Whitepaper

# Zo wordt het mkb cyberweerbaar!

CyberSterk

## Inleiding: feiten en cijfers over cybersecurity in het mkb

6 op de 10 ICT-leveranciers vinden dat hun klanten in het midden- en kleinbedrijf (mkb) te weinig maatregelen nemen om hun eigen digitale omgeving te beschermen. Dit blijkt uit onderzoek van Centraal Beheer.[1]

Veel ICT-leveranciers (42%) hebben het gevoel dat de verantwoordelijkheid rondom cybersecurity op hun schouders wordt gelegd. Dit thema valt onder hun zorgplicht, vinden mkb-ondernemers (68%) dan ook. Opvallend is dat maar 22% van de ICT-leveranciers aangeeft dat er afspraken rondom die verantwoordelijkheid zijn vastgelegd. Hier ontstaat een probleem, want de mate van cyberweerbaarheid moet wel toenemen.

Door deze miscommunicatie blijven mkb'ers achter de feiten aanlopen én bereikt de digitale weerbaarheid niet het gewenste niveau. Dit terwijl het aantal dreigingen groeit. Het belang van digitale weerbaarheid blijkt ook uit de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Hierin wordt gesteld dat aanbieders van essentiële diensten passende technische en organisatorische maatregelen moeten nemen om hun ICT te beveiligen. Verder moeten zij maatregelen treffen om incidenten te voorkomen. Bij een incident moeten de gevolgen daarvan zo veel mogelijk worden beperkt.[2]

Waarom is de mate van cybersecurity vooral bij het mkb een probleem? Deze bedrijven hebben onvoldoende middelen, kennis en/of toegang tot kennis om dreigingen te onderkennen en zich weerbaar te maken. Het mkb is daarom een makkelijk doelwit. Deze ondernemers hebben simpelweg te weinig tijd om aandacht te besteden aan cybersecurity. Ze komen er niet aan toe.

Waar cybercriminelen zich vroeger richtten op grote ondernemingen, zie je nu een verschuiving naar het mkb. Vaak hebben zij de security niet op enterprise niveau ingeregeld.[3] Cybercriminelen voeren aanvallen uit met onder andere malware en phishing op een zo groot mogelijk aantal websites. De kans dat een mkb'er in dit sleepnet verstrikt raakt, is exponentieel toegenomen.

Daarnaast blijkt dat het hacken van ondernemingen in het mkb erg lucratief is. Mkb'ers beschikken over bank-, creditcards- en persoonlijke gegevens die gewild zijn onder criminelen en fraudeurs. Omdat ze vaak hun diensten en leveren aan grotere bedrijven, waarmee ze nauwe (online) banden hebben, is de data die een hacker zou kunnen achterhalen extra interessant.[4]

## Waarom je deze whitepaper moet lezen

In deze whitepaper bespreken we de 3 grootste misvattingen die er bij het mkb bestaan wat betreft cybersecurity. Verder laten we zien welke vormen van cybercrime het meest voorkomen. Aan de hand van een praktijkvoorbeeld schetsen we hoe het fout kan gaan. Uiteindelijk ligt de oplossing in het krijgen van inzicht; hoe dat precies werkt en hoe jij de controle behoudt, lees je ook in deze paper.

### Wat verstaan we onder cybercriminaliteit?

Cybercriminaliteit bestaat uit (1) delicten die worden gepleegd met behulp van en gericht tegen computers of het internet (cybercriminaliteit in enge zin), en (2) traditionele delicten die worden gefaciliteerd door of gepleegd met behulp van computers of het internet (cybercriminaliteit in brede zin).[5]

### Wat verstaan we onder cyberweerbaarheid?

Hieronder verstaan wij het vermogen van mkb'ers om weerstand te kunnen bieden tegen bekende en onbekende vormen van cybercriminaliteit en om snel te kunnen herstellen van een crisis als gevolg van een cyberincident.[6]

## 3 misvattingen over cybersecurity in het mkb ontkracht

Maar liefst 67% van de Nederlandse mkb'ers denkt dat hun organisatie geen interessant doelwit is voor cyberaanvallen. Dat blijkt uit onderzoek van Allianz in samenwerking met onderzoeksbureau Ipsos.[7] Toch is iedere organisatie een interessant doelwit voor cybercriminelen, hoe groot of klein ook. Meer dan een derde geeft aan niet voldoende kennis in huis te hebben om het bedrijf te beschermen tegen een cyberaanval. En dit maakt bedrijven juist vatbaarder voor een dergelijke aanval.

Liesbeth Kempen is IT Security Management Consultant. Met haar bespreken we de belangrijkste misvattingen rondom cybersecurity die op dit moment een grote rol spelen in het mkb.

### 1 "Cybersecurity wordt wel opgepakt door mijn ICT-leverancier"

Deze hebben we in de inleiding al kort aangestipt, maar dit is volgens Kempen toch wel een misvatting die snel moet worden ontkracht. Vaak wordt er gedacht dat de ICT-leverancier alles regelt, dus ook de security. Maar in de praktijk is dit niet zo. Digitale veiligheid is de verantwoordelijkheid van iedereen binnen het bedrijf zelf, met als eindverantwoordelijke de directie. Ook voor de ICT-leveranciers is deze misvatting een probleem. Ze willen graag een oplossing aanbieden, maar dan krijgen ze te horen: "Daar betalen we toch al voor?"

## 2 “Mijn medewerkers snappen niks van cybersecurity”

De meeste mkb’ers gaan ervan uit dat medewerkers het ook allemaal niet snappen. Medewerkers zouden dingen op een bepaalde manier doen omdat ze geen veiligere manier weten. De oplossing zit in de communicatie. Binnen bedrijven moet worden gepraat over de juiste werkwijze. Hierin is volgens Kempen bewustwording hard nodig.

## 3 “Als je een virusscanner en firewall hebt, ben je voldoende beveiligd”

Het gebruik van alleen een virusscanner en firewall is simpelweg niet meer voldoende. Een virusscanner signaleert namelijk alleen bekende dreigingen en kijkt daarbij niet naar abnormaal verkeer in je netwerk. Nieuwe dreigingen worden met een virusscanner niet herkend. Nieuwe technologieën, zoals gedragsanalyse, vormen tegenwoordig een belangrijke rol bij het detecteren van potentieel gevaar. En ook een firewall kan niet al het gevaarlijke netwerkverkeer buiten houden.

Het is het tijd om dieper in te gaan op de precieze vormen van cybercrime. Welke komen het meest voor in het mkb? Dat lees je in de volgende paragraaf.

## Vormen en toepassingen van cybercrime in het mkb

Er zijn talloze vormen van cybercrime, maar wat gebeurt er precies bij zo'n aanval en wat zijn de verschillen? Wij behandelen de meest voorkomende vormen binnen het mkb.[8]

### Malware

Het woord malware, wat schadelijke software betekent, is een samentrekking van malicious en software. Malware is software die schade kan richten aan gegevens of apparaten. Deze vorm van cybercrime wordt vaak ontwikkeld door teams van hackers, meestal om er 'gewoon' geld mee te verdienen. Veel malware wordt namelijk aan de hoogste bieder verkocht op het Dark Web. Dat is het onderdeel van het internet dat alleen met behulp van specifieke software bereikbaar is en waar veel dubieuze zaken plaatsvinden.

Gevallen van ransomware zie je steeds vaker in het nieuws voorbij komen. Afpersers gebruiken dit type malware om je computer en bestanden te vergrendelen. Daarbij dreigen zij alles te wissen, tenzij je losgeld betaalt.[9] Als je als ondernemer niet zeker weet of je al je bestanden op een goede manier hebt geback-upt, dan ben je gauw bereid om het geld te betalen - ondanks het advies van de politie om dit niet te doen.[10] Je houdt zo namelijk wel het criminele proces in stand.

Een ander, extra, probleem is dat dit soort besmettingen met ransomware tegenwoordig niet meteen actief worden. Vaker dwalen zulke virussen 'onzichtbaar' rond binnen het netwerk van een ondernemer. Pas als er genoeg systemen zijn geïnfecteerd, initieert een extern commando de activatie van de ransomware.

Wanneer zo'n virus al maanden actief is, dan heeft het geen zin om een backup van een maand terug uit te rollen. Want dan komt de schadelijke software net zo hard terug.

## Phishing

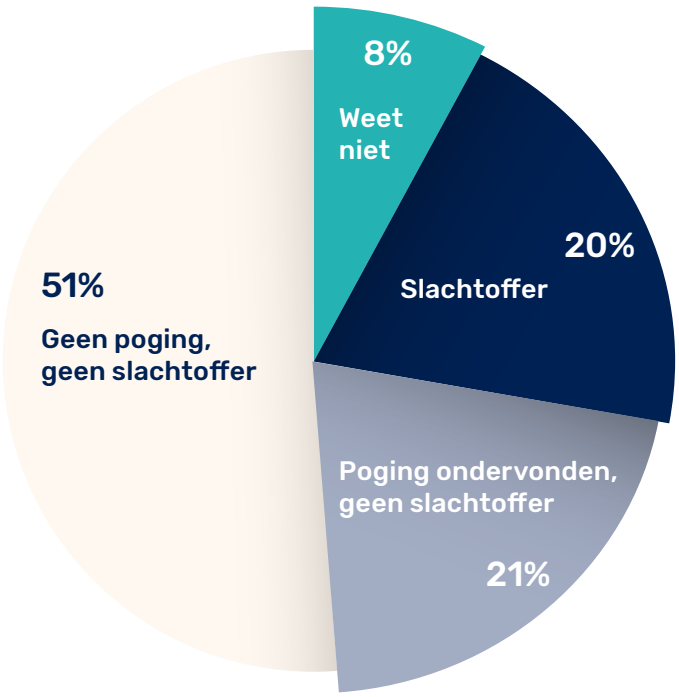
Bij phishing proberen criminelen je door e-mails naar een valse website te lokken. Daar stelen ze jouw gegevens of geld. Het is vaak lastig om een phishingmail te onderscheiden van een echte e-mail.[11] Toch is er wel een aantal tips te noemen. Een e-mail vol met spelfouten herken je snel als phishingmail, maar er zijn voorbeelden die er erg professioneel uitzien. Let op logo's, vage afzenders en een verkeerde aanhef. Controleer ook de link en de URL voordat je erop klikt. Grote partijen zoals ING of ICS hebben een gecertificeerd SSL-certificaat op hun naam staan. In de adresbalk zie je een groen slotje met daarachter de bedrijfsnaam. Ook begint de URL altijd met https:// en nooit met http://.

CEO-fraude is momenteel een trend binnen phishing. Daarbij doet de crimineel zich voor als de hoogste baas van het bedrijf en geeft hij een medewerker opdracht om een geldbedrag over te maken.

## Hacking

Hacken is het zonder toestemming van de eigenaar toegang krijgen tot een systeem, bijvoorbeeld om internetpagina's aan te passen, privédata te stelen of toegang te krijgen tot financiële gegevens.
De meeste websites van het Nederlandse mkb zijn niet veilig en erg gevoelig voor hacks, zo blijkt uit onderzoek van BDO Advisory en Perfect Day.[12] Meer dan 300.000 websites, verdeeld over 17 branches, werden in dit onderzoek onderworpen aan een scan. Gekeken werd naar belangrijke veiligheidskenmerken waaraan een website zou moeten voldoen. Bijvoorbeeld of klantgegevens wel versleuteld worden verzonden.
Als er een gerichte aanval wordt gepleegd op een bedrijf, dan is het vaak een combinatie van verschillende soorten cybercrime. Hoe dat kan aflopen, lees je op de volgende pagina.

**Slachtoffers cybercrime**



## In het ergste geval...

### Ondernemer raakt alles kwijt door hack van zijn bedrijf

Er zijn bedrijven die failliet gaan aan de gevolgen van cybercrime. De afkoopsom die ze moeten betalen is niet direct wat zorgt voor een faillissement. Het is vaker de verloren productietijd. Want als jij niet kunt leveren aan je klanten, is de kans groot dat ze naar een ander gaan. Om dit te illustreren volgt er een case.

*In 1991 wordt Xander Koppelmans ondernemer. Hij start een holding (Xtract bv) en een productie bv (studio PHGR). Al gauw stromen de opdrachten binnen. Er zijn 8 man in dienst en er werken daarnaast zo'n stuk of 30 freelancers voor zijn bedrijven. Hij heeft alles goed op de rit en steekt zijn kop niet in het zand wat betreft zijn digitale veiligheid. Xander heeft 3 back-upservers die de hele dag kopieën maken, zodat er geen data verloren kunnen gaan. Ook investeert hij in een firewall.*

*Toch gaat het helemaal fout. Op 2 april 2015 wordt het bedrijf gehackt. Het blijkt te gaan om een brute force-aanval. Hierbij voeren hackers alle mogelijke manieren van een wachtwoord in om dit te kraken. Alle bestanden en mappen werden automatisch in de prullenbak gesleept, die vervolgens direct geleegd werd. Maar er bestaat zoiets als data recovery toch? Gewiste bestanden kunnen op deze manier worden teruggehaald. Xander stuurt met spoed zijn schijven op, maar dit valt tegen. Alle bestanden zijn op zo'n manier aangetast dat ze onbruikbaar zijn geworden. Alles is weg, blijvend weg.*

*De initiële schade? Die bedraagt 269.000 euro. En dan moesten veel van de video's ook nog opnieuw worden gemaakt... De verzekering dekt 18.000 euro. Maar de werkelijke schade zit in het verminderde vertrouwen van de klanten. Hierdoor komt het bestaansrecht van het bedrijf zo ongeveer te vervallen. Een faillissement is onvermijdelijk.*

Hoe het nu gaat met Xander Koppelmans lees je op deondernemer.nl[13]. Natuurlijk willen we je met deze case niet de stuipen op het lijf jagen, maar wel wijzen op de risico's. Onderschat ze niet, is onze boodschap. Virusscanners en firewalls zijn een goed begin, maar niet voldoende. Welke stappen je verder moet zetten, beschrijven we in de volgende paragraaf.

## De laatste én belangrijkste stap van jouw cyberweerbaarheid

In de securitywereld is 100% veiligheid niet mogelijk. Maar je kunt wel een heel eind komen met wat extra stappen naast een virusscanner en firewall. Dit doe je aan de hand van het creëren van inzicht in de online securityrisico's van jouw bedrijf. Want bij elk bedrijf, hoe groot of klein ook, valt wel iets te halen. Daarnaast is elk bedrijf tegenwoordig een target geworden van hackers die geautomatiseerde tools op je website loslaten.

Neem de mate van cyberweerbaarheid serieus als je de continuïteit van je bedrijf wilt bewaken. Jij bent immers de enige eindverantwoordelijke en aansprakelijke, mocht het mis gaan.

### Zo word je Cybersterk

Idealiter zou kwaadaardig verkeer moeten worden opgespoord aan het begin van je netwerk. Het verkeer kan hier worden geanalyseerd op basis van gedrag, bestemmingen en tijd. Zo ontdek je tijdig uitzonderingen en zit je kort op de bal. Maar vaak zijn meldingen niet leesbaar, althans niet als je geen supertechneut bent.

SIDN, de organisatie achter het .nl-domein, verbindt mensen en organisaties voor een onbezorgd digitaal bestaan. Speciaal voor de ondernemer hebben wij CyberSterk ontwikkeld.  Een begrijpelijke security dienst die je direct inzicht geeft in de digitale risico's van je bedrijf.

Je netwerk en je website worden gecontroleerd door onder andere de fysieke SIDN CyberSterk-box. Ook analyseren we real-time je netwerkverkeer. Bij verdachte – en ongewenste – activiteiten slaan we alarm. Rapporteren van risico's gebeurt in begrijpelijke taal in ons dashboard. Zo kun je snel actie ondernemen om veilig en onbezorgd te blijven ondernemen. Omdat je als ondernemer op deze manier snapt wat er mis is, kun je ook echt het gesprek aangaan met je IT-partner en zoeken naar een oplossing.

### Wat we doen:

- We maken een wekelijkse websitescan op afstand. Die brengt de risico's van jouw website in kaart.
- De fysieke CyberSterk-box die we in je bedrijfsnetwerk plaatsen, detecteert afwijkend internetverkeer in en aanvallen op je bedrijfsnetwerk. Bij verdachte zaken slaan we alarm.
- De resultaten uit de scans geven we in heldere taal weer op een overzichtelijk dashboard, ook op je mobiel, inclusief notificaties van problemen.
- Periodiek voeren we een phishingsimulatie uit en meten we het klikgedrag van je medewerkers.
- Iedere maand sturen we je een rapportage met de belangrijkste resultaten uit de scans.
- We bieden ondersteuning bij het oplossen van problemen. Iets aan de hand? Neem contact op met je IT-partner of ons supportteam.

CyberSterk

www.cybersterk.nl

## Bronnen


1. https://nieuws.centraalbeheer.nl/mkb-legt-verantwoordelijkheid-cyber-security-bij-ict-dienstverlener/

2. https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners

3. Cybersecurity in het MKB - Uitgevoerd in opdracht van Interpolis In samenwerking met Capgemini Consulting (M. van den Berg & T. Reijmer) TNS NIPO Cybersecurity

4. https://www.deondernemer.nl/innovatie/cybersecurity/kleine-mkb-ondernemer-doelwit-hackers-bescherm~2027188

5. Domenie, M. M. L., Leukfeldt, E. R., Wilsem, J. A. van, Jansen, J., & Stol, W. Ph. (2013). Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit. Den Haag: Boom Lemma uitgevers.

6. Kleij, R. van der (2018). 'Digitale weerbaarheid in het mkb: een serieus probleem?', Tijdschrift voor Human Factors, 43(1), 19-21.

7. https://www.allianz.nl/algemeen/nieuws/mkbers-onderschatten-gevaren-cybercriminaliteit.html

8. https://www.sidn.nl/downloads/2mQvN6GXFWFGdxpJWFJYMY/8006d834d72dea4e3971923a6ddcf086/Trends_in_Online_Security_and_e-Identity.pdf

9. https://www.avg.com/nl/signal/what-is-malware

10. https://www.politie.nl/themas/ransomware.html

11. https://www.rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity/vraag-en-antwoord/phishing

12. https://perfectday.works/2019/10/15/merendeel-nederlandse-websites-gevoelig-voor-hack/

13. https://www.deondernemer.nl/financien/faillissement/cybercrime-hack-xander-koppelmans~1965565