avéro | achmea

Uw gids in het land van cybersecurity

Whitepaper cyber

Cybersecurity een moeilijk onderwerp? In deze whitepaper hebben we alle ins en outs voor u op een rij gezet. De risico's van cybercrime maar natuurlijk ook de oplossingen. Zo heeft u alle kennis bij de hand om uw relatie goed te kunnen adviseren.

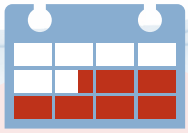
In deze whitepaper

Feiten en cijfers

Wist u dat jaarlijks ongeveer 50% van de bedrijven met meer dan 10 werknemers te maken krijgt met cyberincidenten? Dit blijkt uit onderzoek van het CBS. Gelukkig begint het thema binnen het midden- en kleinbedrijf steeds meer te leven. Even wat feiten en cijfers op een rij.

Van alle ondernemers denkt **43%** dat zijn bedrijf niet interessant is voor cybercriminelen

Toch krijgt **50%** van alle ondernemers met meer dan 10 medewerkers te maken met cyberincidenten



Gemiddeld ontdekken bedrijven pas na een **halfjaar** dat ze zijn gehackt

De economische schade per incident bedraagt **78.700 euro**

De schade door cyberincidenten op jaarbasis voor het mkb is **een miljard euro**

Voor het hele Nederlandse bedrijfsleven is dat nog **10 keer** zoveel

Slechts **23%** maakt zich zorgen over zijn digitale veiligheid

In 2017 werden **10.000** datalekken gemeld

20% van de ontvangers klikt weleens op phishing-links in e-mails

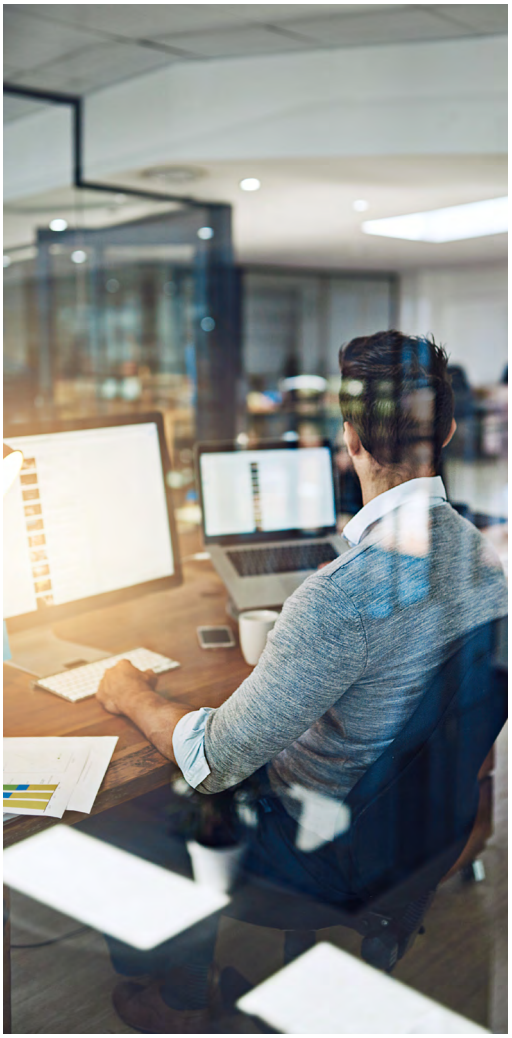
Bronnen:
- Cybersecuritymonitor 2018 van het CBS
- Cybersecurityonderzoek 20108 van Centraal Beheer
- Onderzoek Kantar_TNS_Interpolis-Cybersecurityrapport 2017

Valkuilen en risico's van cybercrime

Cybercrime is meestal niet specifiek gericht

Veel ondernemers denken: "Wie wil mij nu hacken? Ik ben toch helemaal niet interessant?" Of: "Mijn bedrijf heeft maar een bescheiden omzet. Dus er valt toch niks te halen?". Maar niets is minder waar. Dit zijn de grootste misverstanden over cybercrime.

Iedereen die geld heeft, is interessant voor cybercriminelen. Dat hoeven echt geen tonnen te zijn. Zelfs particulieren met alleen een AOW zijn doelwit voor internetcriminelen. Kortom: iedereen is een potentieel doelwit van cybercrime. Dus ook consumenten, zzp'ers en zéker het mkb. We zetten wat voorbeelden voor u op een rij.



Met phishing worden veel wachtwoorden gestolen
Phishing is precies wat het woord zegt: hengelen. Alleen hengelt een cybercrimineel niet naar vis, maar naar wachtwoorden. Uw relatie krijgt ermee te maken als een medewerker per ongeluk op een verkeerde link klikt. Zulke phishing-links zitten verstopt in e-mails. Dat zijn vaak e-mailberichten die lijken op die van de bank, of een andere vertrouwde instantie. Er staat een link in die de hacker bijvoorbeeld toegang geeft tot inloggegevens voor internetbankieren. Hoewel phishing al jaren bestaat en door de overheid onder de aandacht wordt gebracht van consumenten, klikt nog altijd zo'n 20% van de ontvangers op dergelijke schadelijke links.

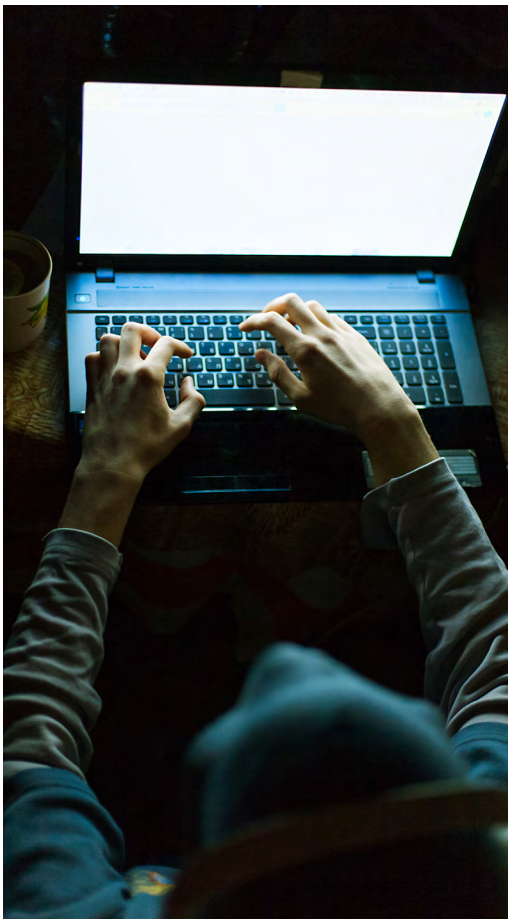
CEO-fraude richt ook schade aan bij Nederlandse bedrijven
Een andere manier van phishing blijkt ook succesvol: CEO-fraude. Alleen vragen de criminelen daarbij niet om op een link te klikken, maar gewoon om geld over te

maken. Dat doet natuurlijk niemand, zou je zeggen. Maar dat is helaas niet zo. De mails lijken namelijk afkomstig van de directeur. Vandaar de naam CEO-fraude. Ze zijn gericht aan een medewerker die wordt gevraagd om met spoed geld over te boeken naar een bekend bedrijf. De mails spelen in op de angst van de medewerker om iets fout te doen. Om de directeur niet te gehoorzamen. Dus maken ze het gevraagde bedrag over. Alleen het rekeningnummer is niet van het bekende bedrijf, maar van de hacker bij een bank in een ander land. En zie dat geld maar eens terug te krijgen.

Online apparatuur en gadgets zijn kwetsbaar
Veel ondernemers weten niet dat ze online apparaten in hun netwerk hebben. Dat komt doordat werknemers tegenwoordig zelf van alles kunnen koppelen via wifi. Denk maar eens aan een internetradio. Of aan een tablet waar thuis de kinderen mee spelen. Maar ook het bedrijf zelf gebruikt bijvoorbeeld beveiligingscamera's waarvan je online de beelden kunt monitoren. Of een alarmsysteem dat meldingen stuurt naar een app op je telefoon. Al die apparaten maken gebruik van netwerkverbindingen. En die zijn niet allemaal even veilig. Zulke apparatuur is een makkelijke ingang voor hackers. Moeten we ze dan maar niet gebruiken? Nee, zo is het ook niet. Online apparatuur is niet meer weg te denken uit het bedrijfsleven. Maar goede beveiliging is wel heel belangrijk. Het is daarom aan te bevelen een goede partij in de arm te nemen die ook dit soort risico's kan beveiligen.

Ook cyberspionage komt voor in het mkb
Het klinkt bijna als een James Bondfilm, maar het is echt waar. Waarschijnlijk niet direct, maar zeker indirect. Zogenaamde dataminers behoren tot de slimste jongetjes van de klas. Ze 'delven' naar data, hoe meer hoe beter. En tussen al die gegevens leggen ze verbanden. Wachtwoorden van medewerkers van grote technologiebedrijven zijn een hoop geld waard. Die zijn

dan ook optimaal beveiligd. Maar die medewerkers kopen weleens iets online, op de website van een mkb-bedrijf. Als ze daarbij hetzelfde wachtwoord gebruiken als op hun werk, dan zit dat wachtwoord dus ook in het relatiebestand van die ondernemer. Daarom is elk willekeurig bestand interessant en in potentie waardevol voor internetcriminelen. Ook de bestanden van uw relatie. Door zoveel mogelijk data aan elkaar te koppelen, kunnen ze bovendien complete profielen samenstellen. Van soms wel miljoenen nietsvermoedende mensen. En die profielen verkopen ze door. Aan criminelen die zich bezighouden met identiteitsfraude, bijvoorbeeld. Zo is het mogelijk dat het hacken van een vooraanstaande multinational begint met een databestand afkomstig van uw relatie.



Internetcriminaliteit is inventief en onvoorspelbaar

Misschien is het een sombere conclusie, maar het is helaas niet anders. Internetcriminelen zijn slim. Ze delen hun kennis en bedenken steeds weer nieuwe trucs om bedrijven op te lichten. Is daar dan helemaal niks tegen te doen? Gelukkig wel. Daarover gaat de rest van deze whitepaper.

10 tips om uw relaties te adviseren over cybersecurity

1 **Maak ondernemers cyberbewust**
Er bestaan 2 soorten bedrijven, zeggen experts. Bedrijven die met cyberincidenten te maken hebben gehad. En bedrijven die er nog mee te maken krijgen. Laat uw relaties zien wat de risico's zijn.

2 **Ontdek waar uw klanten kwetsbaar zijn**
Door risico's in kaart te brengen kunt u ondernemers beter adviseren.
Maak samen met uw relatie een lijst van alle bedrijfsmiddelen die zijn verbonden met het internet of die kunnen worden aangesloten op een computer.

3 **Voorkom misverstanden over cybercrime**
De meeste ondernemers denken dat zij niet interessant zijn voor cybercriminelen. Gelukkig zijn zulke misverstanden makkelijk op te helderen. En met de juiste informatie kan uw relatie beter beslissen over het belang van cybersecurity in zijn bedrijf.

4 **Zorg voor een slot op de deur**
Cybercriminelen zijn uit op financieel gewin. Een klantenbestand bijvoorbeeld kan veel waard zijn. Adviseer uw relaties zich te beschermen met een goede firewall.

5 **Houd virussen buiten de poort**
Een virus kan computers onbruikbaar maken. Of gegevens stelen. In het ergste geval krijgt een hacker er toegang mee tot het netwerk van uw relatie. Met een robuuste antivirusoplossing houdt uw relatie dat gevaar buiten de deur.

6 **Benadruk het belang van beheer**
Computers, laptops, tablets en telefoons hebben onderhoud nodig. Waarom? Omdat criminelen steeds weer nieuwe manieren ontdekken om ze te hacken. Door altijd de nieuwste software en updates te installeren, maken cybercriminelen veel minder kans.

7 **Let op verborgen risico's**
Ondernemers weten vaak niet waar de gevaren schuilen. Behalve computers, laptops en telefoons zijn ook andere apparaten doelwit van hackers. Denk maar eens aan alarmsystemen, camera's of een internetradio. Onderschat het risico van online apparatuur niet.

8 **Laat uw klanten altijd aangifte doen**
Cybercriminelen denken dat niemand ze wat kan maken. En zelfs al ontspringen ze de dans, aangifte doen maakt een groot verschil. U helpt er de opsporingsdiensten mee. En dus ook andere ondernemers. Bovendien is het belangrijk voor een eventuele verzekeringsclaim.

9 **Adviseer uw klanten back-ups te maken**
Betrouwbare backupsoftware is onmisbaar als er toch iets misgaat. Met een degelijke back-up strategie kan uw relatie dankzij de back-up vaak dezelfde dag weer gewoon verder met zijn bedrijf.

10 **Ga het gesprek over cyber niet uit de weg**
Het is misschien niet het makkelijkste gesprek, maar mogelijk wel het belangrijkste. Het gaat ten slotte om de continuïteit van het bedrijf van uw relatie. En als adviseur speelt u daarin een belangrijke rol.

Meer weten?

Wilt u na deze tips nog meer weten over beschermende producten en diensten voor cybersecurity? We hebben al onze diensten en oplossingen voor u samengebracht op een handige overzichtspagina. Maar bedenk wel: cybersecurity is nooit waterdicht. En als schade niet 100% voorkomen kan worden, is het verstandig de gevolgen ervan te beperken. Onze Cyberverzekering dekt financiële schade veroorzaakt door menselijk handelen en cybercrime. Uw relatie is verzekerd voor eigen schade en schade van anderen die door een cyberincident bij uw relatie worden geraakt.

Goed advies was nog nooit zo belangrijk

Cybercriminaliteit is onderdeel van het dagelijks leven. Net zoals inbraak, winkeldiefstal en bedrijfsbrand. Preventie is het beste wapen in de strijd tegen hackers. Want niet iedereen die te maken krijgt met een cyberaanval wordt ook slachtoffer. Bedrijven die hun security goed in de hand hebben, kunnen zelfs de heftigste aanvallen weerstaan. Soms zelfs dagenlang!

Dé waterdichte beveiliging bestaat niet
Toch is zelfs de beste beveiliging geen garantie. 100% security bestaat namelijk niet. Het verschil tussen 80% en 100%, zit in menselijk handelen. En mensen maken fouten. Bedrijven waar security topprioriteit is zoals banken, verzekeraars en internetproviders, hebben zeer strikte regels voor hun personeel. Maar ook daar is menselijk falen niet uit te sluiten. Dat zou een onwerkbare situatie opleveren. Bedrijven en hun medewerkers moeten nou eenmaal kunnen inspelen op onverwachte situaties. Daar is een bepaalde mate van vrijheid voor nodig.

“Niet iedereen die te maken krijgt met een cyberaanval wordt ook slachtoffer”

“100% security bestaat niet”

Als het fout gaat, gaat het vaak goed fout
Bedrijven doen er vaak tientallen jaren over om een naam op te bouwen. Om concurrerend te zijn en blijven investeren ze veel in innovatie. Dat kan allemaal op slag weg zijn, als het noodlot toeslaat. Stelt u zich dit gefictionaliseerde scenario voor:

Een klein ambitieus architectenbureau schrijft zich in voor een opdracht in Rotterdam. Op een prominente plaats aan de haven wil een projectontwikkelaar een toren bouwen met woonwerkfunctie. Het gebouw moet een echte eyecatcher worden met internationale uitstraling. Een unieke kans voor het architectebureautje, want ze waren al een tijd op zoek naar een dergelijke opdracht omdat ze graag internationaal naam willen maken. Dergelijke projecten worden niet zomaar vergund. Daarom werken de vennoten, 3 getalenteerde architecten, dag en nacht aan hun ontwerp. Op de ochtend voor de presentatie in Rotterdam is de laptop van 1 van de partners stuk. Gelukkig heeft hij de presentatie ook op een USB-stick staan. Wat hij niet weet, is dat die stick is besmet met een virus. Op het moment dat hij op kantoor de stick in zijn computer stopt verspreidt het virus zich over het netwerk. Binnen een halfuur zijn alle computers en servers besmet. De 1ste die het merkt is de secretaresse. Als ze haar agenda wil openen, krijgt ze een foutmelding. Daarna gaat het hard. Binnen een paar uur zijn alle bestanden van het bedrijf versleuteld en niet meer te openen. Ook alle bestanden voor het megaproject in Rotterdam. Waar ze maanden aan hebben gewerkt. Een hacker meldt zich met de mededeling dat ze de sleutel kunnen krijgen om hun bestanden weer toegankelijk te maken. Maar dan moeten ze wel eerst 500 euro in Bitcoin overmaken. Ten einde raad gaat het bedrijf overstag. Ze betalen het 'losgeld'. Maar de hacker laat niets meer van zich horen.

Verzekeren is geen overbodige luxe
Het is bijna niet te geloven, maar dit soort praktijken zijn doodnormaal in de wereld van cybercriminelen. De gevolgen laten zich raden. Het is te hopen dat het bedrijf in dit scenario een goede en recente back-up had. Maar zelfs dan kan de presentatie van hun gloednieuwe ontwerp niet diezelfde dag doorgaan. Want een back-up terugzetten kan dagen duren. Maar nog erger is het als ze geen back-up hebben. Dat maakt de kans op een faillissement niet ondenkbaar. En dan is een goede verzekering geen overbodige luxe.

“U kunt de veerkracht zijn om cybercrime het hoofd te bieden.”

Uw rol als adviseur is van groot belang
U kunt de veerkracht zijn die nodig is om het hoofd te bieden aan de gevolgen van cybercrime. Want het gesprek over cyber begint bij u. Bewustwording, informatieverstrekking en inzicht in concrete risico’s en tegenmaatregelen. U kent het bedrijf, u weet uit welke hoek de bedreigingen komen. En wat de gevolgen kunnen zijn. Met andere woorden: u bent allang geen beginneling meer als het om cyber gaat. En daarom bent u de ideale sparringpartner voor uw relatie.

Wij helpen u graag

Als adviseur heeft u bovendien toegang tot uitgebreide documentatie over cybersecurity. Hoe kunt u bedrijven aanzetten tot het back-uppen van hun systemen? En ervoor zorgen dat iedereen grondige securitymaatregelen neemt? Dat lukt alleen als u uw relaties ervan overtuigt dat niemand, ook zij niet, daar nog onderuit komt. En daar helpen we u graag bij.

Bronnen en hulpmiddelen

De 3 grootste misverstanden over cybercrime

Checklist cyberrisico's

Blog cybercriminaliteit

De risico's van IoT

De antivirusoplossing van Avéro Achmea

De back-up oplossing van Avéro Achmea

De Avéro Achmea Kennisbank

Het gesprek met uw relaties over cybercriminaliteit

Alle oplossingen van Avéro Achmea voor cybercrime

Bekijk onze themapagina Cyber voor nog meer interessante informatie.