Zicht risico- en verzekeringsadviseurs

Whitepaper cybercrime

Het is niet meer de vraag of een bedrijf met cybercriminaliteit te maken krijgt, maar wanneer. Cybersecurity is dus essentieel. Voor ieder bedrijf, zowel groot als klein. Want wist u dat cybercrime invloed kan hebben op ALLE schakels binnen uw bedrijf? Dus niet alleen op IT, maar ook op medewerkers, klanten, leveranciers en zelfs uw bedrijfsimago. Hoe cyber-bewust bent u?

VERZEKERING • BEDRIJFSRISICO • HYPOTHEEK • PENSIOEN

gelukkig geregeld!

Inhoudsopgave

Wat is cybercrime en wat zijn de risico's voor uw onderneming?

Kan uw onderneming blijven draaien op het moment dat de ICT niet meer functioneert vanwege een cyberaanval? Kan een datalek een faillissement van uw onderneming betekenen? Zomaar twee vragen die met cybercriminaliteit te maken hebben. Er wordt veel over gesproken, maar wat is het precies?

Wat is cybercriminaliteit?

Cybercriminaliteit en -datalekken zijn vormen van criminaliteit met ICT als middel. Maar ook als doelwit. Dit kan via uw computer, mobiele telefoon, maar ook via de computerchips die in de meeste telefoons en bankpassen zitten. En wist u dat ook bedrijfssystemen, moderne auto's en chipkaarten vatbaar zijn voor cybercriminaliteit?

Oorzaken inbreuk op data

Veel mensen denken dat door een goede ICT-beveiliging de kans op een cyberaanval minimaal is. In de praktijk blijkt dat het falen van een IT-systeem bijna nooit de echte oorzaak is van een inbreuk op data. De drie voornaamste oorzaken van cyberrisico's zijn:

- Criminele aanval; anderen verspreiden kwaadaardige software of hacken een computer.
- Menselijk falen; bijvoorbeeld door een makkelijk wachtwoord of een computer zonder firewall, maar ook het klikken op een verkeerde link.
- Technisch falen; door een storing of uitval.

De risico's voor uw onderneming

Bij de risico's van cybercriminaliteit denkt u waarschijnlijk aan het verlies van data of persoonlijke informatie. Waar u misschien niet aan denkt is dat uw bedrijfsvoering voor enige tijd plat kan komen te liggen. En dat u de schade met uw eigen team niet opgelost krijgt. Of dat u imagoschade oploopt en eigenlijk helemaal niet weet waar u moet beginnen om dit op te lossen. Met een cyberverzekering verzekert u zich van de juiste professionele hulp.

Wat is een datalek?

We spreken van een datalek als er een inbreuk is op de beveiliging zoals bedoeld in artikel 13 van de Wet bescherming Persoonsgegevens. Het gaat om de toegang tot persoonsgegevens of vernietiging, wijziging of het 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.

Meldplicht datalekken

Bedrijven en overheden zijn sinds 1 januari 2016 verplicht direct een melding te doen bij de Autoriteit Persoonsgegevens zodra zij een datalek hebben. Als het datalek mogelijk schadelijk is voor de persoonlijke levenssfeer van personen, dan moeten deze personen ook op de hoogte gebracht worden. Met deze meldplicht wil de overheid de persoonsgegevens nog beter beschermen.

Top 5 misverstanden rond cybercriminaliteit?

"Cybercrime is een serieus probleem voor Nederlandse bedrijven. Dat cybercriminelen onze ondernemingen zo interessant vinden, komt omdat Nederlandse bedrijven bovengemiddeld digitaal zijn en voorop lopen in kennis en innovatie", aldus Dave Maasland, misschien wel DE cybersecurity expert van Nederland. "Als je zelf de kennis niet in huis hebt, dan steel je het gewoon." Hoe komt het dan dat er toch nog steeds te weinig bedrijven cybercriminaliteit hoog op de activiteitenkalender hebben staan? Wij zijn met Dave in gesprek gegaan over de top 5 misverstanden.

Wie is Dave Maasland?

Dave Maasland (1990) is CEO bij ESET Nederland. Dit is één van de grootste IT-Security bedrijven van Nederland en het merk ESET is wereldwijd vertegenwoordigd. Naast zijn CEO functie bij ESET Nederland, spreekt Maasland vol enthousiasme over de risico's en niet te vergeten, de mogelijkheden die de digitale wereld ons biedt. Op deze wijze wil hij mensen enthousiasmeren en de angst door onwetendheid ontnemen. Dit doet hij ook regelmatig bij actualiteitenprogramma's op TV. Zijn persoonlijke missie is: 'Mensen en bedrijven verder helpen en Nederland, samen met onze partners en eindklanten, op deze manier steeds veiliger maken'.

Top 5 misverstanden

1. Het grootste misverstand is dat de mens de zwakste schakel is

"We moeten stoppen met het simpelweg afschuiven van alle cyberrisico's op de 'mens'. Dat is echt te kort door de bocht. Het echte probleem zit veel dieper: netwerken en systemen zijn vaak nog steeds niet robuust genoeg ontworpen. Cyberaanvallen kunnen alleen succesvol zijn als ze door meerdere lagen van onvoldoende beveiliging kunnen breken. Training en awareness zijn nuttig, maar die hebben pas echt impact als we eerst focussen op het bouwen van intrinsiek veilige systemen en netwerken. Dan pas kunt u van mensen verwachten dat ze met kennis van zaken bijdragen."

2. Cyberrisico's gaan alleen over cyber

"Ondanks dat cybersecurity belangrijk is, is dat slechts één van de vele risico's waarmee ondernemers te maken hebben. Het is cruciaal om cyberrisico's te vertalen naar echte business impact. Uiteindelijk gaat het erom dat we cybersecurity zien als een onderdeel van het bredere risicomanagement binnen een organisatie. Als dat lukt, gaat cybersecurity op in de strategische bedrijfsvoering en dat is precies wat nodig is."

3. Cybersecurity is alleen een verzekering

"Veel mensen zien cybersecurity als een verzekering, maar dat is een beperkte visie. Cybersecurity moet juist worden gezien als een manier om sneller te innoveren en met vertrouwen te kunnen opereren. Zo kan een goede cyberstrategie een bedrijf juist helpen om sneller en veiliger te groeien. Het gaat erom technologie strategisch in te zetten en de bijbehorende risico's proactief te beheersen, zodat het bedrijf sneller en sterker kan innoveren."

4. Cyberrisico's aanpakken vereist een compleet nieuwe expertise
"Het klopt dat cyberrisico's specifieke kennis vereisen, maar we moeten vooral kijken naar integratie. Cybersecurity zou onderdeel moeten worden van de bestaande kwaliteitsprocessen en frameworks. Heeft u al een kwaliteits-managementsysteem? Voeg cyber eraan toe. Heeft u al vergaderingen over risico's? Zet cybersecurity op de agenda. Zo maakt u cybersecurity onderdeel van de dagelijkse bedrijfsvoering, zonder dat u het als een compleet nieuwe uitdaging ziet."

5. "Ik ben geen techneut, dus ik begrijp niets van cyberrisico's"
"Cyberrisico's gaan niet meer alleen over IT. Het gaat om de rol van technologie binnen het bedrijf en de strategische keuzes die gemaakt worden. U heeft als ondernemer juist een belangrijke stem in de richting die uw bedrijf opgaat en welke doelen u nastreeft. Slimme mensen om u heen kunnen helpen de technische risico's te beperken. Uiteindelijk gaat het erom dat u cybersecurity ziet als onderdeel van de bredere bedrijfsvoering, niet als iets wat losstaat van de rest van de organisatie."

Vertrouwen herstellen is lastiger dan systemen herstellen | een voorbeeld

Onze adviseurs horen vaak 'dat overkomt mij niet'. Toch werd ook een typisch MKB-bedrijf (een accountantskantoor met zo'n 20 medewerkers) recent slachtoffer van een ransomware-aanval. Criminelen versleutelden alle bedrijfsdata, inclusief de zeer gevoelige informatie van hun klanten. Denk hierbij aan financiële overzichten, belastingaangiften en zelfs persoonlijke gegevens van eigenaren. Het grootste probleem? Hun back-up bleek niet goed te functioneren. Alle data was nu in handen van de criminelen, en het bedrijf had geen toegang meer tot hun eigen systemen. Twee weken lang lagen hun digitale processen stil, waardoor ze klanten niet konden bedienen en hun reputatie een flinke klap kreeg. Dit soort aanvallen kan bij elk MKB gebeuren en het herstellen van vertrouwen is vaak nog moeilijker dan het herstellen van de systemen.

In het nieuws komen vaak de cyberaanvallen bij grote bedrijven aan bod. Maar ook binnen onze MKB-klantenkring maken we helaas cybercriminaliteit mee. Het kan echt ieder bedrijf overkomen. Bekijk hier nog meer voorbeelden.

Welke soorten cybercrime zijn er?

Cybercriminaliteit kent veel vormen en is daarom moeilijk aan te pakken. We benoemen zes soorten cybercrime die regelmatig voorkomen bij bedrijven.

Hacken

Het platleggen of misbruiken van uw website of computernetwerk. Hierdoor kunnen persoonlijke gegevens achterhaald worden, maar bijvoorbeeld ook illegale bestanden op uw netwerk worden opgeslagen.

Hoe herkent u deze vorm?

- Uw computer is merkbaar trager.
- Bepaalde programma's werken niet meer.
- Namen van mappen en bestanden zijn plotseling gewijzigd of verdwenen.
- Er staan bestanden op uw computer waar u niets van weet.

Ransomware

Uw systemen en/of bestanden zijn geblokkeerd en er wordt geld gevraagd om de computer weer te 'bevrijden'.

De tip van Zicht

Krijgt u een melding dat u een openstaande rekening of boete moet betalen om weer bij uw bestanden te kunnen? Dit gaat waarschijnlijk om ransomware. Niet doen dus! Het is namelijk helemaal niet zeker dat u na betaling weer overal toegang toe heeft. Bovendien beloont u daarmee de criminelen en wordt het probleem in de toekomst alleen maar erger. Doe wel altijd aangifte bij de politie.

Phishing

Met valse e-mails of berichten probeert iemand uw persoonlijke gegevens te krijgen. Hierbij wordt geprobeerd uw creditcardgegevens te achterhalen of uw wachtwoorden om in te loggen bij bijvoorbeeld uw online bankomgeving.

Hoe herkent u deze vorm?

- Er wordt gevraagd om uw creditcardnummer en de CVC/CVV-code en/of uw verificatiecode.
- Er wordt gevraagd om uw pincode of inloggegevens.
- Er wordt gevraagd om uw gegevens via een link op een website.
- Uw mailprovider of spamfilter heeft een indicatie van ‘spam’ gegeven.

Identiteitsfraude

Misbruiken van uw persoonlijke gegevens. Onder uw naam worden bijvoorbeeld producten besteld, betalingen gedaan of creditcards aangevraagd.

Hoe herkent u deze vorm?

- Er zijn betalingen gedaan met uw creditcard door een onbekende partij en zonder uw toestemming.
- Uw klanten ontvangen e-mails die u niet verstuurd heeft.
- U ontvangt rekeningen van producten die u nooit besteld heeft.
- Er staan bestanden op uw computer waar u niets van weet.

DDoS-aanvallen

DDoS staat voor Distributed denial-of-service. Doordat een groot aantal computers een website of internetdienst opvraagt, raakt de server overbelast en is de website of dienst niet meer bereikbaar voor normale internetgebruikers.

Hoe herkent u deze vorm?

- Het netwerk is ongebruikelijk traag.
- Bepaalde websites zijn niet beschikbaar of het lukt niet om ze te bezoeken.
- Een drastische toename van spamberichten.

Menselijke fout

Een medewerker kan, al dan niet opzettelijk, (een onderdeel van) een computersysteem of data die persoonsgegevens bevatten verliezen. Of een boze oud-medewerker kan bijvoorbeeld moedwillig belangrijke gegevens verduisteren of een opening in het systeem publiceren.

Wat kunt u zelf doen?

Cybercrime is nooit 100% te voorkomen. Maar de kans dat het u overkomt beperken is wel mogelijk. Maak, in samenwerking met een ervaren online beveiligingsspecialist, een risicoanalyse. U weet dan welke onderdelen van uw bedrijfsvoering een potentieel risico voor cybercrime vormen. Denk aan desktops, laptops, smartphones en tablets, e-mail, internettoegang en databases.

Datarisicoanalyse

Stel uzelf deze vragen

- 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 naar 'losse' producten, ook naar geïntegreerde oplossingen. Die zijn vaak voordeliger, overzichtelijker en veiliger.
- Zijn uw medewerkers op de hoogte van de risico's van cybercriminaliteit en datalekken?

Goed om te weten

- Via beschermjebedrijf.nl heeft u binnen enkele minuten inzicht hoe het zit met de beveiliging van uw informatie.
- Zorg voor een helder internet- en e-mailbeleid.
- U kunt zelf ook meer bewustzijn creëren bij uw werknemers. Stimuleert u bijvoorbeeld het gebruik van sterke wachtwoorden?

Aanpak van cybercrimerisico's in 4 stappen

In 4 stappen kunt u het cyberrisico beperken.

Stap 1. Maak de organisatorische maatregelen inzichtelijk

In de meeste gevallen is cybercriminaliteit nog steeds het gevolg van menselijk handelen. Daarom is het verstandig organisatorische maatregelen te treffen. Maak inzichtelijk wat het beleid is en welke procedures er gelden. Zorg dat alle medewerkers hiervan op de hoogte zijn, bijvoorbeeld door een training te geven.

Stap 2: Breng de technische maatregelen in kaart

Om een sterk front te vormen tegen cyberrisico's is het belangrijk de juiste balans te vinden tussen organisatorische en technische maatregelen. Breng de risico's en kwetsbaarheden van uw IT-omgeving in kaart. Door dit te doen, kunt u deze tijdig aanpakken en uw IT-beveiliging naar een hoger niveau tillen.

Stap 3: Voer de maatregelen ook echt door

U weet welke acties u nog moet ondernemen. Essentieel is dat u deze wijzigingen daadwerkelijk doorvoert. Denk bijvoorbeeld aan

- medewerkers voorlichting geven over potentiële risico's.
- medewerkers informeren dat het 'zomaar' klikken op links in e-mails risicovol is.
- zorgen dat uw medewerkers regelmatig hun wachtwoorden wijzigen en stimuleer het gebruik van sterke wachtwoorden.
- een beveiligingsproduct kiezen dat goed bij uw bedrijf past én overzichtelijke en begrijpelijke rapportages geeft.
- regelmatig evalueren of de gekozen beveiligingsoplossing past nog bij uw huidige én de toekomstige situatie.

Stap 4: Sluit een passende cyber- en datariskverzekering af

Snel en doelgericht reageren op dataverlies, hackers of cyberaanvallen beperkt de schade. Een cyber- en datariskverzekering 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 om uw databases en websites te repareren, belanghebbenden te informeren en het juridische traject op te starten. En uw eigen kosten? Die zijn gedekt.

Onderzoek cyberrisico onder ondernemers

Tijdens de gesprekken met onze klanten horen we vaak 'dat overkomt mij niet'. Of 'ik ben daar te klein en niet interessant voor'. Toch blijkt de praktijk anders. We hebben daarom 138 ondernemers gevraagd onze cybertest in te vullen om te kijken of ze een verhoogd cyberrisico liepen. De belangrijkste resultaten vindt u hieronder.

Gevolgen van verdwenen data

66% weet wat de gevolgen van verdwenen data zijn, 34% heeft geen inzicht of weet het niet.

> ***Conclusie***
> Veel ondernemers weten niet wat de gevolgen zijn van verdwenen data. Het is belangrijk om dit inzichtelijk te maken en daar beleid op te maken of aan te passen.

Gevolgen bij datalek

Bij 40% is niet inzichtelijk wat er moet gebeuren als er een datalek plaats vindt. Het uitvoeren van de juiste acties beperkt niet alleen de risico's, maar voorkomt ook een hoge boete.

> ***Onze tip***
> Maak hier beleid voor, zorg dat uw medewerkers op de hoogte zijn en zorg dat zo snel mogelijk na een datalek de juiste acties worden ondernomen.

Software up-to-date

Bij 88% van de bedrijven is de software altijd up-to-date. Een mooi resultaat, maar dat betekent dat 12% van de bedrijven hier risico's lopen. Hoe heeft u dit geregeld?

Privé e-mail

Een kleine meerderheid (52%) geeft aan beleid op te hebben gesteld over het openen van privé e-mail op het bedrijfsnetwerk of computers. Terwijl dit een van de grootste risico's is voor een datalek.

Thuis werken

62% geeft aan dat voor werken vanuit huis organisatorische en technische maatregelen zijn getroffen. Een belangrijk onderwerp nu veel medewerkers thuiswerken.

Wachtwoordbeleid

Bij 77% van de bedrijven moeten medewerkers regelmatig hun wachtwoord wijzigen en kiezen voor sterke wachtwoorden. 23% heeft nog een belangrijke stap hierin te zetten.

Ook weten of uw bedrijf een verhoogd risico loopt?
Doe de Zicht cybertest op www.zichtadviseurs.nl/cybertest

Cybercrimeverzekering

Zoals eerder aangegeven, 100% voorkomen dat u getroffen wordt door cybercriminaliteit kunt u nooit. Als het u overkomt, is het wel fijn als u terug kunt vallen op een verzekering die u snel op gang helpt. Want hoe langer u stil ligt, hoe groter de gevolgen kunnen zijn. En dan hebben we het nog niet over het werk dat het met zich mee brengt. Weet u wat u moet doen?

Als u een cybercrimeverzekering heeft, dan staat er een team van ervaren professionals voor uw klaar. Zij helpen u om uw databases en websites te repareren. Maar ook om belanghebbenden te informeren en het juridische traject op te starten.

Dekking

Met een cyberverzekering bent u verzekerd van de dekking* van de volgende kosten:

- forensisch onderzoek
- communicatie met providers, klanten, toezichthouders, justitie, creditmaatschappijen en andere belanghebbenden
- crisismanagement, reputatieherstel en PR-campagnes
- extra klantondersteuning, bijvoorbeeld via een call center
- onderzoek en advies in systeembeveiliging
- betaald losgeld

Maar u heeft ook dekking voor:

- hulp van een security-adviesbureau
- compensatie omzetverlies in uw online- en offline verkoop
- reparatie, vervanging of herstel van websites, programma's of data
- kosten van gestolen software of data
- kosten claims individuele personen
- kosten boetes opgelegd door toezichthouders of andere verplichte vergoedingen
- kosten schade als uw website of e-mail onbedoeld het auteursrecht schendt, laster verspreidt of een virus bevat

** afhankelijk van de situatie*

Cybercrimeverzekering afsluiten of persoonlijk advies?

Ook u kunt de dupe worden van cybercriminaliteit. Daarom is ons advies: ga in gesprek met uw adviseur om de risico's voor uw bedrijf te analyseren en een passende oplossing voor te stellen.

Heeft u een concrete cybervraag of bent u benieuwd wat de adviseurs van Zicht voor u kunnen betekenen? Vul dan het formulier op www.zichtadviseurs.nl/cyber-bewust in en één van onze adviseurs neemt binnen 1 werkdag contact met u op.

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 vestigingen door heel Nederland adviseren onze 450 deskundige medewerkers u graag.

Z.WP.cyber.1024