Interview | Edwin Feldmann

F-Secure: van niche speler naar breed inzetbare cybersecurityleverancier

‘Klanten moeten kunnen vertrouwen op security-partners’

Het tekort aan securityspecialisten treft de hele branche. Niet alleen de IT-security-leveranciers maar ook hun resellers en distributeurs hebben moeite om aan getalenteerde securitydeskundigen te komen. En dat is lastig voor bedrijven die niet enkel veelvoorkomende aanvallen willen voorkomen, maar ook geavanceerde en gerichte aanvallen willen weren. “Gebrek aan specialisten wordt één van de grootste problemen voor bedrijven op het gebied van cybersecurity.”

“Mkb-bedrijven beschikken wel over interessante data voor hackers, maar ze hebben niet de geavanceerde beveiliging die midden- en grote ondernemingen vaak hebben omdat ze geen medewerker in dienst hebben die fulltime met IT-security bezig is. Daarom zijn ze vatbaar voor geavanceerde hacks en aanvallen”, aldus Aart Jonkers, Country Sales Manager Corporate Sales Benelux bij F-Secure. Voor de goede beveiliging vertrouwen velen daarom blind op hun ICT-partners. De tools en kennis van partners is daarom heel belangrijk, stelt Jonkers.

In 2013 was F-Secure nog erg bezig met de producten waarmee consumenten en bedrijven konden voorkomen dat ze te maken kregen met cyberincidenten. En dat gold niet alleen voor F-Secure, heel de markt investeerde sterk in die prevent-oplossingen, aldus Jonkers. “Bedrijven hebben doorgaans wel goede producten om cyberaanvallen gebaseerd op commodity threats te voorkomen, echter zien we steeds vaker geavanceerde en gerichte aanvallen welke geavanceerdere cyberbeveiligingstechnieken vereisen”, weet Jonkers.

De strategie die F-Secure sinds enige tijd aan partners probeert over te brengen, gaat over de hele security-cyclus. F-Secure deelt informatiebeveiliging in vier fases: predict, prevent, detect en respond. In de eerste fase wordt een risicoprofiel gemaakt van een bedrijf. Een bakker heeft bijvoorbeeld een ander risicoprofiel dan een verzekeraar. Vervolgens worden er in de prevent-fase maatregelen genomen om te voorkomen dat je slachtoffer wordt van een cyberincident. Dat heeft jarenlang bestaan uit het beveiligen met antivirussoftware, spamfilters en firewalls. Hoe goed die producten ook mogen zijn, het bedreigingslandschap verandert.

“We zien steeds meer geavanceerde en gerichte aanvallen. Een dergelijke aanval of datalek uitsluiten is zeer lastig met enkel preventieve oplossingen en dus moeten er ook detect-oplossingen worden ingezet om een eventuele cybercrimineel te ontdekken als die er toch in slaagt om de beveiliging te omzeilen. En indien nodig moet er gereageerd kunnen worden om een mogelijke aanval alsnog af te slaan (respond-fase). Daarom heeft F-Secure dit jaar RDR op de markt gebracht, wat staat voor Rapid Detection & Response.”

Meer bewustwording

Wel ziet Jonkers dat de bewustwording bij bedrijven de afgelopen jaren flink is gestegen. Steeds meer bedrijven beseffen dat alleen het voorkomen van cybercincidenten niet voldoende is. De kans is groot dat elk bedrijf een keer slachtoffer wordt van een hack of cyberaanval, en dus moeten ze zich ook beveiligen met detectie- en respond-oplossingen. Hij ziet het als een taak van F-Secure om die boodschap nog verder in de markt te verspreiden.

Sinds april 2013 heeft F-Secure zelf een hele transitie ondergaan, van endpoint-protectiebedrijf naar volwaardige cybersecurity- vendor/leverancier. Jonkers: “Persoonlijk ben ik trots op de ontwikkeling van F-Secure in de Benelux, op wat we samen hebben bereikt en op alles wat ik daaraan heb kunnen bijdragen.” Hij heeft er alle vertrouwen in dat het bedrijf de huidige groei de komende jaren kan continueren.

www.f-secure.nl | 030 602 0110 | twitter.com/FSecure