Centraal Beheer

Cyber Check

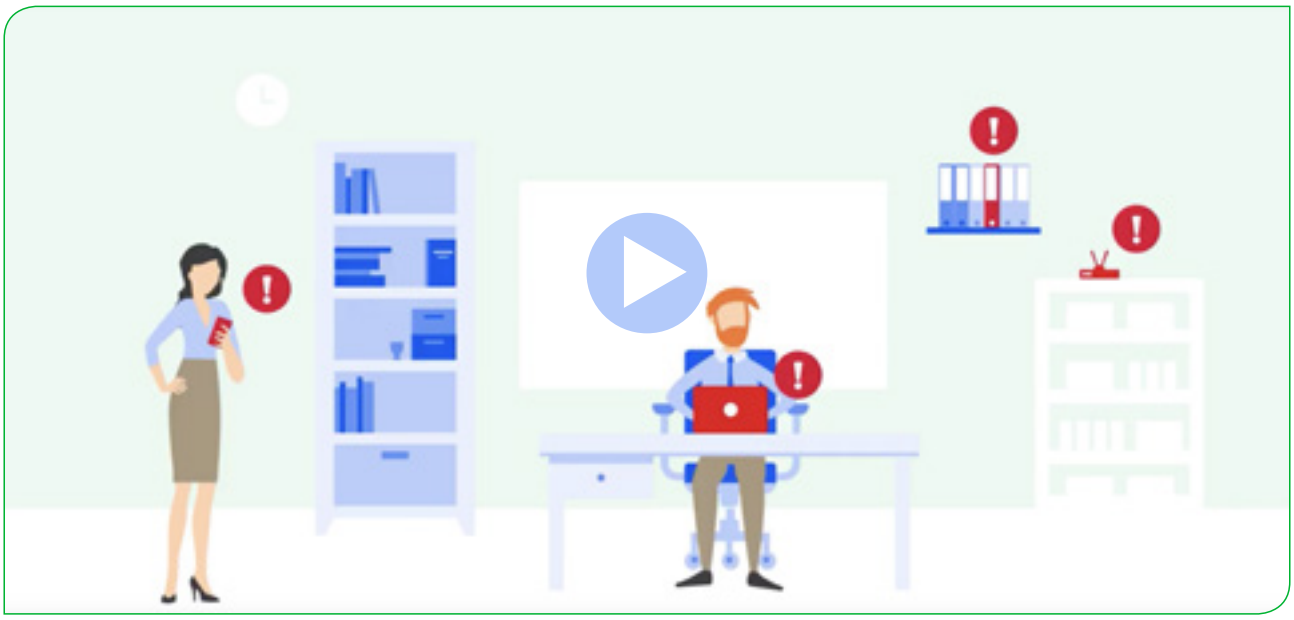
Aandacht voor digitale veiligheid (E-book 1)

Ondernemen kent risico's. Maar wist u dat een cyberaanval een van de grootste risico's is? Zeker 50% van de mkb-bedrijven heeft er al eens mee te maken gehad. En natuurlijk kan het iedereen overkomen. De vraag is alleen: wanneer? De gevolgen kunnen groot zijn. Gelukkig is er genoeg te doen om cybercriminelen tegen te houden. In dit e-book leest u wat cybersecurity inhoudt en hoe u de kans op cybercriminaliteit kunt verkleinen. Want digitale veiligheid is nu belangrijker dan ooit.

Wat leest u in dit e-book?

01
Over cybercriminaliteit en de gevolgen

Cybercriminaliteit: er wordt veel over gesproken, maar wat is het nu precies? De politie noemt het misdaden die worden gepleegd met ICT. Het gaat hier vaak om aanvallen via het internet. De crimineel zelf blijft onzichtbaar. De schade niet, die wordt juist steeds groter.



Bekijk het animatiefilmpje 'Wat is cybercrime?'

1.1 Cybercriminaliteit kent vele vormen

We zetten er een aantal voor u op een rij.

- Een inbraak in computers of netwerken (hack);
- Softwareprogramma's die systemen verstoren of data verzamelen (malware);
- Het lekken van data (datalek);
- Een platgelegd systeem waarbij losgeld wordt geëist (ransomware);
- Een nepmail met een link die data of geld prijsgeeft als je erop klikt (phishing);
- Een mail zogenaamd vanuit de directeur aan de financiële administratie om grote geldbedragen over te maken (CEO-fraude);
- Een aanval op websites of systemen om deze te overbelasten en onbereikbaar te maken voor klanten (DDos-aanval).

1.2 Misvattingen over cybercriminaliteit

Cybercriminaliteit wordt helaas nog te vaak onderschat. Maar zoals u nu weet kan iedereen een keer aan de beurt zijn. Dit zijn de 3 meest voorkomende misvattingen over cybersecurity.

Misvatting 1:
Als kleine onderneming is het niet nodig om maatregelen tegen cybercrime te nemen.

Misvatting 2:
Denken dat u (of uw toeleveranciers) alles goed geregeld heeft.

Misvatting 3:
Een cybercrime-aanval gebeurt niet zo vaak. Hoe erg kan het zijn?

1.3 De 3 cyberrisico's en de gevolgen

Er zijn 3 risico's die een cyberincident mogelijk maken. 1 van de 3 is al genoeg om schade te veroorzaken. En wat zijn dan de mogelijke gevolgen?

Risico 1: Menselijk handelen
Mensen maken fouten. Denk aan iemand die een USB-stick met geheime bestanden verliest. Ook kunnen bestanden of data beschadigd raken door een menselijke fout. Een veelgebruikt wachtwoord? Dit zorgt ervoor dat criminelen makkelijker inbreken.
Slechte gewoonten van medewerkers zorgen er voor dat de deur voor cyberaanvallen bij hun werkgever open komt te staan. In 66% van alle gevallen worden cyberaanvallen veroorzaakt of vergemakkelijkt door de nalatigheid en/of kwaadwilligheid van werknemers.

Bron: Willis Towers Watson

Risico 2: Technisch falen
Soms werkt de techniek niet mee. Denk dan aan het falen van hardware zoals harde schijven, programma's of besturingssystemen, of netwerken en servers. Hierdoor kan een cyberincident plaatsvinden.
Een mkb-bedrijf heeft 43% kans op een ICT- of softwarestoring: een uitgelezen kans voor cybercriminelen

Bron: Cybersecuritymonitor 2018, CBS

Risico 3: Cybercrime

Dit is het domein van cybercriminelen. Zij doen er alles aan om data of geld los te krijgen bij mensen en bedrijven. En soms leggen ze een website of bedrijf plat voor de lol of de eer. Om te laten zien dat ze het kunnen.

Malware – kwaadaardige software – is de grootste dreiging. 90% van de malware-besmettingen vindt plaats via e-mail

Bron: Cybersecuritymonitor 2018, CBS

Wat zijn de mogelijke gevolgen van cybercrime?

- Bedrijfsstilstand
- Herstel systemen en data
- (Gevoelige) informatie verloren, beschadigd of openbaar
- Juridische kosten
- Eis losgeld
- Reputatieschade
- In het ergste geval: faillissement

02
Cijfers & feiten cybersecurity in het mkb

Cybersecurity laat zich goed meten. We weten al dat 50% van de mkb-bedrijven te maken heeft gehad met cybercriminaliteit. Maar dat is niet het enige wat opvalt bij het zien van alle cijfers en feiten. Hoe veilig denkt het mkb dat ze zijn? En wie is er verantwoordelijk voor de digitale veiligheid? Wij zetten alle feiten en cijfers voor u op een rijtje.

2.1 Cijfers cybersecurity van nu in het mkb

Er zijn dus veel misverstanden als het gaat om cybersecurity. En ja: elk bedrijf loopt risico, óók in het mkb. Wat is de gemiddelde schade? Bent u goed beschermd... of juist niet?

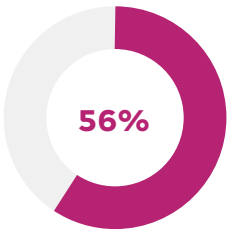
23%

maakt zich zorgen over de eigen cybersecurity

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

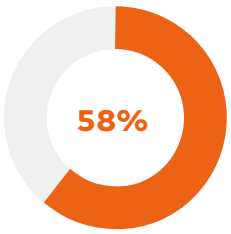
Goed beschermd, of niet?

MKB-bedrijven



Heeft het gevoel dat het bedrijf **goed** beschermd is

IT-beheerders



Geeft aan dat hun MKB-klanten **onvoldoende** beschermd zijn

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

Gemiddelde schade per cyberincident:[2]

€ 78.700

Bron: IT Security: Cost-center or Strategic Investment, 2017, Kaspersky Lab and B2B International.

€ 1.000.000.000

Jaarlijkse schade van cyberincidenten voor het mkb (10 miljard euro voor heel het bedrijfsleven)

Bron: Cyber Value at Risk in The Netherlands 2017, Deloitte

Uitgaven voldoende

Het MKB vindt het geld dat ze aan cyberveiligheid uitgeven voldoende.

- Zeker voldoende
- Waarschijnlijk onvoldoende
- Weet ik niet
- Waarschijnlijk voldoende
- Zeker onvoldoende

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

Ondernemers komen er na

191 dagen

achter dat ze slachtoffer zijn![4]

Bron: Cybersecuritymonitor 2018, CBS

Wat te doen bij een cyberincident

MKB-bedrijven

IT-beheerders

48% van de MKB-bedrijven zegt dat ze weten wat ze moeten doen bij een cyberincident. IT-beheerders schatten het percentage MKB-bedrijven dat dit weet een stuk lager in.

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

2.2 Wie is verantwoordelijk voor de cybersecurity?

Bent u als ondernemer of is de IT-beheerder verantwoordelijk voor de cybersecurity? Of allebei? We zetten graag de meest opvallende uitkomsten van het Cybersecurity Onderzoek van Centraal Beheer, uitgevoerd door Ipsos, voor u op een rij.

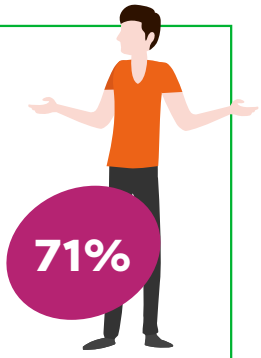
Eindverantwoordelijk
77% van de mkb-bedrijven geeft aan zelf eindverantwoordelijk te zijn voor de cybersecurity

IT-beheerders zeggen dat hun klanten vaak vinden dat de IT-beheerders daarvoor verantwoordelijk zijn:

Voor een deel bij MKB-klant en voor een deel bij IT-beheerder

- Helemaal bij MKB-lant
- Voor het grootste deel bij MKB-klant
- Helemaal bij IT-beheerder
- Voor het grootste deel bij IT-beheerder

Afspraken over cybersecurity



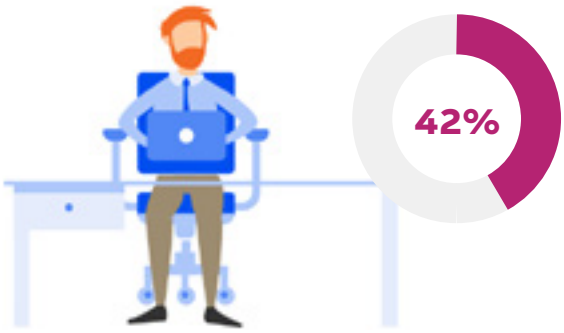
71% van de MKB-bedrijven verwacht goede cybersecurity van hun IT-beheerder

Toch worden daar geen duidelijke afspraken over opgeschreven. Maar 22% van de IT-beheerders geeft aan dat er duidelijke afspraken zijn gemaakt rondom cybersecurity.

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

Verwachting
Bijna de helft (46%) van alle IT-beheerders geeft aan dat mkb-klanten verwachten dat zij de cybersecurity verzorgen. Zonder dat daar duidelijke afspraken over zijn gemaakt en opgeschreven.

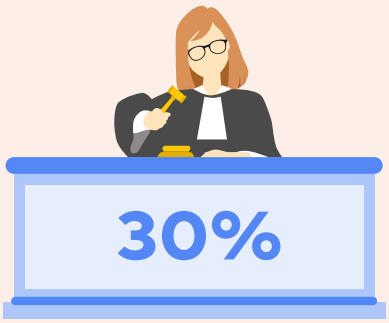
Verantwoordelijkheid



42% van de IT-beheerders geeft aan dat hun MKB-klanten de verantwoordelijkheid over cybersecurity op hen afschuiven.

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

Aansprakelijk stellen bij cyberincidenten



30% van de MKB-bedrijven geeft aan dat zij hun IT-beheerder aansprakelijk stellen als er een cyberincident komt.

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

03

Hoe herkent u een hack

Een bekende vorm van cybercriminaliteit is een hack. Hoe eerder u zo'n hack herkent, hoe beter natuurlijk. Maar gemiddeld duurt het ruim een half jaar voor bedrijven iets opmerken. Soms sluipen inbrekers uw systemen binnen zonder dat u er iets van ziet. Wat zijn de signalen? En hoe reageert u? 5 praktijkvoorbeelden om u te helpen.

1 **De computer doet raar**
Een gek scherm dat soms in beeld verschijnt. Mails die blijven hangen. Of medewerkers die moeite hebben met inloggen. De computer geeft ten onrechte aan dat er te vaak een verkeerd wachtwoord is ingevuld. Dit kunnen allemaal signalen zijn dat u bent gehackt. Zorg dat uw medewerkers weten waarop ze moeten letten, zodat ze een incident direct kunnen melden. En laat de zaak onderzoeken door een securityspecialist.

2 **Er gebeurt van alles op uw computernetwerk**
Inlogpogingen vanaf een ongebruikelijke plek. Meer dataverkeer op uw netwerk dan normaal. Zegt uw onderbuikgevoel u dat er iets aan de hand is? Laat uw systemen altijd digitaal monitoren door een expert. Dan weet u het onmiddellijk wanneer u wordt gehackt. Door direct maatregelen te nemen, voorkomt u dat een cybercrimineel dieper in uw systemen doordringt.

3 **Hackers misbruiken uw website**
U krijgt klachten binnen bij uw klantenservice dat uw website wordt misbruikt. Of u komt er zelf achter dat u opeens producten verkoopt buiten uw assortiment. Bijvoorbeeld illegale medicijnen. Houd altijd een oogje op uw website. Ook die kunt u laten monitoren. Zo bent u direct op de hoogte van eventuele kwetsbaarheden of ongewenst bezoek. En kunt u actie ondernemen.

4 **Een ‘vreemde’ vraag van de baas**

De directeur mailt tijdens zijn vakantie: hij wil per direct een fors bedrag over laten maken. Waarschijnlijk niet de normale gang van zaken, wel een geval van CEO-fraude. De e-mail is gehackt. En de accountgegevens van de directeur zijn buitgemaakt. Een expert helpt u de oorzaak te vinden en het lek te dichten. Maar het begint met medewerkers die letten op ‘vreemde’ vragen. Ook een vierogenprincipe werkt goed. Zo bent u extra alert.

CEO-fraude van € 19.244.304,-

Begin 2018 werd de Nederlandse tak van bioscoopketen Pathé slachtoffer van CEO-fraude. Een cyberbende weet maar liefst 19,2 miljoen euro binnen te halen door zich voor te doen als leidinggevenden van het Franse moederbedrijf.

Bron: Het Parool

5 **Dit is een gijzeling**

Uw computersystemen zitten op slot. Op het scherm staat dat de systemen gegijzeld zijn. Of u zo vriendelijk wilt zijn om losgeld te betalen. Anders blijven de systemen geblokkeerd en ligt uw bedrijf stil. Haal er direct een expert bij, dat is het beste. Natuurlijk is voorkomen beter dan genezen. Bescherm uw bedrijf tegen ransomware en andere online bedreigingen. En verbeter uw cybersecurity.

Database hacken via het aquarium

In een Amerikaans casino was de temperatuursensor van een aquarium gekoppeld aan het draadloze netwerk van het casino. Handig? Niet echt. Dat apparaatje is namelijk vrij simpel te kraken. Zo lukte het hackers om via de temperatuurregelaar van het aquarium klantgegevens van het casino te stelen.

04
Preventietips tegen cybercriminaliteit

Bij elk bedrijf valt iets te halen voor cybercriminelen. Gelukkig kunt u genoeg zelf doen om risico's te beperken. Het mooie is dat dit lang niet altijd veel geld of tijd hoeft te kosten. Met deze preventietips vergroot u eenvoudig uw digitale veiligheid en het cyberveilige gedrag van uw medewerkers.

4.1 10 tips: uw cybersecurity beter op orde

Inbrekers rammelen aan iedere deur om te zien hoe ze het makkelijkst binnenkomen. Cybercriminelen doen precies hetzelfde. Om hen buiten te houden zijn 2 dingen belangrijk: bescherm uw bedrijf en beperk de risico's. 10 tips om nú uw risico's te verkleinen.

1 **Inventariseer uw cyberrisico's**
Daar begint het verbeteren van uw cybersecurity mee. Wat zijn uw kroonjuwelen? Bepaal welke informatie echt belangrijk is om uw bedrijf draaiende te houden en waarom. Wat gebeurt er bijvoorbeeld als privacygevoelige gegevens, zoals creditcardgegevens, op straat komen te liggen?

2 **Check uw digitale veiligheid**
Ga om de tafel met uw ICT-manager of externe ICT-partner. Is uw software up-to-date? En maakt uw bedrijf regelmatig back-ups van systemen? Test ook of u deze back-ups terug kunt plaatsen op uw netwerk. Heeft u een goede firewall en gebruikt u antivirussoftware? Installeer altijd de laatste updates. Dit zijn enkele basismaatregelen die elk bedrijf moet nemen.

3 **Kijk eens naar uw beveiligingsinstellingen**
Vergeet ook niet te informeren of de beveiligingsinstellingen van uw software goed staan. Daarmee voorkomt u veel ellende. Bijvoorbeeld bij de meeste cloudapplicaties is '2-factor-authenticatie' en dus veiliger inloggen ook een kwestie van instellen. Uw medewerkers moeten dan bijvoorbeeld naast een gebruikersnaam en wachtwoord ook een code intoetsen. Deze code ontvangen ze via sms of een app.

4 **Bewaar belangrijke gegevens**
Vraag uw ICT-expert ook welke 'loggegevens' uw systemen of cloudapplicaties automatisch opslaan. Dat zijn gegevens die bijvoorbeeld vertellen wie er heeft ingelogd, wanneer en hoe. En check deze logbestanden regelmatig. Het helpt u de oorzaak van problemen door een cyberaanval te achterhalen. Ook hackers laten sporen achter.

5 **Vind de hiaten in uw bedrijfsprocessen**
Veilig werken is meer dan ICT: kijk ook naar uw processen. Neem CEO-fraude. Tijdens de afwezigheid van de CEO sturen cyberhackers uit diens naam een verzoek naar de financiële afdeling om geld over te maken naar hun rekening. Daar gaan veel bedrijven op in. Als meer mensen een betaling moeten goedkeuren, maakt u de kans kleiner dat dit gebeurt.

"Bepaal welke informatie echt belangrijk is om uw bedrijf draaiende te houden en waarom"

6 **Kijk hoe veilig uw mensen werken**
Mensen zijn vaak de zwakste schakel in de beveiliging. Gebruiken uw medewerkers voor alles hetzelfde wachtwoord? Loggen ze met hun laptop in op openbare netwerken die vaak slecht zijn beveiligd? Maak uw medewerkers bewust van de risico's. Hoe u dat doet, leest u in 3.2 .

7 **Doe een externe scan**
Cybersecurity is complex. En ieder bedrijf is anders. Laat een externe specialist de veiligheid van uw bedrijf in kaart brengen. Zij weten wat de juiste vragen en maatregelen zijn voor u. Met regelmatige scans laat u bovendien zien dat u werk maakt van de AVG-wet.

8 **Laat uw bedrijf monitoren**
Cybercriminelen worden steeds slimmer. Hoe goed uw beveiliging ook is, er kan toch iets gebeuren. Vaak zonder dat u het door heeft. Houd uw systemen en website op afstand in de gaten. Dan kunt u direct actie nemen als er ongewenste activiteiten plaatsvinden.

61%

Gebrek aan kennis wordt het vaakst opgegeven als reden om ICT-beheer uit te besteden.

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

9 **Geef iemand de taak: cybersecurity**
Zorg dat een medewerker in uw bedrijf de tijd krijgt om in dit onderwerp te duiken. Die persoon informeert andere medewerkers over ontwikkelingen en is het aanspreekpunt bij incidenten. Een dagdeel per maand aandacht voor cybersecurity kan het verschil al maken.

10 **Maak een stappenplan voor incidenten**
Wat als er toch een incident is? Wees voorbereid. Bepaal welke stappen uw bedrijf moet nemen en zorg dat uw medewerkers dit weten. Communicatie naar de buitenwacht hoort er ook bij. Ligt er gevoelige informatie op straat? Vertel uw klanten en leveranciers dan direct wat er speelt. U bent het niet alleen verplicht vanuit de AVG-wet, het wordt ook gewaardeerd!

4.2 5 tips voor cyberveilig gedrag bij medewerkers

Bij cybersecurity wordt al snel aan techniek gedacht. Maar weet u hoe belangrijk mensen zijn bij de beveiliging van uw bedrijf? Met deze 5 tips voor cyberveilige medewerkers maakt u ze alert. Want alleen samen verlaagt u cyberrisico's echt.

1 **Maak cyberincidenten bespreekbaar**
Een verdacht telefoontje of een dubieuze mail waarop is geklikt? Zorg dat uw mensen het aan iemand kwijt kunnen. Stel een meldpunt voor cyberincidenten in. Dat kan de ICT-servicedesk zijn. Of geef iedere afdeling een 'ambassadeur'. Zet cybersecurity ook op de agenda bij het teamoverleg. En beloon goede tips. Op die manier zorgt u voor bewustzijn én betrokkenheid; cyber-alerte medewerkers dus.

'Een verdacht telefoontje of een dubieuze mail waarop is geklikt? Stel een meldpunt voor cyberincidenten in'

Getroffen door cybercriminaliteit?
50% van de werknemers onderneemt **geen** actie.

2 **Zorg voor veilig wachtwoordgebruik**
Veel mensen gebruiken eenvoudige wachtwoorden. Of steeds dezelfde. Maar die zijn snel te kraken of te raden. Leer uw medewerkers wat sterke wachtwoorden zijn. En maak het beleid dat ze deze regelmatig vernieuwen. Met een password manager maken ze op een makkelijke manier unieke wachtwoorden aan. Nog veiliger: laat uw mensen in meer stappen inloggen. Naast een wachtwoord moet uw medewerker dan ook een SMS of code van een app invoeren.

123456
is al jaren het meest gebruikte wachtwoord.

3 **Leer uw medewerkers phishingmails herkennen**
Cybercriminelen werken steeds slimmer. Ze sturen 'phishingmails' die bijna niet van echt te onderscheiden zijn. Zó echt dat veel mensen erin trappen. Hackers proberen zo toegang te krijgen tot uw systemen. Of gevoelige data te ontfutselen. Leer uw medewerkers phishingmails te herkennen. En test of ze hier alert op zijn. Bijvoorbeeld door ze tijdens het werk nepmails te sturen.

4 **Maak duidelijke afspraken over veilig werken**
Cyberveilige medewerkers gebruiken geen openbare wifi-netwerken. Want dan zet u de achterdeur open voor hackers en dat maakt uw bedrijf kwetsbaar. Maar het gaat verder dan ICT. Laat bijvoorbeeld geen documenten op de printer slingeren. Of neem geen onbeveiligde USB-sticks met klantgegevens mee naar huis. Maak duidelijke afspraken met uw medewerkers over uw informatiebeveiliging. Vertel wat u van ze verwacht en wat ze moeten doen als er iets gebeurt.

4 **Houd uw medewerkers alert**
Blijf continu aandacht besteden aan cyberveilig werken. En zorg voor variatie om het leuk te houden. Train medewerkers via een e-learning. Of organiseer hackdemo's. Daarbij laten 'ethisch hackers' zien wat er gebeurt bij cyberattacks. Games werken ook goed. Een pubquiz zet u zelf eenvoudig in elkaar. Zo houdt u cyberveilige medewerkers. En voorkomt u vervelende incidenten.

Blijf zelf alert als ondernemer: menselijk handelen wordt gezien als het grootste cyberrisico. Toch vergroot maar 44% van de mkb-bedrijven het cyberbewustzijn van de medewerkers.

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

05
Cyberexperts aan het woord

Voor cybersecurity werkt Centraal Beheer samen met een aantal experts. Zij denken graag mee. Ook nu. Redenen om cybersecurity aan te pakken? Uzelf beschermen tegen ransomware? Onze experts geven tips.

5.1 5 redenen om cybersecurity aan te pakken

Digitale bedreigingen zijn overal. Wie zijn bedrijf daar niet tegen beveiligt, loopt risico's. Effectieve cybersecurity helpt uw bedrijf te beschermen én biedt zakelijk voordeel. De link met de AVG en databescherming is snel gelegd. Toch is het meer dan een wettelijke verplichting. Onze cyberexperts geven 5 goede redenen om cybersecurity aan te pakken.

Experts: Eva Eenhoorn en Dennis de Geus van Capgemini, René van Etten van ThreadStone en Remco Verhoef van CyberBorg.

1 **Bescherm de continuïteit van uw bedrijf**
Stel, een cyberaanval legt uw website plat. Of zelfs al uw digitale bedrijfsprocessen. "Als u uw klanten niet kunt helpen, gaat de geldkraan dicht. Zeker in het mkb bestaat de kans dat uw onderneming dat niet overleeft", zegt Eva Eenhoorn, senior consultant cybersecurity & privacy bij Capgemini.
En dan zijn er nog de kosten voor het herstel van data en systemen. Het kan ook zijn dat u losgeld moet betalen om uw computers te bevrijden van ransomware (zie ook 5.2).

Of u leidt financiële- en reputatieschade door het hacken van concurrentiegevoelige data. Goede cybersecurity verkleint de kans op zo'n aanval.

2 **Vermijd AVG-boetes**
Nieuws over datalekken, de media staan er vol mee. Als ondernemer bent u verantwoordelijk voor wat er met uw data gebeurt. Remco Verhoef, eigenaar van CyberBorg: "Heeft uw bedrijf data gelekt? Volgens de AVG moet u precies weten om welke data het gaat en het lek snel melden. Anders riskeert u een flinke boete." Ook moet u aantonen dat u 'passende maatregelen'

heeft genomen. Door regelmatig uw website te monitoren en uw cybersecurity te checken laat u zien dat u de bescherming van uw data steeds verbetert.

3 **Voorkom reputatieschade**

Een hacker maakt uw bedrijfsdata openbaar. Of een medewerker is slordig met informatie. Een datalek doet uw bedrijfsreputatie hoe dan ook geen goed. Klanten en zakenpartners verliezen hun vertrouwen: heeft u wel genoeg gedaan om hun data te beschermen? “Met de AVG focussen veel bedrijven zich op cookies of juridische zaken. Niet op de bescherming van hun data, terwijl het daar juist om gaat”, zegt René van Etten, manager bij ThreadStone Cybersecurity. Zet dus vol in op cybersecurity. Gaat het toch mis? Een helder noodplan en goede communicatie naar uw klanten en ketenpartners beperken de reputatieschade.

10.000+

meldingen van een datalek in 2017

Bron: Autoriteit Persoonsgegevens

4 **Bescherm ook uw klanten en partners**

Malware kan zich via uw website verspreiden en klanten of zakenpartners besmetten. “Dan is de schade nog groter en kunt u zelfs klanten kwijtraken door een cyberincident”, zegt Remco Verhoef van CyberBorg. Bovendien stellen vooral grote bedrijven steeds hogere eisen aan hun leveranciers: ze willen de garantie dat ze cyberveilig werken. Dat maakt het nog belangrijker om uw cybersecurity snel op orde te hebben.

‘Maak van het investeren in cybersecurity een USP. Zo laat u klanten zien dat hun data bij u in goede handen zijn’

5 **Maak een troef van cybersecurity**

Cybersecurity gaat niet alleen om bedreigingen, maar ook om kansen. “Maak van het investeren in cybersecurity een USP. Laat deze in uw communicatie terugkomen, zoals in offertes en op uw website. Zo onderscheidt u zich van de concurrentie en laat u klanten zien dat hun data bij u in goede handen zijn”, zegt René van Etten van ThreadStone. Ook consumenten vinden cybersecurity belangrijk, zo blijkt. Dennis de Geus, lead cybersecurity & privacy van Capgemini: Laatst hielden we een onderzoek onder consumenten. Daar kwam uit dat cyberveiligheid zelfs in de top 3 staat van redenen om al dan niet voor een leverancier te kiezen.” Bijvoorbeeld bij een online bestelling.

‘Als u uw klanten niet kunt helpen na een cyberaanval, gaat de geldkraan dicht. Zeker in het mkb bestaat de kans dat uw onderneming dat niet overleeft’

1/4

Nog geen kwart van de mkb-bedrijven geeft aan een informatiebeveiligingsbeleid te hebben.

Bron: Cybersecurity Onderzoek 2018, Centraal Beheer door Ipsos

5.2 Ransomware: hoe beschermt u zich ertegen?

Een ransomware-aanval is een van de grootste cyberrisico’s voor het mkb. Wat gebeurt er dan? En hoe maakt u de kans op een aanval zo klein mogelijk? Een praktijkvoorbeeld. Mét waardevol advies van een securityexpert.

Expert: Lodi Hensen van Fox IT

Een ransomware-aanval: wat nu?
Het begint als een gewone werkdag. Maar dan blijken alle computersystemen op slot. Ze zijn gehackt en gegijzeld met ransomware, een kwaadaardig programma dat software en data versleutelt. De hackers vragen om losgeld. Een centrale computer stond per ongeluk ‘open’: de verbinding met het internet was niet beveiligd. Via een zwak wachtwoord zijn cybercriminelen diep in de computersystemen doorgedrongen.

Het bedrijf valt stil. De binnendienst kan geen afspraken meer maken met klanten. De buitendienst kan niet bij zijn digitale werkinformatie. En de administratie kan geen facturen maken of betalen. Dat zijn maar een aantal mogelijke problemen. Terug naar pen en papier is voorlopig de enige optie.

Dit praktijkvoorbeeld kan ook in uw bedrijf gebeuren. Want aanvallen met ransomware zijn vaak gericht op het mkb. Hoe bent u snel weer aan de slag na zo’n aanval? En hoe beperkt u de schade zoveel mogelijk?

Snel weer aan de slag
Fox IT helpt bij het oplossen van ransomware-aanvallen en andere cyberincidenten. Het is een van de specialisten waar Centraal Beheer mee samenwerkt. “We komen direct in actie: onderzoeken wat er aan de hand is en kijken naar de herstelmogelijkheden”, vertelt Lodi Hensen, senior incident handler van Fox IT.

‘Een ransomware-aanval is niet altijd te vermijden, dus je moet goed voorbereid zijn’

€ 4000,-

Het gemiddelde losgeldbedrag

€ 40.000,-

De gemiddelde totale kosten om weer op te starten na een ransomware-aanval zijn 10 keer hoger.

Bron: Datto

Is er een back-up?
Het is belangrijk dat bedrijven zeer regelmatig een back-up van hun systemen maken. En ook met regelmaat testen of ze die kunnen terugzetten. “Zo ja, dan is dat goed nieuws. Maar het kan gebeuren dat de back-up niet goed werkt, of ook versleuteld is door de cybercriminelen. Dat proberen we eerst op te lossen.”

Zijn loggegevens bewaard?
Ook de logbestanden van de computers zijn van belang. “Deze logbestanden vertellen welke systemen en data zijn geraakt en hoe dat is gebeurd. Maar je moet wel de júiste loggegevens bewaren. Het beste bewaar je ze voor een lange periode. Dat kun je instellen in je software. Een ransomware-aanval is niet altijd te vermijden, dus je moet goed voorbereid zijn.”

Kosten? Meer dan alleen losgeld
Geen backup(s)? De tijd dat een bedrijf stilligt kost natuurlijk geld. Vaak is er hulp van buitenaf nodig: IT stuurt ook facturen. Denk ook nog aan mogelijke kosten om data of het vertrouwen van klanten te herstellen. Het eventueel betalen van losgeld is dus 1 van de vele kosten na een ransomware-aanval.

Wat kunt u zelf doen?
Het bedrijf in dit praktijkvoorbeeld had de ransomware-aanval kunnen voorkomen, zegt Lodi Hensen. “Je moet zorgen dat ‘vreemden’ niet op afstand binnen kunnen in je digitale systemen. Hier stonden de veiligheidsinstellingen van een server niet goed: er stond een ‘poort’ open naar het internet. Maar je kunt ook besmet raken door op een link te klikken in een phishingmail. Maak je medewerkers hierop alert. Met een monitoringsysteem om malware op je systemen op te sporen, kun je dit soort problemen snel signaleren en aanpakken. Want alleen antivirussoftware is niet genoeg.”

‘Het kan gebeuren dat de back-up niet goed werkt, of ook versleuteld is door de cybercriminelen’

Stop snelle verspreiding
Zijn tweede advies? Sterkere wachtwoorden. “En dat geldt niet alleen voor de medewerkers. We zien bijvoorbeeld vaak dat systeembeheerders zwakke wachtwoorden gebruiken voor ‘testaccounts’. Dat zijn verzonnen gebruikers waarmee ze programma’s testen. Als zo’n account met veel administratorrechten wordt gehackt, kan een aanval zich snel verspreiden.”

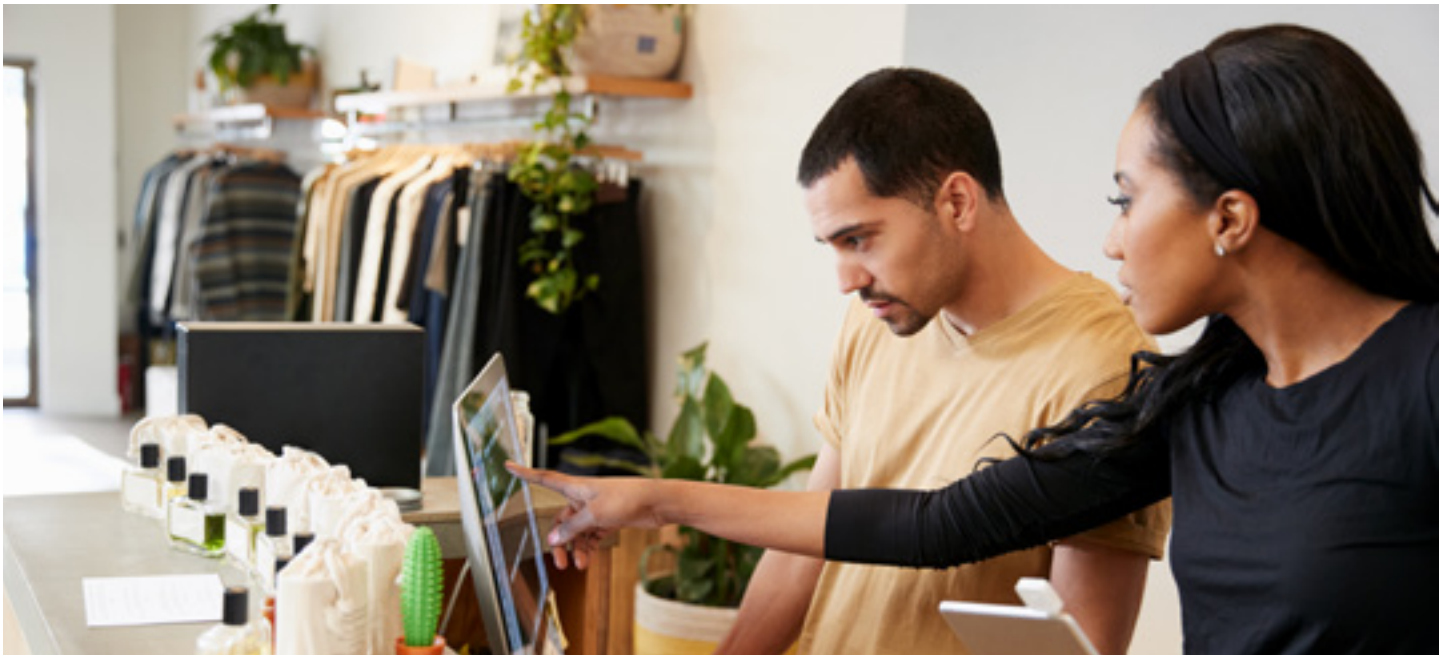
06

Breng uw cyberrisico's in kaart

Als ondernemer wilt u door! U moet er dan ook niet aan dénken dat uw bedrijf te maken krijgt met een hack, phishingmail of virus. Daarom heeft Centraal Beheer verschillende cyberoplossingen. Ook als u niet bij Centraal Beheer verzekerd bent. Kijk op centraalbeheer.nl/cyber.

Heeft u vragen over uw cybersecurity?
Maak online een vrijblijvende afspraak of bel 'Even Apeldoorn': (055) 579 8421.

Wilt u meer lezen over hoe u inzicht krijgt in uw eigen risico's? En hoe u cyberincidenten kunt voorkomen? Lees dan ook het vervolg op dit e-book: Cyber Check deel 2.



07
Goed om te weten

Bij Centraal Beheer staan we al meer dan 100 jaar klaar voor onze klanten. U kent ons vast van ‘Even Apeldoorn bellen’.

U kunt bij ons financiële producten en diensten afsluiten

Zoals verzekeringen, pensioenen, hypotheken, spaarrekeningen, beleggingsproducten en diensten voor HR en Risicomanagement. Rechtstreeks en via adviseurs die met ons samenwerken.

Vanaf 1995 horen wij bij Achmea

Centraal Beheer is een merk van Achmea Schadeverzekeringen N.V. in Apeldoorn.
Achmea is de grootste verzekeraar van Nederland.
Achmea Schadeverzekeringen N.V. is ingeschreven bij de Kamer van Koophandel onder nummer 08053410 en de AFM onder nummer 12000606.

Uw gegevens in vertrouwde handen

Sluit u een verzekering of financiële dienst af? Dan hebben wij uw gegevens nodig. Denk aan uw naam, adres en woonplaats, e-mailadres, telefoonnummer en bankrekeningnummer. Soms hebben wij ook meer gegevens van u nodig. Achmea B.V. is verantwoordelijk voor een goede verwerking van uw persoonsgegevens.

Wilt u weten welke gegevens wij verwerken en waarvoor?

Kijk dan in ons Privacy Statement op centraalbeheer.nl/privacy. Daar leest u ook wat uw rechten zijn. En wanneer u bezwaar kunt maken tegen verwerking van uw gegevens. Wilt u ons Privacy Statement op papier ontvangen? Stuur dan een brief naar: Centraal Beheer Relatiebeheer, Postbus 9150, 7300 HZ Apeldoorn

Staan er fouten in deze brochure?

Ons doel is dat al onze informatie klopt en volledig is. En dat u alles zo goed mogelijk begrijpt. Maar er kan altijd ergens een fout staan. Wij zijn niet aansprakelijk voor eventuele gevolgen van die fout.

Staat er iets anders in de productvoorwaarden?

Uw en onze rechten en plichten staan in de productvoorwaarden. Staat in deze brochure wat anders dan in de productvoorwaarden? Dan gelden de productvoorwaarden.

Bent u niet tevreden? Laat het ons weten.

Bent u het niet met ons eens of heeft u een klacht? Dan horen wij dit graag. We willen u namelijk zo goed mogelijk helpen. Kijk voor meer informatie en ons klachtenformulier op centraalbeheer.nl/klachtdoorgeven. U kunt ook een brief sturen naar: Centraal Beheer Klachtenbureau, Postbus 9150, 7300 HZ Apeldoorn

Meer informatie over Centraal Beheer

Kijk voor meer informatie over ons en ons beleid, onze producten en onze gegevens op centraalbeheer.nl.
Het adres van Centraal Beheer is:
Laan van Malkenschoten 20, 7333 NP Apeldoorn

Contact met Apeldoorn

Stuur een e-mail
info@centraalbeheer.nl

Chat met ons
Dat kan eenvoudig via onze app.

Stuur een brief
Centraal Beheer, Postbus 9150, 7300 HZ Apeldoorn

Bel 'Even Apeldoorn' (055) 579 8421
Dat kan van maandag tot en met vrijdag van 8.00 tot 21.00 uur en op zaterdag van 9.00 tot 16.30 uur. Wij helpen u graag verder.

centraalbeheer.nl/cyber

19030112 19.05