Microsoft Defender for Office 365

24/7 hulp tegen cybercrime

IRISONE ICT

Vroeg of laat krijgt bijna elk bedrijf ermee te maken: datalekken, gijzelsoftware of virussen gooien roet in het eten, waardoor het werk stopt. Meestal begint de cyberellende met een malafide e-mail. Iemand in het bedrijf let niet goed op en klik, je bedrijf staat stil. Wij helpen je zorgeloos te werken!

In Nederland kost cybercriminaliteit jaarlijks zeker 10 miljard euro. Inmiddels heeft bijna de helft van de kleine en middelgrote bedrijven te maken gehad met cyberaanvallen. Ransomware-aanvallen zijn volgens de Nederlandse politie juist bij het mkb schering en inslag. Ondanks deze impact en groeiende dreiging staat digitale veiligheid nog niet bij elke mkb'er bovenaan de agenda. Steeds vaker zijn het mkb'ers die weken, dagen of maanden niet bij hun data kunnen.

Nederlandse bedrijven zijn extra kwetsbaar

Eigenlijk kan geen enkel bedrijf zich een cyberaanval veroorloven. Want als de IT het niet doet, staat het bedrijf stil en lopen klanten weg. Nederlandse bedrijven lopen voorop in de digitale transformatie en hebben veel bedrijfsmiddelen verbonden met internet. Dat is natuurlijk goed, want daardoor kunnen we snel en efficiënt samenwerken. Het maakt de Nederlandse bedrijven hierdoor wel een gewild doelwit voor cybercriminelen.

Phisingmail grootste oorzaak van geslaagde cyberaanvallen

Meestal gaat het mis bij e-mails met links naar onveilige webpagina's of e-mails met schadelijke bijlagen. De tijd van de krakkemikkig geschreven phisingmails ligt alweer enkele jaren achter ons. De frauduleuze e-mails van nu zijn bijna niet van authentiek te onderscheiden. Tegenwoordig moet je soms wel minutenlang een e-mail controleren op echtheid. Veel ondernemers hebben die tijd niet. Slinkse trucs verleiden ze om toch die bijlage te openen of op die link te klikken. Het klikken op linkjes in phishingmails blijft de grootste oorzaak van alle geslaagde cyberaanvallen.

Altijd een wakend oog

Voor de meeste van ons zou het handig zijn als een IT-specialist alle e-mails checkt voordat ze in je inbox komen. Maar dan wel een IT-specialist die alle wereldwijd verzonden e-mails ziet, zodat die een goede keuze kan maken welke e-mails echt een gevaar vormen voor je bedrijfsvoering. Door je Outlook een beveiligingsupgrade te geven met Microsoft Defender for Office 365, doe je dat precies. Deze cybersecurity-oplossing beveiligt zowel je e-mail van Microsoft 365 als de lokale Outlook.

Microsoft Defender for Office 365 ontmaskert onveilige e-mails

Het checkt niet alleen of de afzender van een e-mail legitiem is, maar ook de links en de bijlagen. Alle berichten worden vooraf in een geïsoleerde omgeving gescreend. Daar wordt bepaald of ze je inbox in mogen. Afhankelijk van het ingestelde beleid worden gevaarlijke e-mails in de map 'ongewenste e-mail' geplaatst, naar een ander e-mailadres omgeleid (dat van IT-beheer) of worden ze in quarantaine gezet. Zo is het meteen duidelijk dat een e-mail een boosaardige intentie heeft. Ook onveilige bestanden in SharePoint, OneDrive en Teams worden op deze manier onschadelijk gemaakt.

Microsoft Defender for Office 365 identificeert gevaarlijk links

Vaak bevatten phishingmails links naar onveilige websites. Klik je daarop, dan kan zomaar je computer gegijzeld worden of dringen ongenode gasten het bedrijfsnetwerk binnen. Microsoft Defender for Office 365 herkent gevaarlijke links. Klik je er toch op? Dan word je doorverwezen naar een veilige pagina van Microsoft met uitleg over het gevaar van de link die je eerder aanklikte.

Tijd voor een veiligheidsupgrade

Wil jij ook zorgeloos e-mailen zonder dat je je hoeft druk te maken om de beveiliging? Dan is een upgrade naar Microsoft Defender for Office 365 iets voor jouw bedrijf. Het beveiligt de e-mail op je vaste computers, smartphones en tablets, zodat je altijd en overal goed beveiligd kan werken.