BIG DATA, BI EN IOT

SECURITY-PARTNERS KUNNEN MET RDR EENVOUDIG HUN VERKOOPMODEL UITBREIDEN

Aart Jonkers
country sales manager
F-Secure Benelux

Het accent van endpointsecurity heeft jarenlang gelegen op preventieve maatregelen, maar cyberincidenten uitsluiten kan niemand. Om te voorkomen dat het toch mis gaat, biedt het Finse F-Secure middelgrote- en grote bedrijven een nieuwe beveiligingsoplossing: Rapid Detection & Response (RDR).

Tekst Edwin Feldmann

RDR is half mei onthuld in het bijzijn van een groot aantal partners. Als we spreken met Aart Jonkers, country sales manager voor F-Secure Benelux, is hij nog in Londen is voor het tweedaagse partnerevent Species. “Hier laten we natuurlijk aan Nederlandse en Belgische partners zien wie we zijn en wat we doen, met een hoop interessante keynotes. Maar belangrijker nog is de introductie van Rapid Detection & Response. Dit is F-Secure’s nieuwste endpoint detection & response (EDR)-oplossing die bedrijven zonder grote IT- en beveiligingsteams de geavanceerde mogelijkheden biedt om zich te beschermen tegen gerichte cyberaanvallen”, legt Jonkers uit. Het bijzondere aan RDR is dat het via partners gemanaged wordt. Dit betekent een nieuw en interessant verdienmodel voor security-resellers.

De Finse beveiligingsspecialist F-Secure combineert met de nieuwe RDR-oplossing de beveiligingskennis van zijn experts met geavanceerde technologie, zoals artificial intelligence. Dit helpt bedrijven om allerlei soorten cyberaanvallen, pogingen om toegangsrechten te bemachtigen en andere slimme tactieken van cybercriminelen te detecteren. “Lang gingen vendoren ervan uit dat het mogelijk was om te voorkomen dat je met een cyberincident te maken krijgt”, zegt Jonkers. “Inmiddels weten we dat je dat nooit helemaal kunt uitsluiten.

Dit kan bijvoorbeeld gebeuren door het ontbreken van voldoende bewustzijn bij mensen, of omdat het op zo’n manier gebeurt dat het je het niet kunt tegenhouden, of omdat er gewoon fouten gemaakt worden.” Volgens Jonkers realiseren bedrijven zich nu steeds meer dat het noodzakelijk is om niet alleen preventieve maatregelen te nemen, maar ook maatregelen waarmee zij (via de partners) aanvallen kunnen detecteren. Daar is het nieuwe product RDR op gebaseerd.

Het risico van een gerichte aanval

Volgens een recent onderzoeksrapport van F-Secure vertegenwoordigden gerichte aanvallen ruim de helft van alle beveiligingsincidenten. Bijna 80 procent van alle onderzoeken ging van start nadat de beveiliging aan de netwerkrand (zoals firewalls) reeds was doorbroken. Bedrijven kregen daardoor te maken met gegevensdiefstal, fraude en andere onwenselijke zaken. Met F-Secure Rapid Detection & Response kunnen bedrijven die zelf geen IT-beveiligers in dienst hebben, dus toch tijdig incidenten signaleren en er adequaat op reageren. Als de oplossing een geavanceerde bedreiging detecteert, krijgt de klant via de managed-serviceprovider (MSP) aanbevelingen over hoe er het beste kan worden gehandeld. Bij het optreden tegen cyberincidenten is dus een belangrijke rol weggelegd voor partners van F-Secure, stelt Jonkers. “Technisch zorgt F-Secure ervoor dat incidenten daadwerkelijk gedetecteerd en opgelost kunnen worden. Voor onze kanaalpartners betekent het dat zij extra diensten aan hun klanten kunnen leveren en daarmee hun eigen businessmodel kunnen uitbreiden”, besluit Jonkers. Bovendien is een voordeel dat de oplossing samenwerkt met elke endpoint-beveiliging, ongeacht de fabrikant. Dus elke partner kan RDR aanbieden bovenop zijn eigen endpoint-detectieproducten. «

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