WHITEPAPER

Cybersecurity in het MKB

HOE JE TE WAPENEN TEGEN CYBER GEWELD

Cybersecurity in het MKB

“Matige beveiliging terwijl cybercriminaliteit groeit”

Cyberaanvallen, hacks en digitale lekken zijn regelmatig in het nieuws. Als bedrijf is het geen optie om niets te doen, maar toch krijgt cybersecurity niet de aandacht die het verdient.

“Hoe voorkom je cyberschade aan je bedrijf?”

Datalekken en hacks blijven niet beperkt tot grote bedrijven. Ook de Nederlandse MKB’er loopt steeds meer risico. Reden hiervoor is dat grote bedrijven de beveiliging wel op orde hebben en dat cybercriminelen dus uitwijken naar bedrijven in het MKB. Risico's worden volgens verschillende onderzoeken steeds groter en de aanvallen steeds geavanceerder. Cybercriminaliteit is big business en in handen van goed georganiseer-de bendes. Zij gebruiken verschillende technieken waarmee websites worden stilgelegd en data gestolen of gegijzeld wordt.

In deze whitepaper gaan wij verder in op **cybercrime, cybersecurity**.

Tools van de cybercrimineel

Crypto- en ransomware: cryptoware versleutelt data en ransomware blokkeert toegang tot het systeem. De gijzeling duurt tot er een bedrag is betaald. Crypto- en ransomware wordt naar duizenden e-mailadressen gestuurd. Met een malafide link waar op geklikt wordt of een bijlage komt de malware in het systeem.

Phising: een bijna niet van echt te onderscheiden e-mail waarmee je naar een valse website wordt gelokt en waar gevraagd wordt gegevens in te vullen.

Ddos-aanvallen: leggen computers, volledige netwerken of websites lam door een teveel aan aanvragen.

Virussen: kleine programma's die gegevens op computers beschadigen of verwijderen. Hacking is het inbreken in een computersysteem of netwerk. Hierbij wordt gebruik gemaakt van virussen, spyware, phishing en poortscans.

"Het MKB doet te weinig aan cybersecurity"

Veel bedrijven hebben grote onkosten door cybercriminaliteit dus je zou denken dat cybersecurity hoog op de agenda staat van MKB'ers. Niets is helaas minder waar. De meesten denken geen risico te lopen.

Daarnaast blijkt dat veel bedrijven niet voldoen aan de cyber-security wetgeving volgens de Cyber Security Raad (CSR).

"Het gevaar van cybercrime is een groot probleem"

Het probleem wordt niet herkend door veel bedrijven en zij steken hun hoofd in het zand en worden massaal aangevallen op welke manier dan ook. Dat dit gebeurt is vreemd want de huidige wet- en regelgeving verplicht bedrijven een goede digitale beveiliging te hebben. Word je als bedrijf toch getroffen door cybercrime dan moet je de gevolgen actief beperken om verdere incidenten te voorkomen. Ondernemers blijken hier onvoldoende van op de hoogte en worden aansprakelijk voor de schade die consumenten en andere bedrijven lijden.

"De CSR verwacht dat schade in de toekomst vaker verhaald zal worden op bedrijven"

Weinig kennis van de regels

Het blijkt dat bedrijven dus niet goed op de hoogte zijn van de huidige wetgeving, maar dat ook de nieuwe Europese regels die in mei 2018 zijn ingegaan nog niet overal zijn doorgedrongen.
Meer dan driekwart van de ICT-beslissers in het MKB weet niet goed wat de gevolgen zijn van de GDPR. Nu de GDPR van kracht is moeten bedrijven kunnen aantonen dat de data die ze in datacenters of een cloud buiten de EU opslaan, voldoet aan de eisen van de nieuwe regelgeving.

“Datalekken moeten binnen 72 uur gemeld worden”

Bedrijven moeten persoonsgegevens kunnen wissen van wie daarom vraagt, als er geen geldig tegenargument is. Dat geldt ook als de data is gedeeld met derde partijen. Daarnaast zijn nog tal van andere zaken die verandert zijn. Om de huidige en nieuwe regels na te leven moeten bedrijven weten waar ze de persoonsgegevens bewaren, hoe ze beschermd worden en hoe de verwerking plaatsvindt. Wordt dit niet gedaan dan is er naast imagoschade kans op hoge boetes.

“Cybercriminaliteit wordt een steeds groter probleem”

Het feit dat MKB’ers uitstellen of nalaten iets te doen aan cybersecurity kan ernstige gevolgen hebben voor hun omzet en productiviteit. Uit een onderzoek gepubliceerd in 2016 blijkt dat 60% van de Nederlandse bedrijven vasthoudt aan lokale servers in eigen beheer. Ze zouden risico’s kunnen voorkomen door verouderde software en zwakke firewalls door te lichten.

Toch blijven ondernemers hierin achter en wordt er geen actie ondernomen en komen er steeds meer virussen zoals ransomware en malware. Elk bedrijf heeft de laatste jaren veel data verzameld op de kantoorservers. Projectgegevens, financiële informatie, klantdata, procesinformatie. Data die heel belangrijk is en waarvan je niet wilt dat het op straat komt te liggen.

“Door het toenemende gebruik van mobiele apparaten is een goede securitystrategie heel belangrijk”

Securitystrategie

Goede cybersecurity bestaat uit drie componenten;

Bescherming

Detectie

Reactie

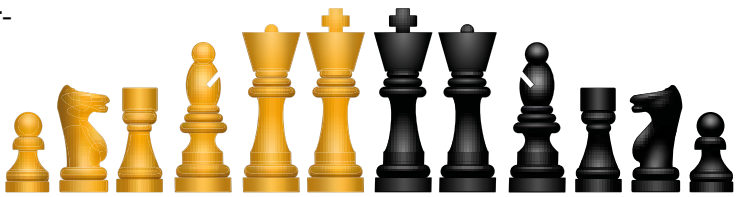
Bescherming Het begint allemaal met bescherming van waardevolle data tegen cyberaanvallen. Dat is mogelijk op 4 niveaus: infrastructuur, identiteit, mobiele apparaten, apps en data. Een veilige infrastructuur zorgt voor een solide basis. Als je grip hebt op bedrijfs- en persoonlijke apparaten zorg je dat je overal veilig kunt werken. Door apps en data extra te beveiligen leg je een extra beveiliging bovenop de wachtwoordbeveiliging.

Infrastructuur: kwaadwillende software dringt binnen via gaten in verouderde software, daarom is up-to-date blijven noodzakelijk. Door alle computers uit te rusten met de nieuwste versies, bug-fixes en patches van alle programma's loopt data in het netwerk het minste risico. Verouderde besturingssoftware van hardware, de firmware kan openstaan waardoor cybercriminelen binnen kunnen dringen. Een computer heeft meerdere ingangen en daar gaat het internetverkeer doorheen. De ingangen staan standaard open ook als ze niet in gebruik zijn. Cybercriminelen kunnen met speciale software veel computers in één keer scannen en zoeken zo naar open poorten.

Identiteit: succesvolle cybercriminaliteit is het gevolg van onoplettendheid van ondernemers. Met phishing-mails worden ze verleid om een prijs te incasseren, of in te loggen op een niet van echt te onderscheiden nepsite. Goed opletten is het motto, of wegklikken van zulke mails die toch door de e-mailscanner zijn gekomen.

Mobiele apparaten**:** mobiele telefoons en laptops zijn bij veel MKB'ers net zo belangrijk als een kantoorserver. Mobiel werken in de nieuwe standaard. Het is daarom handig om het apparaat bij verlies of diefstal op afstand te kunnen wissen. Daar zijn tools voor, en uiteraard zijn de apparaten goed beveiligd met een wachtwoord.

Apps en data**:** virusscanners en firewalls zorgen al voor een goede beveiliging, door apps extra te beveiligen met een wachtwoord of pincode zijn ze veiliger. Data kan via versleuteling worden beveiligd zodat criminelen er niets mee kunnen. Zeker bij privacygevoelige informatie is encryptie aan te raden en is soms zelfs verplicht.



Securitystrategie

Detectie Ondernemers proberen met een firewall of antivirussoftware te voorkomen dat een cybercrimineel binnenkomt. Vaak bevindt de aanvaller zich echter al binnen de muren, de aanval wordt in de meeste gevallen pas na 200 dagen ontdekt en daarna duurt het vaak nog maanden voordat een bedrijf de schade herstelt. Naast imagoschade is het verlies van intellectueel eigendom en persoonlijke gegevens dan al gebeurt. Een constante interne en externe beveiliging is daarom heel belangrijk. Een kenmerk van een hackaanval is dat er volgens een bepaald patroon een serie van e-mails met malware wordt verstuurd. Die schadelijke software kan verstopt zijn in Word of Excel bestanden.

“ Als je veel mail ontvangt uit China of Rusland en je hebt daar geen relatie mee, dan is het verdacht”

Het inrichten van een goed detectie- en preventiesysteem helpt bij het op tijd waarnemen van afwijkingen. Tools die patronen herkennen en proactief gevaren waarnemen.

Reactie de eerder genoemde maatregelen zorgen voor een snelle opsporing en neutralisering van het cybergevaar. Aanvallen worden afgeslagen voordat ze schade aan kunnen brengen. Besmette mobieltjes of laptops kunnen op afstand worden geblokkeerd of gewist en verdachte apps worden niet toegelaten op het netwerk. Gevaarlijke e-mails worden gefilterd voordat ze worden aangeklikt en toegang voor onbevoegden wordt afgesloten.

Loopt mijn bedrijf risico?

Beantwoord de onderstaande vragen en ontdek of jouw bedrijf een makkelijk slachtoffer is van cybercrime.

- ☐ Is uw bedrijf afhankelijk van ICT?
- ☐ Bewaart of verwerkt uw bedrijf vertrouwelijke gegevens van anderen?
- ☐ Zorgt u voor regelmatige updates van uw applicaties/systemen?
- ☐ Is uw website beveiligd met een SSL-certificaat?
- ☐ Maakt u dagelijks een backup van uw gegevens?

“ Als u één of meerdere vinkjes niet kunt invullen loopt uw bedrijf al een groot risico”

Het voorkomen van cybercrime begint dus bij een inventarisatie van de cyberrisicos van jouw bedrijf. Dat gaat verder dan bovenstaande vragen. Met een goed inzicht in de risico’s kun je de juiste beslissingen nemen en de juiste keuzes maken. Dat is essentieel voor de bedrijfscontinuïteit.

Wat kunnen wij voor jou doen?

Wij kunnen helpen om weer een integraal overzicht te krijgen van de beveiliging. Dit doen wij door middel van een scan. Deze scan bevat technische aspecten maar ook organisatorische aspecten. De scan geeft inzicht in wachtwoordbeleid, externe toegang en geeft ook handreikingen om verbeteringen uit te laten voeren.
Het is de bedoeling dat op basis van de aanbevelingen van dit rapport de beveiliging van het netwerk en de organisatie wordt verhoogd.

"Dit doen wij op een praktische manier"

Ook voor privacy management hebben we een Quickscan. Deze kunnen wij ook uitvoeren voor verdergaande verbeteringen bij het omgaan met informatiebeveiliging.
Beveiliging van het netwerk is een momentopname. Bij het professionaliseren van het netwerk is het van belang dat er getest blijft worden. Dit doen wij met een terugkerende APK, hiermee voorkom je dat de hacker met een klein begin een grote impact op je bedrijf kan hebben.

Flevo ict

Tot slot
De beveiligingsscan biedt geen garantie. IT beveiliging is aan veel verandering onderhevig. Wij doen constateringen, die worden verwoord in een samenvatting. Het doorvoeren van de veranderingen die wij aanraden zal er voor zorgen dat het systeem robuuster wordt en minder vatbaar voor de risico's van buitenaf.

"Zijn wij de organisatie die jou verder gaat helpen om risico's te vermijden en veilige toegang tot data te faciliteren?"

Neem contact met ons op om een plan van aanpak te maken.

Flevo ict
de Dieze 26
Dronten
0321 386230
https://flevoict.nl

Ook zijn wij te volgen op de volgende social media

https://twitter.com/flevoict

https://www.linkedin.com/company/flevoict

https://www.facebook.com/flevoict.nl