E-book deel 3

Cybersecurity

Laat ondernemen niet eindigen in ‘Er was eens...’

avéro achmea

In dit E-book

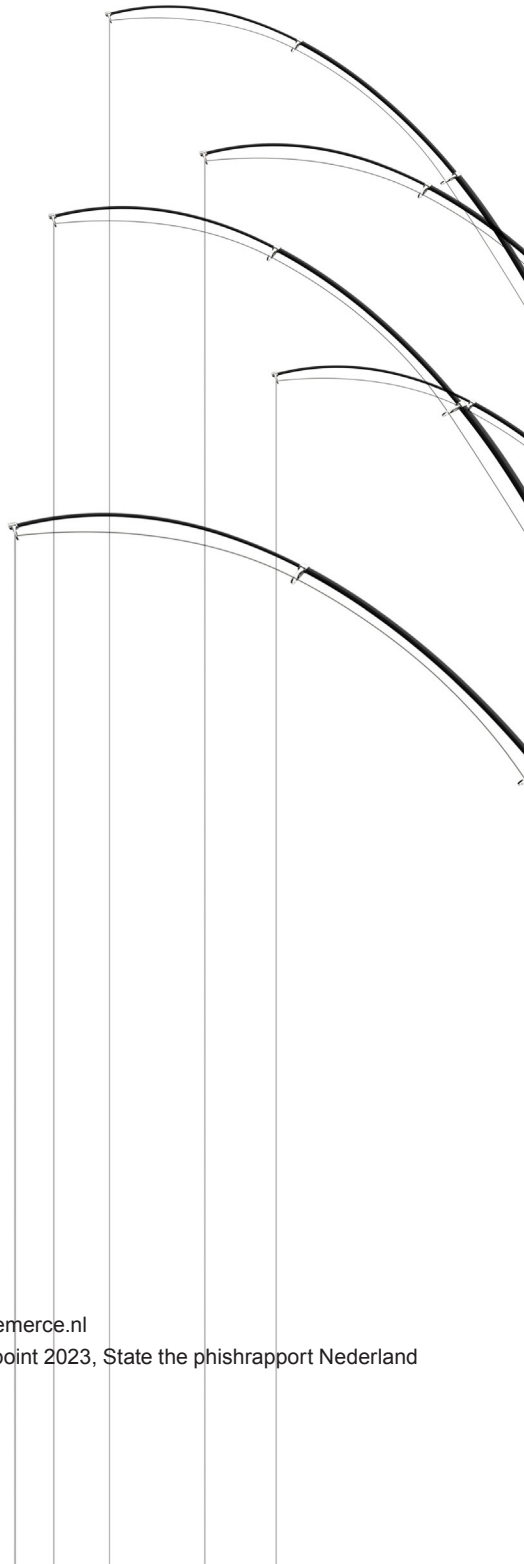
De impact van cybercriminaliteit op het mkb

Vrijwel het hele Nederlandse bedrijfsleven (94%) was in 2023 doelwit van cybercriminelen[1]. In 76% van de gevallen was de aanval bovendien succesvol. Door de razendsnelle ontwikkelingen op het gebied van artificiële intelligentie (AI) worden de aanvallen steeds geraffineerder. In dit e-book zetten we voor u op een rij wat cybercrime betekent voor u en uw relaties.

We spraken met René van Etten, beveiligingsexpert en oprichter van cybersecuritybedrijf Threadstone, over de risico's voor het mkb, de methoden van moderne hackers en Europese wetgeving die bedrijven en organisaties weerbaarder moet maken. Edwin Meinsma geeft als productmanager Cyberverzekering bij Achmea zijn visie op cybercriminaliteit, en hoe u uw relaties kunt helpen hun organisatie te beschermen tegen cybercriminelen. Tim Libanon vertelt over zijn ervaringen als beveiligings-expert en incident handler bij Fox-IT. Het Nederlandse cybersecuritybedrijf is wereldwijd actief en werkt in eigen land onder meer samen met het Ministerie van Defensie en Avéro Achmea.

Het mkb heeft goede onafhankelijke adviseurs nodig

Volgens René van Etten zijn onafhankelijke adviseurs van groot belang om cybersecurity op de agenda van hun relaties te krijgen. "Wij testen voor veel bedrijven de status van hun beveiliging. Een onderdeel daarvan is bijvoorbeeld een phishingmail die we sturen, om te kijken of medewerkers van een bedrijf zich om de tuin laten leiden. Gemiddeld hapt 15 tot 20 procent toe en dat is zorgelijk. We rapporteren de resultaten aan de opdrachtgever en koppelen daar advies aan, of e-learnings om de medewerkers van het bedrijf beter te wapenen tegen de verleidingen van phishing e-mails. Dat levert goede resultaten op, maar we bereiken natuurlijk lang niet het hele bedrijfsleven. Daarom zijn goede adviseurs voor het mkb enorm belangrijk.



[1] www.emerce.nl
Proofpoint 2023, State the phishrapport Nederland

Niet om in de diepte te gaan over cybersecurity, maar om bewustzijn te creëren. Want de schade kan enorm zijn als een medewerker klikt op een linkje in een phishing e-mail."

Ondernemers lopen achter met maatregelen tegen cybersecurity

Ondernemers zetten cybercrime op de 2e plek als het gaat om bedreigingen voor hun bedrijf, onder de krapte op de arbeidsmarkt, en boven inflatie en schaarste van grondstoffen. 62% van de mkb'ers in de dienstensector ziet cybercrime als een groot risico, net als 45% van de ondernemers in de industrie. Toch geeft slechts 27% van het mkb aan dat de beveiliging tegen cybercrime hoog op de agenda staat. Maar liefst 55% van de zelfstandige mkb-ondernemers zegt zelfs helemaal geen maatregelen te nemen tegen cybercriminaliteit, en 31% van de mkb'ers wint geen advies in over risico's[2].

Van Etten: "In mijn ervaring zijn daar een paar redenen voor. Ten eerste horen bedrijven wel over de risico's, maar ze denken vaak: 'Dat overkomt mij niet, want ik heb alles goed geregeld.' Dit wordt ook wel de 'optimisme bias' genoemd. Men denkt dat het anderen overkomt, maar niet henzelf. De achterliggende reden is dat bedrijven denken dat een paar basismaatregelen wel genoeg zijn. Of ze hebben de beveiliging uitbesteed en denken er verder niet meer over na. Wat we ook nog steeds vaak horen: 'Ik werk met Mac, dus ik ben veilig.' Of 'Ik ben geen potentieel slachtoffer, daarvoor zijn wij niet interessant genoeg, of groot genoeg.' Dat blijft een hardnekkige misvatting, want het grootste deel van de cybercriminelen gaat helemaal niet gericht te werk. Die hackers schieten met hagel en zien wel wat er uit de lucht komt vallen."

"Het grootste deel van de cybercriminelen gaat niet gericht te werk. Die hackers schieten met hagel en zien wel wat er uit de lucht komt vallen."

René van Etten

[2] Nationale Monitor Risicomanagement MKB 2023, Universiteit Twente & Avéro Achmea

Alle mkb'ers zijn doelwit van criminelen

"In tegenstelling tot wat veel mensen denken, zijn alle mkb-bedrijven doelwit van cybercriminelen", vertelt Tim Libanon van Fox-IT. "Als de beveiliging niet optimaal is, worden ze slachtoffer van willekeurige aanvallen. Denk bijvoorbeeld aan scripts die geautomatiseerd het internet afzoeken naar systemen die niet tijdig zijn bijgewerkt om een beveiligingslek te dichten. Elke keer als het script zo'n systeem vindt, zullen de hackers proberen het te infiltreren. En omdat ze precies weten waar de kwetsbaarheid zit, lukt dat veel te vaak."

> **"Hackers doen zich aan de balie voor als leverancier, of als onderhoudsmonteur, en als ze eenmaal binnen zijn proberen ze een systeem te manipuleren zodat ze er van afstand bij kunnen."**
>
> Tim Libanon

Hoewel veel ondernemers zich liever niet bezighouden met maatregelen om de cybercriminaliteit te voorkomen, zijn er volgens Van Etten toch 3 momenten waarop bedrijven wél in actie komen om hun beveiliging te verbeteren.

- Na een cyberaanval: "Als ze al gehackt zijn, is het natuurlijk al te laat. Maar het kan wel een wake-up call zijn om de beveiliging te verscherpen."
- Als de wetgever het verplicht: "De Algemene Verordening Gegevensbescherming is een voorbeeld van een wet die bedrijven verplicht om maatregelen te nemen om persoonsgegevens te beschermen. De AVG geeft een uniforme set regels voor de veilige verwerking van persoonsgegevens in de hele EU, waar elk bedrijf zich aan moet houden."
- Als klanten of partners ernaar vragen: "Grote bedrijven, corporaties en enterprises, eisen steeds vaker van hun leveranciers dat ze aantoonbaar goed omgaan met cybersecurity. Dit kan een sterke motivatie zijn voor bedrijven om hun beveiliging te verbeteren."

Ketenverantwoordelijkheid brengt kansen voor mkb én adviseurs

Bedrijven die kunnen aantonen dat ze hun cybersecurity goed op orde hebben, hebben een streep voor op hun concurrenten. Het versterkt hun reputatie en helpt bij het aantrekken van nieuwe klanten. “Dat hangt samen met Europese wetgeving die eraan zit te komen”, legt Van Etten uit. “De Europese richtlijn NIS2 verplicht grotere partijen om bij hun leveranciers te controleren hoe zij de informatie-beveiliging regelen. Daarmee legt de wetgever de nadruk op ketenverantwoordelijkheid. Veel grote partijen werken al zo, maar binnenkort vallen nog veel meer bedrijven onder deze richtlijn, en dat gaat het mkb zeker merken. Als toeleverancier moet je dan aantonen dat je cyber-security en databeveiliging goed geregeld zijn. Dat is geen kleine opgave, maar als je kunt laten zien dat je het goed doet, kun je daar nieuwe klanten mee aantrekken. We zien op dat punt al dingen gebeuren in de markt. Zo waren er toeleveranciers van een grote supermarktketen, die vertelden: ‘We moeten van de supermarkt aan de NIS2-regeling voldoen en laten zien hoe we ervoor staan. Maar we weten eigenlijk nog helemaal niet waar we staan op dit moment, dus kunnen jullie een nulmeting uitvoeren? Dat is wetgeving die een enorme impact gaat hebben op de markt. Bedrijven moeten hun cybersecurity echt serieus gaan nemen, willen ze een plek in de markt houden.”

Europese richtlijn raakt straks vrijwel alle bedrijven

Als adviseur kunt u uw relaties wijzen op de kansen die dit voor hen met zich meebrengt. Een positie als preferred supplier voor een grote organisatie komt een stuk dichterbij als uw relatie de beveiliging op orde heeft. De NIS2-richtlijn biedt daarbij houvast. Die heeft tot doel om de weerbaarheid van bedrijven te verbeteren. Zij krijgen te maken met een aantal verplichtingen, zoals:

- Risicobeoordeling: Organisaties moeten periodiek een risicobeoordeling uitvoeren om vast te stellen welke gevaren hun systemen en diensten bedreigen.

- Technische en organisatorische maatregelen: Op basis van de risicobeoordeling moeten passende maatregelen worden genomen om de risico's te beperken. Dit kan gaan om technische maatregelen, zoals firewalls en encryptie, maar ook om organisatorische maatregelen, zoals bewustwordingstrainingen voor medewerkers.
- Meldplicht incidenten: Ernstige incidenten die de dienstverlening verstoren, moeten binnen 24 uur gemeld worden bij de toezichthouder.
- Toezicht: Organisaties worden gecontroleerd door een onafhankelijke toezichthouder op naleving van de richtlijn.

Wanneer organisaties zich niet houden aan de richtlijn, kunnen ze boetes krijgen, oplopend tot 2% van de (wereldwijde) jaaromzet.

Als adviseur kunt u uw relaties wijzen op de impact van de NIS2-richtlijn, bijvoorbeeld door te verwijzen naar deze websites van de overheid:
- Wat is de NIS2-richtlijn?
- Wat gaat de NIS2-richtlijn betekenen voor uw organisatie?

Beveiliging begint met het identificeren van kwetsbaarheden

"Wij adviseren onze klanten altijd om hun beveiliging goed te laten doorlichten", vertelt Libanon. "Daarvoor maken we analyses van hun netwerken en systemen, om kwetsbaarheden te identificeren. Onze hackers proberen dan vervolgens of ze binnen kunnen komen. Als de klant dat wil, kijken we zelfs of we de organisatie fysiek kunnen infiltreren. Komen we voorbij de balie en kunnen we dan ergens toegang krijgen tot een systeem? Zo werken hackers ook, en daar zijn ze bijzonder creatief in. Ze doen zich voor als leverancier, of als onderhoudsmonteur, en als ze eenmaal binnen zijn proberen ze een systeem te manipuleren zodat ze er van afstand bij kunnen. Als dat lukt, hebben ze in wezen vrij spel om te doen wat ze willen."

Cybercriminaliteit loont

Criminelen gebruiken geautomatiseerde systemen om zwakheden in de beveiliging van een bedrijf te vinden en zo hun slag te slaan. Cybercriminaliteit is een goed georganiseerd businessmodel geworden waar veel geld in omgaat. Printerfabrikant Hewlett Packard berekende dat in 2023 de schade door cybercriminaliteit wereldwijd 8 biljoen dollar bedroeg, ofwel 7.338.280.000.000 euro. Dat is bijna 8 keer zoveel als het bruto binnenlands product van Nederland.

Phishing is de meest voorkomende vorm van cybercriminaliteit

Bij phishing proberen hackers om gevoelige informatie los te krijgen van het slachtoffer. In e-mails, sms-berichten en tegenwoordig ook steeds vaker telefoongesprekken doen ze zich voor als een persoon, bedrijf of een instantie die het slachtoffer vertrouwt. Zo proberen ze gebruikers-namen en wachtwoorden los te krijgen, of andere informatie die ze kunnen gebruiken. Professionele criminelen richten zich vaak op het installeren van malware op de systemen van slachtoffers. Door de inzet van kunstmatige intelligentie (AI) wordt phishing steeds moeilijker te herkennen.

Onderzoeken wat afwijkt van het normale

Binnen het Security Operations Centre (SOC) van Fox-IT worden aanvallen van hackers op de voet gevolgd. Tim Libanon: “Vanuit het SOC monitoren we netwerken en systemen van klanten. Dat monitoren is een soort constante speurtocht naar alles wat afwijkt van het normale. Gebeurt er iets vanaf een onbekend systeem, of vanaf een systeem dat normaal gesproken niet bij een proces betrokken is? Dan is de vraag meteen of dat wel oké is. We melden het incident bij de klant, die dan kan aangeven of het incident legitiem is of niet. Soms blijkt na onderzoek dat een medewerker onbekend is met een bepaalde procedure en iets in gang heeft gezet waardoor bij ons – als afwijking van het gangbare – een belletje afgaat.”

> “Als je zo’n incident volgt, dan zie je hoe een hacker te werk gaat, op zoek naar waardevolle data, of naar manieren om een organisatie te chanteren.”
>
> Tim Libanon

“Maar vaak is het ook wél raak”, vertelt Libanon. “Dan probeert een crimineel binnen te komen in een systeem. Als de oorzaak niet meteen duidelijk is, kan onze forensische afdeling alle beschikbare data analyseren om een oorzaak te achterhalen. Wat is er gebeurd, wat is de mogelijke impact, wat kunnen we doen om het lek te dichten?”

“Als je zo’n incident volgt, dan zie je hoe een hacker tewerk gaat om zijn toegang uit te breiden. Want het doel is natuurlijk niet die ene machine. Criminelen zijn op zoek naar waardevolle data, of naar manieren om een organisatie te chanteren. Bijvoorbeeld door ransomware te installeren en alle bedrijfsgegevens onbruikbaar te maken. Met die kennis, is de juiste reactie om alles stil te leggen en te zoeken naar het lek. Alles om te voorkomen dat de hacker zijn doel bereikt. Maar kan dat wel? Veel organisaties hebben verplichtingen die hen verhinderen tijdelijk buiten bedrijf te zijn. Daarom adviseren we bijvoorbeeld om netwerken op te delen in segmenten. Dan kun je dat deel waar de hacker actief is, afsluiten van de rest zonder dat het bedrijf helemaal stil komt te liggen.”

De grootste schade ontstaat door ransomware

De meeste slachtoffers vallen door zogenaamde ransom-software. Dat is een stukje software dat alle bestanden van een bedrijf met encryptie versleutelt, zodat het bedrijf er geen toegang meer toe heeft. Dat heeft grote gevolgen voor de bedrijfscontinuïteit. Het bedrijf kan zelfs volledig stil komen te liggen. Onderzoeken bevestigen deze trend[3] en organisaties besteden steeds meer aandacht aan dit probleem. IT-bedrijven spelen hierop in door betere beveiligingsproposities te ontwikkelen.

[3] www.dutchitchannel.nl
Helft van de malware bij mkb’ers zijn keyloggers, spyware en stealers

“In 9 van de 10 gevallen begint een ransomware-aanval met een phishing e-mail”, zegt Van Etten. “Meestal doordat er geen meervoudige authenticatie wordt gebruikt en doordat medewerkers vaak dezelfde wachtwoorden op verschillende systemen gebruiken. Als 1 systeem gehackt wordt, kunnen hackers diezelfde inloggegevens vervolgens proberen op andere platforms zoals Microsoft 365, of Google clouddiensten. Zodra hackers eenmaal toegang hebben tot een mailbox, kunnen ze ransomware of andere malware verspreiden. Het gevaar wordt nog groter als hackers langere tijd onopgemerkt in de systemen kunnen blijven, waardoor zelfs back-ups onbetrouwbaar kunnen worden. In dat geval kan het bedrijf de schade niet meer herstellen en blijft er maar 1 optie over: losgeld betalen.”

“De zwakke schakel bij phishing, ransomware en social engineering is altijd de mens.”

Edwin Meinsma

Hackers manipuleren slachtoffers met social engineering

Bij social engineering zoekt een hacker naar zwakke punten van zijn slachtoffer om zijn doel te bereiken. Social engineering, ofwel sociale manipulatie, maakt gebruik van menselijke zwakheden om slachtoffers te manipuleren. De hacker speelt in op emoties zoals angst, nieuwsgierigheid, behulpzaamheid en autoriteitsgevoeligheid. Door een gevoel van vertrouwen te creëren of door mensen onder druk te zetten, reageert het slachtoffer niet meer alert. Daar maakt de hacker misbruik van om bijvoorbeeld gevoelige informatie te ontfutselen. Social engineering kent diverse verschijningsvormen, zowel fysiek als digitaal. Enkele veelvoorkomende voorbeelden:

Fysieke social engineering:

- Criminelen doorzoeken afval op zoek naar bedrijfsgegevens of andere gevoelige informatie. Die kunnen dan weer worden gebruikt om het slachtoffer te misleiden.

- De hacker doet zich voor als een betrouwbare persoon, zoals een IT-dienstverlener, om toegang te krijgen tot een computersysteem.
- Mensen die op een openbare plek werken, kunnen het slachtoffer worden van social engineering als een hacker stiekem meekijkt om aan wachtwoorden of andere gevoelige informatie te komen.

Digitale social engineering:

- Criminelen gebruiken social media-profielen om persoonlijke informatie te verzamelen die kan worden gebruikt voor gerichte aanvallen.
- Hackers doen zich voor als een medewerker van een vertrouwd bedrijf of organisatie om het slachtoffer geld te laten over maken of gevoelige informatie te laten delen.
- Hackers sturen gerichte e-mails die lijken te komen van de directie van een bedrijf (CEO-fraude). Daarin staat dan dat de medewerker met spoed een bedrag moet overmaken, omdat het bedrijf anders in de problemen kan komen.

“De zwakke schakel bij phishing, ransomware en social engineering is altijd de mens”, zegt Edwin Meinsma van Achmea. “Ieder bedrijf is kwetsbaar, al was het alleen maar omdat de menselijke factor zo’n grote rol speelt. Er is overal nog altijd een groot gebrek aan bewustzijn over cyberrisico’s. Daar ligt volgens mij een belangrijke taak voor de onafhankelijke adviseur. Ga het gesprek aan over cybersecurity, laat die ondernemers nadenken over hun eigen kwetsbaarheid. Dat hoeft niet ingewikkeld te zijn, geen gesprek over technische zaken, liever niet zelfs. Bewustwording is genoeg, maar tegelijk ook belangrijker dan ooit.”

Lees in hoofdstuk 5 alle tips van Edwin Meinsma en René van Etten om het gesprek over cyberrisico’s aan te gaan.

Criminelen misbruiken zwakheden in systemen van derden

“Bij Fox-IT maken we ons vooral zorgen om de zogenaamde edge devices in de netwerken van onze klanten.”, vertelt Tim Libanon. “Dat zijn apparaten die de toegang regelen tot netwerken, of delen daarvan. Bijna elk bedrijf, hoe klein ook, is afhankelijk van zulke systemen. Hackers richten zich daarom steeds vaker op de

fabrikanten van edge systemen. Ze zoeken naar zwakke plekken in de beveiliging, en als ze die vinden kunnen ze zich bij alle klanten van die leverancier toegang verschaffen. Ook software die wordt gebruikt voor thuiswerkplekken, of om beveiligde verbindingen op te zetten, is steeds vaker doelwit van cybercriminelen. Daarom is het zo enorm belangrijk dat elke update die een leverancier uitbrengt, direct wordt geïnstalleerd. Die updates zijn er vooral om zwakheden in de beveiliging op te lossen, zodat hackers geen kans krijgen."

DDoS-aanvallen brengen de bedrijfscontinuïteit in gevaar

Met een DDoS-aanval proberen cybercriminelen een bedrijf onbereikbaar te maken voor klanten. De afkorting DDoS staat voor Distributed Denial-of-Service attack. Bij zo'n aanval zijn tienduizenden, of zelfs honderdduizenden computers betrokken. Al die computers zijn door de criminelen geïnfecteerd met een stukje software. Dat maakt het mogelijk voor de hackers om al die computers gelijktijdig een website of systeem te overspoelen met aanvragen voor informatie. De site raakt daardoor overbelast, zodat echte klanten er niet meer terecht kunnen. Het doel van zo'n DDoS-aanval is vaak om een bedrijf te chanteren. Pas als er losgeld wordt betaald, stopt de aanval. Vaak komt het bedrijf in kwestie ook in het nieuws door zo'n aanval, en dat is natuurlijk niet best voor de reputatie.

"Over losgeld voor versleutelde data kan vaak onderhandeld worden. Verzekeraars hebben daarvoor specialisten, die precies weten wat je wel en niet moet doen."

René van Etten

Een goede cyberverzekering voorkomt faillissementen

Bedrijven die in grote mate afhankelijk zijn van hun IT-systemen kunnen tegenwoordig eigenlijk niet meer zonder verzekering die de schade van een cyberaanval dekt, zegt Edwin Meinsma. “Zo’n verzekering biedt het bedrijf ook ondersteuning om de schade te beperken. Wij werken bijvoorbeeld met Fox-IT. Die zijn 24/7 beschikbaar om DDoS-aanvallen te stoppen, of versleutelde bestanden terug te krijgen. Helaas is dat lang niet altijd mogelijk, en dan loopt de schade hard op. Niet alleen de eigen schade omdat het bedrijf stil ligt, maar ook schade die kan ontstaan bij derden en waarvoor het bedrijf aansprakelijk kan worden gesteld.”

Bij Avéro Achmea zijn zulke onderhandelingen ook inbegrepen bij de Cyberverzekering voor Bedrijven, net als het beperken van imagoschade en uiteraard kosten voor herstel van schade. De Cyberverzekering dekt bovendien ook andere kosten waar uw relatie mee te maken kan krijgen als gevolg van een cyberincident. Op deze pagina leest u alles over de dekking en voorwaarden van de verzekering.

Het mkb heeft de beveiliging niet op orde

De financiële schade door ransomware is groot

Bijna alle Nederlandse bedrijven (94%) kregen in 2023 te maken met een ransomware-aanval. In 76% van de gevallen lukte het de criminelen om de computersystemen te gijzelen. De meeste bedrijven (52%) kregen na betaling weer toegang tot hun data. 90% daarvan kreeg dankzij een cyberverzekering de toegang tot hun documenten terug. De verzekeraars betaalden het losgeld, of een deel daarvan.[4] Cybercriminaliteit loont dus voor de criminelen, maar kost ondernemers nog altijd handen vol geld, want een geslaagde hack levert een Nederlandse mkb'er gemiddeld nog altijd een schadepost op van 270.000 euro.[5]

Volgens René van Etten zijn aanvallen met ransomware vaak maatwerk: "meestal is het gevraagde losgeld een percentage van de jaaromzet. Zo zorgen de criminelen dat de kans op betaling reëel is. Voor hen is het een business-model, en daarom leveren ze na betaling ook vrijwel altijd de sleutel om de bestanden weer toegankelijk te maken. Als ze dat niet zouden doen, dan zouden bedrijven natuurlijk snel ophouden met betalen." Maar bedrijven verliezen niet alleen geld door het losgeld te betalen. Ook productieverlies, reputatieschade en de kosten van het herstellen van systemen zijn enorme schadeposten voor een bedrijf.

Reputatieschade is voor elk bedrijf een probleem

LockBit is een groep georganiseerde cybercriminelen die veel slachtoffers maakt met ransomware. Zodra ze binnen zijn bij een bedrijf versleutelen ze alle bedrijfsdata en eisen losgeld voor de digitale sleutel waarmee de data weer toegankelijk wordt. Maar ze gaan nog een stapje verder. Zij dreigen gevoelige gegevens publiekelijk te lekken als bedrijven niet voldoen aan hun eisen. Ook een grote Nederlandse sportbond werd slachtoffer van LockBit. Volgens de nieuwssite van RTL bedroeg het geëiste losgeld meer dan 1 miljoen euro. De criminelen dreigden onder meer paspoorten en contracten van sporters openbaar te maken.

94%

Van de Nederlandse bedrijven kregen in 2023 te maken met een ransomware-aanval

52%

Van de bedrijven kregen na betaling weer toegang tot hun data

90%

daarvan kreeg dankzij een cyberverzekering de toegang tot hun documenten terug.

[4] www.emerce.nl
Proofpoint 2023 State of the Phish-rapport: Nederland aan kop met cyberaanvallen van zowel insiders als outsiders

[5] www.eset.com
ESET-onderzoek: beveiligingsincident kost mkb-onderneming gemiddeld meer dan een kwart miljoen

> **“Het mkb loopt onaanvaardbare risico’s. Elk bedrijf dat zijn beveiliging niet tiptop in orde heeft, komt aan de beurt. En de gevolgen zijn maar al te vaak groter dan een mkb-onderneming kan dragen.”**
>
> René van Etten

“Het mkb loopt nu onaanvaardbare risico’s”, zegt René van Etten. “Elk bedrijf dat zijn beveiliging niet tiptop in orde heeft, komt aan de beurt. En de gevolgen zijn maar al te vaak groter dan een mkb-onderneming kan dragen.” Dat probleem ziet ook Edwin Meinsma. “Veel te vaak is de beveiliging niet op orde. Men maakt geen back-ups. Of de gemaakte back-ups staan op hetzelfde netwerk waar de hackers toegang toe hebben. Updates worden niet of niet snel genoeg geïnstalleerd. Er is geen professionele firewall aanwezig. Of de software om malware en virussen buiten de deur te houden is niet up-to-date. Om nog maar te zwijgen van de manier waarop bedrijven en medewerkers omgaan met wachtwoorden. Er hoeft maar een klein detail niet te kloppen, en een hacker heeft een ingang.

Houd hackers buiten de deur

Een goede beveiliging is nooit klaar

De wereld van digitale veiligheid verandert voortdurend. Wat gisteren nog veilig was, kan vandaag alweer kwetsbaar zijn. Daarom is het belangrijk om constant alert te blijven en de digitale weerbaarheid doorlopend te verbeteren.
Veel partijen zetten zich in om de digitale veiligheid te verbeteren. Denk aan de overheid, bedrijven en belangenorganisaties. Maar ook u als adviseur kan een belangrijke bijdrage leveren. Uw adviesrol kan precies dat zetje geven voor uw klant om de beveiliging van zijn bedrijf de prioriteit te geven die het verdient.

Wat kan uw relatie zelf doen om hackers buiten de deur te houden?

- Investeren in basismaatregelen. Denk aan het gebruik van sterke wachtwoorden, een door professionals beheerde firewall en betrouwbare antivirussoftware.
- Medewerkers bewust maken van de risico's. Talloze bedrijven bieden trainingen aan om medewerkers te leren hoe ze cyberaanvallen kunnen herkennen en voorkomen.
- Een waterdichte back-upstrategie implementeren. Uit cijfers van het Digital Trust Centre van de Rijksoverheid (DTC) in 2023[6] blijkt dat 58% van de bedrijven die door ransomware zijn getroffen, geen goede back-up had.
- Voorbereidingen treffen voor als het toch misgaat. Met een degelijk bedrijfscontinuïteitsplan kan uw relatie de schade van een cyberaanval flink beperken.

[6] www.digitaltrustcenter.nl/nieuws Meerderheid ransomware-slachtoffers had geen back-up

7 Tips voor een gesprek over cybercriminaliteit met ondernemers

Zowel René van Etten als Edwin Meinsma zijn stellig over de rol van de onafhankelijke adviseur. Die is onmisbaar in de strijd tegen cybercriminelen! De adviseur kan zijn relaties heel veel narigheid besparen door op tijd het gesprek over cybersecurity aan te gaan.
Om u als adviseur op weg te helpen, geven ze tot slot van dit e-book hier hun tips.

1. Begin het gesprek met eenvoudige vragen over de beveiliging van het bedrijf. Zijn de basismaatregelen genomen, is er een back-upstrategie, zijn de antivirussoftware en de firewall up-to-date? U merkt het snel genoeg als uw relatie niet alle antwoorden paraat heeft. Dat is uw signaal om nog even door te vragen.

2. Wees duidelijk over mythes en misvattingen zoals de gedachte dat alleen grote bedrijven interessant zijn voor hackers. Ook restaurants, kledingwinkels en zelfs banketbakkers worden afgeperst door hackers.

3. Vraag ook eens of de medewerkers van het bedrijf weleens een cursus hebben gehad in cybersecurity. Want zelfs als uw relatie de beveiliging heeft uitbesteed aan een topbedrijf, dan nog blijft menselijk handelen het grootste risico. Phishing en social engineering herkennen is misschien wel het belangrijkste voor de veiligheid van een bedrijf.

4. Gebruik een vergelijkbaar bedrijf als voorbeeld van hoe het mis kan gaan. In elke sector worden bedrijven slachtoffer van cybercriminelen. Een rondje googelen levert al snel een voorbeeld op van een slachtoffer dat herkenbaar is voor uw relatie.

5. Vraag uw relatie eens wat het kost als zijn bedrijf een week stilligt. Hoe klanten zouden reageren als hun gegevens op straat kwamen te liggen. Maak inzichtelijk wat er werkelijk op het spel staat.

6. Gebruik tools als de Risicoklassenindeling Digitale Veiligheid van het Digital Trust Center. Daarmee krijgt uw relatie inzicht in de werkelijke risico's die het bedrijf loopt en welke maatregelen noodzakelijk zijn om hackers buiten de deur te houden.

7. Met de Cyber Assessment van Avéro Achmea heeft uw relatie snel inzicht in de informatiebeveiliging binnen zijn bedrijf. En met de Hacktest maakt een ethisch hacker een analyse van de kwetsbaarheden.
Avéro Achmea helpt dan bij het voorzien van passende begeleiding en praktisch advies.

Met dank aan:

René van Etten - Beveiliginsexpert en oprichter Threadstone
Edwin Meinsma - Productmanager Cyberverzekering bij Achmea
Tim Libanon - Beveilingsexpert en incident handler Fox IT

7498C 23.05