Paul Hermans

Cybersecurity in het mkb

Bijna maandelijks zie je in het nieuws dat er bij een bedrijf een groot beveiligingslek is ontdekt. Denk bijvoorbeeld aan de hackers die op de servers van HBO binnendrongen en maar liefst 1,5 terabyte aan informatie buitmaakten. Zij eisten miljoenen dollars of anders zouden ze nog niet uitgezonden afleveringen van series online plaatsen. Dichterbij huis zijn er genoeg andere voorbeelden. Dit jaar was een groot datalek ontdekt bij de Nationale Goede Doelen Loterijen waardoor meer dan 400.000 persoonsgegevens van deelnemers in handen waren gekomen van een hacker.

Deze bedrijven lijden hierdoor niet alleen imagoschade, maar dit kan ze ook miljoenen kosten. Niet alleen grote organisaties hebben hiermee te maken. Cybersecurity moet ook door mkb-bedrijven serieus worden genomen. Juist voor hen kan een groot beveiligingslek ernstige schade aanrichten. Je kunt het vertrouwen van je klanten verliezen. En wat als de financiële schade te hoog oploopt? Dan kan het wel eens zijn dat je je bedrijf moet sluiten. Dit wil je natuurlijk voorkomen. Maar wat kan je tegen zo'n lek doen? En waar begin je eigenlijk?

Cybersecurity begint bij het ontdekken van zwakke punten in je omgeving. Waar zitten de gaten? We hebben hiervoor tests om je omgeving te scannen. Door zogenaamde hacks uit te voeren, ontdekken we waar de veiligheidsproblemen zitten. Dit kan op verschillende niveaus, zoals het netwerk, de endpoints of de firewall. Deze scans zijn ook verkrijgbaar in een SaaS-oplossing, Managed Security Services, zodat je omgeving regelmatig kan worden getest. Cybercriminelen vinden steeds sneller nieuwe manieren om binnen te dringen. Daarom is het belangrijk om continu te testen of je omgeving nog wel veilig is.

Als je je zwakke punten eenmaal kent, is het nemen van maatregelen de volgende stap. De rapporten die uit de scans komen, kunnen partners of onze security-consultants laten analyseren. De partners of wij koppelen de beveiligingslekken vervolgens aan bepaalde security-oplossingen die bescherming bieden tegen bijvoorbeeld malware, ransomware en geavanceerde online bedreigingen. Moderne security-oplossingen zorgen ervoor dat je omgeving op verschillende niveaus optimaal beveiligd is.

Oplossingen implementeren is één ding, maar je medewerkers en het beleid dat je erop nahoudt, moeten niet worden vergeten. Je kan een hele veilige omgeving hebben, maar als medewerkers onvoorzichtig met gegevens omgaan, dan liggen beveiligingslekken alsnog om de hoek. Tijdens security-trainingen wordt dit en nog veel meer uitgelicht. Denk hierbij onder meer aan de diverse cyberaanvallen en hoe je deze kunt bestrijden. Maar wanneer er eenmaal een veilige omgeving is, krijgt ook deze aandacht. Denk aan het cybersecurity-beleid en alle processen die daarbij horen. Ook al komen beveiligingslekken bij mkb-bedrijven minder vaak in het nieuws, juist deze bedrijven moeten cybersecurity serieus nemen.

***Paul Hermans** is senior sales manager Software & Cloud Benelux bij Ingram Micro Cloud.*
***Reageren?** Paul.Hermans@ingrammicro.com*