

Cybersecurity in het MKB is onvoldoende voorbereid op ransomware-aanval, zegt ING



Het Nederlandse MKB heeft een probleem met de cybersecurity, die is in veel gevallen ruim onvoldoende in vergelijking met de toenemende dreiging van cyberaanvallen met bijvoorbeeld ransomware. Dat blijkt uit onderzoek van [ING](#).

Maar de oorzaak van dat probleem is niet alleen toe te schrijven aan de MKB'ers. Ook de IT-dienstverleners zijn hier medeschuldig aan. Bedrijven zijn door de complexe oplossingen toegewezen op cybersecurity-experts, maar die kunnen de vraag niet aan. Daardoor komen de ondernemers vaak uit bij **IT-dienstverleners, maar die kampen met een tekort aan kennis en kunnen die moeilijk vinden.**

Volgens ING is het logisch dat IT-dienstverleners doorgroeien naar beveiliging, maar dan moeten ze er wel in investeren. Iets wat het volgens de bank zeker waard is, want er zou tot 2025 ruim 11 miljard euro aan uitgegeven worden. In 2020 was dat nog maximaal 7 miljard euro.

Toenemende cyberdreiging voor bedrijven

Aan de andere kant stijgen de inkomsten van cybercriminelen ook nog steeds. Door de inzet van bijvoorbeeld populairder wordende ransomware, waarmee bestanden op computers worden versleuteld tot het slachtoffer betaald, zorgden de dieven voor een schadepost van tussen de 8 tot 12 miljard euro, schat ING.

ING zag sinds de tweede helft van 2019 een toename van meer dan 300 procent in aanvalspogingen met ransomware. Tussen juli en december van 2019 kwam de teller uit op net geen 100.000. In de eerste helft van 2021 waren dat er ongeveer 300.000.

De grootste schade is volgens de bank overigens niet het door de criminelen geëiste bedrag (want dat zou je nooit moeten betalen), **maar het verlies aan omzet tijdens de aanval, de opgelopen reputatieschade en de investering die nodig is om na de aanval alles weer op orde te krijgen.**

Daarbij wordt het voor bedrijven steeds moeilijker om zich goed te beveiligen tegen deze dreigingen. Het dievengilde zit niet stil en ontwikkeld steeds geavanceerdere aanvalstechnieken en professionaliseert tegelijkertijd in de aanpak. Bedrijven en organisaties hebben dus aanzienlijk meer beveiliging nodig, met name in het monitoren van risico's, stelt ING.