzoek bedragen vaak duizenden euro's per dag**. Ook juridische bijstand is erg kostbaar, maar essentieel wanneer u een cyberincident heeft. Deze mensen zijn bekend in het woud van regels en procedures en zijn de aangewezen personen om uw bedrijf weer snel productief te maken.

Praktijkvoorbeeld

Bron: Chubb brochure Cyberschades uit de praktijk

Aanval door ransomware	Impact	Kosten
Een werknemer van een productie-bedrijf van auto-onderdelen klikte op een link in een e-mail, waardoor malware op de server van het bedrijf werd gedownload en alle gegevens werden versleuteld. Op de computer van de werknemer verscheen een e-mail waarin € 10.000 aan Bitcoins werd geëist binnen 48 uur in ruil voor de decryptie-sleutel. Het bedrijf belde het Chubb Cyber Incident Response nummer voor hulp. De toegewezen cyber incident manager regelde forensische ICT-experts om de bedreiging te beoordelen en te bepalen of het bedrijf de betaling van het losgeld kon voorkomen.	**Aansprakelijkheid voor netwerkbeveiliging** - het falen van de netwerkbeveiliging van verzekerde om kwaadwillige handelingen via de computer te voorkomen	Zie cyber incidentkosten (onder)
	Digitale afpersing - kosten voor de aanpak van afpersingsbedreigingen om informatie of een kwaad-aardige code vrij te geven, tenzij afpersingsgeld wordt betaald	
	- Kosten voor een ICT-consultant om onder andere de back-up- mogelijkheden te beoordelen	€ 16.000
	Cyber incidentkosten	
	- Forensische onderzoekskosten om de malware op te sporen, de impact te analyseren en de schade in kaart te brengen	€ 21.000
	- Kosten voor juridisch advies	€ 8.000
	- Kosten voor cyber incident manager	€ 7.000
	Verlies van data - kosten voor het vervangen van verloren of beschadigde data	€ 17.000
Conclusie Hoewel de eis in Bitcoin lager was dan de kosten die onder de verzekering waren gemaakt, wordt door zowel Europol als de FBI aangeraden om geen cyber losgeld te betalen. Niet alleen worden door het betalen van het losgeld criminele activiteiten in stand gehouden, maar het impliceert ook een gebrek aan effectieve en betrouwbare back-up procedures van een bedrijf. Back-ups moeten off-site en buiten het netwerk om worden opgeslagen. Desondanks begrijpt Chubb dat het betalen van losgeld onder sommige omstandigheden de beste optie kan zijn.		**€ 69.000**

Praktijkvoorbeeld

Bron: Chubb brochure Cyberschades uit de praktijk

Fout door werknemer	Impact	Kosten
Een recruiter van een zorginstelling stuurde per ongeluk het verkeerde bestand mee in een e-mail naar vier kandidaten. Het bestand bevatte namen, adressen en BSN-nummers van voormalige werknemers. De verzekerde belde het Chubb Cyber Incident Response nummer voor assistentie en een cyber incident manager werd aangesteld. Juridische adviseurs werden ingeschakeld om de met regelgeving samenhangende gevolgen te managen.	**Privacy-aansprakelijkheid** - onzorgvuldig beheer van persoonsgegevens en/of vertrouwelijke bedrijfs-gegevens, inbreuk op het privacybeleid van de zorginstelling. - Verweerkosten die voortvloeien uit de Meldplicht Datalekken - Verweerkosten en schikkingsbedragen voor claims van werknemers van wie de identiteit openbaar is gemaakt **Cyber incidentkosten** - Kosten voor cyber incident manager - Melding aan getroffen personen - Identiteitsdiefstal monitoringsdiensten voor getroffen personen - Kosten voor juridisch advies	 € 65.000 € 115.000 € 5.800 € 3.500 € 15.000 € 12.000
Conclusie Het gaat bij cyber lang niet altijd om technologische incidenten. Veel schades zijn het gevolg van menselijke fouten.		**€ 216.300**

Praktijkvoorbeeld

Bron: Chubb brochure Cyberschades uit de praktijk

Distributed denial-of-service (DDoS) aanval	Impact	Kosten
Een distributed denial-of-service aanval vond plaats bij een datacentrum waar een website van een webshop werd gehost. De aanval overspoelde het netwerk van het datacentrum met zoveel verkeer dat het netwerk uitviel. Hierdoor was de webshop 12 uur ontoegankelijk, voordat het back-up systeem de 100% functionaliteit hersteld had. In dit scenario was de online webshop de verzekerde. Nadat het Chubb Cyber Incident Response nummer was gebeld,werd een cyber incident manager aangesteld.	**Herstelkosten** - Extra arbeidskosten om de website weer te laten functioneren - Kosten van het inhuren van een externe serviceprovider **Bedrijfsschade** - Verlies van omzet en opbrengsten doordat de website niet bereikbaar was **Cyber incidentkosten** - Forensisch ICT-bedrijf - Kosten voor juridisch advies - Kosten voor cyber incident manager	 € 10.000 € 14.000 € 111.000 € 14.000 € 11.500 € 7.000
Conclusie Distributed denial-of-service (DDoS) aanvallen komen veelvuldiger voor doordat het gebruik van eenvoudig te hacken internet of things-apparatuur toeneemt. Om de impact van een scenario als dit zoveel mogelijk te beperken, is het belangrijk om een bedrijfscontinuïteitsplan op te stellen dat erop toeziet dat bedrijfskritische applicaties, systemen en activiteiten niet afhankelijk zijn van één kritieke ICT-leverancier. De cyber incident managers en leveranciers van Chubb zijn ervaren in het omgaan met DDoS-aanvallen en helpen om uw bedrijf zo snel mogelijk weer operationeel te krijgen.		**€ 167.500**

Over ons

Wij zijn Heilbron. Een totale financiële dienstverlener en risicomanager voor onze relaties op het gebied van verzekeringen, hypotheken, verzuim & pensioenen, inkomen & vermogen en makelaardij. Met jaren ervaring en een team van meer dan 200 specialisten op zowel particulier als zakelijk gebied.

Onze missie? Wij helpen klanten om privé en zakelijk (financiële) risico's in kaart te brengen en deze te minimaliseren. Dit doen we lokaal, dichtbij en samen met u als relatie van Heilbron.

Contact
Heilbron Leusden
Burgemeester de Beaufortweg 18
3833 AG Leusden

030 - 221 2777
leusden@heilbron.nl