

'Bedrijven hebben behoefte aan meer dan alleen antivirusbeveiliging'

F-Secure introduceert nieuwe securitydiensten

Steeds vaker zien we dat naast grote organisaties, juist ook het midden- en kleinbedrijf het slachtoffer van cyberaanvallen wordt. Daarom heeft het Finse F-Secure zich in de Benelux ontwikkeld tot een allround beveiligingsleverancier voor zowel grote ondernemingen en kleine en middelgrote bedrijven, met oplossingen voor het voorspellen, het voorkomen, het detecteren en het reageren op beveiligingsincidenten.

Tekst Edwin Feldmann

We zien dat vooral het midden-segment van het mkb steeds meer het slachtoffer is van geavanceerde cyberaanvallen", zegt Aart Jonkers, country sales manager voor de Benelux bij F-Secure. Die bedrijven hebben doorgaans ook data die voor criminelen interessant zijn, maar minder geavanceerde IT-beveiliging.

Als reactie op de cyberaanvallen die steeds geavanceerder worden, onafhankelijk van de grootte van een bedrijf, heeft F-Secure zijn strategie aangepast. Het beveiligingsbedrijf dat dit jaar 30 jaar bestaat, leverde jaren geleden vooral producten en diensten die gericht waren op het voorkomen van datalekken en hacks (preventie). Tegenwoordig bestaat IT-beveiliging volgens Jonkers uit vier elementen. Naast preventie gaat het ook om het voorspellen van het risico (predict), het detecteren van gevaren en het reageren op een security-incident (response). Dat is waar F-Secure tegenwoordig producten en diensten voor ontwikkelt.

Detection & Response

Voor de bovenkant van de markt biedt F-Secure zijn managed-securitydienst genaamd Rapid Detection Service; een door F-Secure gemanagede service. "Klanten worden 24/7 door ons

gemonitord en als er breaches worden gedetecteerd, hanteren wij een SLA van 30 minuten om deze te melden. We kunnen deze ook voor hen oplossen, samen met de partners via wie wij deze dienst leveren."

'Het alleen voorkomen van cyberaanvallen is niet meer voldoende'

Voor de middelgrote en kleinere ondernemingen brengt F-Secure later dit jaar EDR op de markt. EDR is een 'endpoint detection and response'-oplossing die niet direct door F-Secure wordt gemanaged, maar door de channelpartners. "Het is eigenlijk de 'unmanaged' variant van RDS", vertelt Jonkers.

Bij een breach is het bij EDR-klanten afhankelijk van de kennis van de klant of hij zelf het incident oplost of dat de partner dat doet (managed). Juist binnen het mkb besteden bedrijven vaak hun IT-zaken uit aan resellers die voor hen de IT-specialist zijn.

Rol van partners

Het op de markt brengen van EDR gebeurt ook volledig via het resellerkanaal, zo vertelt Jonkers. "We zijn een channelorganisatie omdat we een heel grote rol zien weggelegd voor partners. Als partner krijg je de kans om iets te kunnen toevoegen aan de producten en diensten die we bieden, zoals klanten helpen bij het inrichten van de beveiliging en optreden bij security-incidenten."

"Wat ons daarbij uniek maakt, is onze 'live-security'-benadering", stelt Jonkers. "We hebben technische experts in dienst die bij enterpriseklanten als securityconsultants over de vloer komen. Zij zien direct nieuwe ontwikkelingen en die 'live-kennis', expertise en adviezen voegen wij toe aan onze producten en diensten voor de beste up-to-date bescherming. Voeg daar slimme technieken op basis van artificial intelligence en big data aan toe en je hebt de ideale combinatie van mens en machine, bij ons genaamd het Live Security-concept." «



De vier aspecten van cybersecurity