Altijd goed beveiligd e-mailen

24/7 hulp tegen cybercrime

SAEN-IT
it en telecom dienstverlening

Vroeg of laat krijgt bijna ieder bedrijf ermee te maken: datalekken, gijzelsoftware of virussen gooien roet in het eten en hierdoor ligt het werk stil. Ondanks deze constante dreiging staat digitale veiligheid nog niet bij elk bedrijf met stip bovenaan de agenda. En dit geldt zeker voor het MKB, terwijl hier toch bijna 60% van de cyberaanvallen plaatsvindt. Wij helpen je veilig en zorgeloos werken, zonder dat je altijd achterom hoeft te kijken.

Ze zijn regelmatig in het nieuws: bedrijven die slachtoffer worden van cybercriminaliteit. Groot of klein, elk bedrijf krijgt er ooit mee te maken en hun klanten ook. Misschien stond jij in het voorjaar van 2017 ook met je auto in een Q-Park-parkeergarage en kon je niet betalen... en dus ook niet wegrijden. Dit bedrijf is niet het enige slachtoffer van deze aanval van gijzelsoftware. FedEx, Deutsche Bahn, Renault en recent de Universiteit van Maastricht werden (deels) lamgelegd. De kosten voor de Universiteit van Maastricht worden geraamd op meer dan een miljoen euro. Eigenlijk kan geen enkel bedrijf zich een cyberaanval veroorloven: als de IT het niet doet, staat het bedrijf stil.

Cybercriminaliteit kost miljarden

Wat er in de media verschijnt, is natuurlijk maar het topje van de ijsberg. De schattingen lopen uiteen; van een op
de vijf bedrijven dat slachtoffer wordt tot de helft van de bedrijven. In Nederland kost cybercriminaliteit jaarlijks zeker 10 miljard euro. In de MKB-sector kost een cyberaanval de bedrijven gemiddeld €100.000. Nederlandse bedrijven lopen voorop in de digitale transformatie en hebben veel bedrijfs- middelen verbonden met internet. Dat is natuurlijk goed, want daardoor kunnen we snel en efficiënt samenwerken. Het maakt de Nederlandse bedrijven hierdoor echter 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 crimi-mails van nu zijn bijna niet van authentiek te onderscheiden. Je moet nu wel wat langer naar een e-mailtje kijken om deze te kunnen herkennen als frauduleus. Veel mensen hebben die tijd niet of worden verleid om deze e-mails toch te openen of erin door te klikken. Volgens sommige onderzoeken is bijna 75% van dit onveilige gedrag de oorzaak van alle geslaagde cyberaan- vallen. In elk bedrijf is namelijk wel iemand die op elke link klikt.

Altijd een wakend oog

Voor de meeste van ons zou het handig zijn als een IT-speci- alist 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 Advanced Threat Protection (ATP) doe je dat precies.
Deze cybersecurity-oplossing beveiligt zowel je e-mail van Office 365 als de lokale Outlook.

ATP identificeert gevaarlijk links

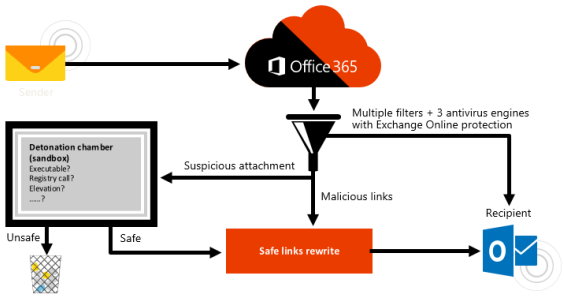
Vaak bevatten phishingmails links naar onveilige websites. Klik je daarop, dan kan zomaar je computer gegijzeld worden of dringen ongenode gasten het bedrijfsnetwerk binnen. ATP herkent gevaarlijke links. Klik je er toch op? Dan word je doorverwezen naar een pagina van Office 365 met uitleg over het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

ATP 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 boosaar- dige intentie heeft. Ook onveilige bestanden in SharePoint, OneDrive en Teams worden op deze manier onschadelijk gemaakt.

ATP ontmaskert onveilige e-mails

Wil jij ook zorgeloos e-mailen zonder dat je je hoeft druk te maken om de beveiliging? Dan is een upgrade naar ATP iets voor jouw bedrijf. Het beveiligt de e-mail op je computer,
op de zaak en op je smartphone of tablet zodat je overal en altijd goed beveiligd kan werken.



Samsonweg 32
1521 RM, Wormerveer
+31 (0)75 3030040
www.saen-it.nl

© 2020 SAEN-IT B.V.