CYBER CRIMINALITEIT BINNEN HET MKB

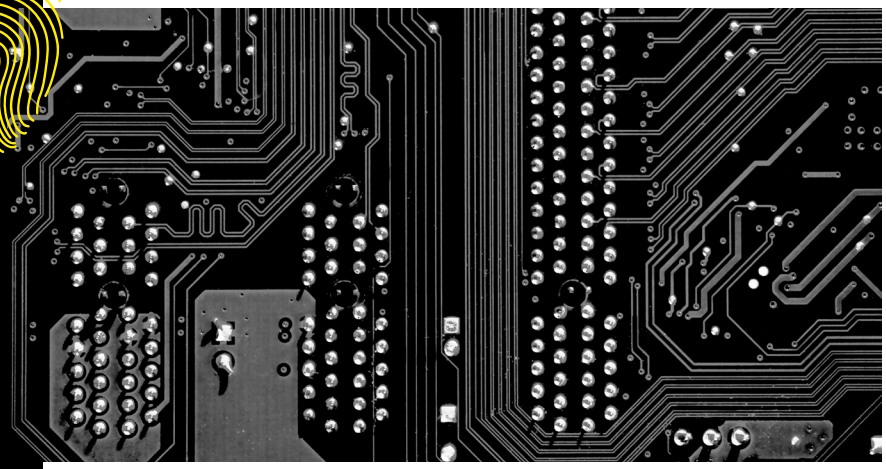
Elk bedrijf moet zich tegen aanvallen van cybercriminelen beschermen. Niks doen, is geen optie!

Terwijl de criminaliteit in de fysieke wereld afneemt, is digitale criminaliteit de afgelopen jaren sterk gestegen[1]. Dat is ook wel logisch omdat de digitalisering van onze maatschappij snel om zich heen heeft gegrepen. Maar criminelen hebben hun weg ook naar het internet gevonden. Tijd dus om maatregelen te nemen! Dat is belangrijk en hoeft niet persé veel tijd te kosten.

In deze folder staan belangrijke tips om je bedrijf tegen cybercriminaliteit te beschermen.

1. WAT IS CYBERCRIMINALITEIT?

Cybercriminaliteit is een veelkoppig monster. Je kan bijvoorbeeld denken aan technische vormen van criminaliteit. zoals een DDoS-aanval waarbij een website onbereikbaar wordt en allerlei vormen van malware zoals virussen en gijzelsoftware. Ook 'ouderwetse oplichting' vindt steeds meer digitaal plaats, zoals betalingsfraude en phishing. Ten slotte zijn er geweldsmisdrijven zoals chantage en bedreiging.



2. HOE RAAKT HET MIJN BEDRIJF?

Dagenlang uit productie door ransomeware.
Het overkomt je omdat cybercriminelen belangrijke gegevens en systemen gijzelen. Je hele bedrijf komt stil te liggen, want alleen door losgeld te betalen aan de criminelen maak je kans om weer bij je gegevens te komen. Wil je een beeld krijgen van wat er speelt in Nederland op het gebied van cybercriminaliteit (in alle sectoren) kijk dan eens op: https://www.digitaltrustcenter.nl/ondernemend-nederland-vertelt

Jouw geld naar criminelen.
Bij deze vorm van digitale oplichting, denk je een factuur te betalen aan een bekende leveranciers of andere bedrijven, maar achteraf blijkt dat je geld hebt overgemaakt naar een crimineel.

Nepbericht van de directeur.
Heb je weleens gehoord van CEO-fraude? Een financiële medewerker krijgt een overtuigend bericht van iemand die zich voordoet als de directeur met het verzoek om met spoed een betaling te doen. De berichten bevatten vaak zeer gedetailleerde informatie over het bedrijf en de directie en zijn daarom moeilijk van echt te onderscheiden. Iedereen kan daarin trappen.

De drie voorbeelden hierboven komen helaas uit de dagelijkse praktijk van ondernemers. Nu denk je waarschijnlijk 'Dat overkomt mijn bedrijf niet! Zo interessant zijn wij niet...'. Uit onderzoek blijkt dat bijna alle ondernemers zo denken. Maar weet je dat niets minder waar is? Ondernemers zijn een zeer aantrekkelijk doelwit voor cybercriminelen. Om slachtofferschap te voorkomen is het dus belangrijk dat jij nu in actie komt om je bedrijf te beschermen!

3. HOE BESCHERM IK MEZELF?

Het begint zoals hierboven al aangegeven bij sterke en unieke wachtwoorden. Naast deze tip heeft het Digital Trust Center speciaal voor ondernemers vijf basisprincipes opgesteld die jou kunnen helpen om slachtofferschap binnen jouw bedrijf te voorkomen: (https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen). Hieronder staan ze alvast kort genoemd.

1. Inventariseer kwetsbaarheden

Hiermee beperk je de digitale risico's en ben je goed voorbereid als je toch slachtoffer wordt. Stel jezelf de volgende vragen:

• Wat is de impact als het internet/systeem er drie dagen, twee weken of een maand uitligt?
• Hoe erg is het als bepaalde gegevens op straat komen te liggen?
• Hoe erg is het als bepaalde gegevens niet meer kloppen?

Moeilijk om die digitale risico's in kaart te brengen? Nee hoor, op https://www.digitaltrustcenter.nl/tools/doe-de-basisscan-cyberweerbaarheid kan je eenvoudig zelf een basisscan invullen. Doe het deze week nog!

2. Kies veilige instellingen

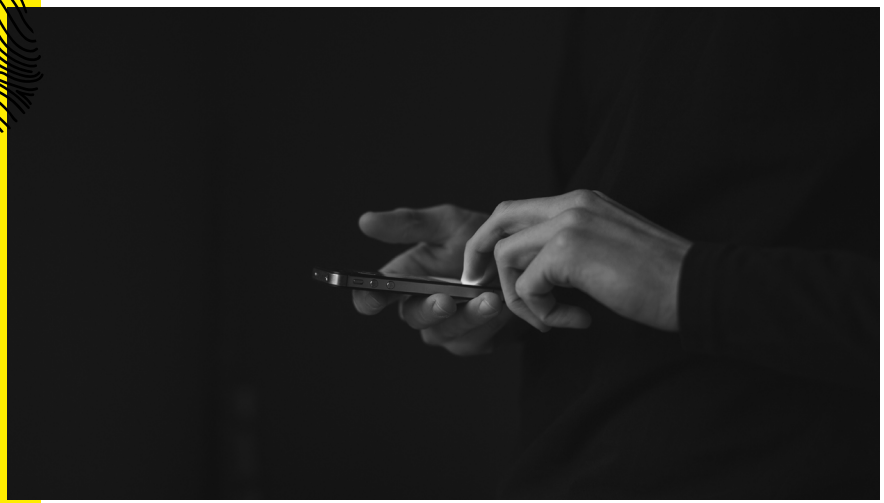
Kijk kritisch naar de instellingen van jouw apparatuur, software en netwerk- en internetverbindingen. Standaardinstellingen zijn niet altijd het meest veilig dus deze kan je aanpassen en ook is het belangrijk om goed te kijken naar functies en diensten die automatisch zijn ingeschakeld. Is dit wel echt nodig?

3. Voer updates uit

Door het installeren van updates worden kwetsbaarheden in software hersteld. Zorg er dus voor dat updates automatisch worden geïnstalleerd, dan kost het je geen tijd. Zo draaien jouw (beveiligings)software en apparaten voortaan altijd op de laatste en dus meest veilige versie.

4. Beperk toegang

Niet iedereen heeft toegang nodig tot alle gegevens van een bedrijf. Bepaal dus per medewerker tot welke systemen en data toegang nodig is om het werk goed uit te kunnen voeren. Verandert iemand van functie? Pas de rechten dan aan!



5. Voorkom virussen en andere malware

Er zijn verschillende manieren waarop je virussen en malware kunt voorkomen: 1) het stimuleren van bewustzijn en veilig gedrag onder medewerkers, 2) een antivirusprogramma gebruiken, 3) apps veilig downloaden en 4) installatiemogelijkheden van software op apparaten van jouw onderneming beperken.

4. TOCH GETROFFEN DOOR CYBERCRIMINALITEIT

Ieder bedrijf loopt het risico om op een dag slachtoffer te worden van cybercriminaliteit. Mocht jouw bedrijf

toch slachtoffer zijn geworden schaam je dan niet, maar kom in actie! Grote kans dat je niet precies weet wat je moet doen. Kijk dan eens op https://www.digitaltrustcenter.nl/informatie-advies/gehackt-wat-nu Op deze website vind je actuele informatie over de stappen die je het beste kan nemen bij slachtofferschap. Hieronder alvast een aantal tips:

1. Maak een herstelplan

Dit is een draaiboek waarin stap voor stap staat beschreven wat je moet doen bij verschillende incidenten. Dit plan kan je dus houvast bieden wanneer jouw bedrijf daadwerkelijk is aangevallen. Print dit plan ook uit zodat het offline beschikbaar is.

2. Zorg voor goede back-ups

Onderzoek samen met je ICT-leverancier hoe binnen jou bedrijf het beste een back-up kan worden gerealiseerd en hoe je deze kunt terugzetten in geval van een aanval met schadelijke software.

3. Doe aangifte bij de politie

Aangifte doen van slachtofferschap kan via 0900-8844 of op een politiebureau bij jou in de buurt. Zorg ervoor dat er geen digitale sporen verloren gaan: zet het apparaat bij voorkeur niet uit en bewaar zoveel mogelijk informatie bijvoorbeeld met foto's of screenshots.

4. Licht de Autoriteit Persoonsgegevens in

Wanneer je te maken hebt met een datalek als gevolg van een aanval van cybercriminelen ben je verplicht om hiervan melding te maken. Bijvoorbeeld na een hack of ransomware aanval. Meer over datalekken vind je op https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

5. Informeer medewerkers, klanten en leveranciers over wat er aan de hand is.

Als jouw bedrijf slachtoffer van cybercriminelen wordt, schaam je dan vooral niet! Het kan elke ondernemer overkomen. Erover praten kan helpen om andere ondernemers bewuster te maken en beschermende maatregelen te laten nemen. Openheid onder ondernemers over slachtofferschap van cybercriminelen is keihard nodig!

Doe bij slachtofferschap van cybercriminaliteit altijd aangifte bij de politie. Dat kost tijd maar met jouw aangifte weten zij wat er speelt, kunnen zij verdachten opsporen en help je andere ondernemers alert te zijn! Je kan de slachtofferschap ook online melden bij de Fraudehelpdesk. Zij kunnen dan andere ondernemers waarschuwen en zo veel ellende voorkomen.

Deze flyer is ontwikkeld in een samenwerking tussen het Veiligheidsnetwerk Oost-Nederland en het lectoraat Maatschappelijke Veiligheid van de Hogeschool Saxion, onder financiering van de Citydeal Lokale Weerbaarheid Cybercrime in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid.