Endpoint Protection: Dynamisch beveiligen tegen steeds slimmere cybercriminelen

Partner Content
Rootsec

Hof van Twente, Randstad en het Europees Medisch Agentschap. Een kleine greep uit de organisaties die de afgelopen twee weken slachtoffer werden van een cyberaanval. Het cybersecurity landschap is enorm veranderd. Niet alleen speelt anno 2020 de business zich voor een groot deel online af, cybercriminelen maken daarnaast gebruik van steeds geavanceerdere methodieken en oplossingen die dankzij het dark web bovendien vrij toegankelijk zijn voor iedereen.

Alex Nijland
Business Development Manager
Rootsec

Het is bijna letterlijk een wapenwedloop geworden waarbij met enkel een firewall, antivirussoftware of periodieke test veiligheid niet of nauwelijks meer gegarandeerd kan worden. Bij alle organisaties die recentelijk slachtoffer zijn geweest waren deze oplossingen aanwezig en toch kon het hier mis gaan. Hoe is dat mogelijk? Ten eerste kunnen deze oplossingen alleen dreigingen scannen en filteren die ze als zodanig herkennen, waarbij nieuwe varianten toch ongezien door de mazen glippen. Ten tweede doen deze defensieve ook niets wanneer cybercriminelen zich reeds toegang hebben verschaft tot uw interne netwerk, systemen en data. Dat maakt deze oplossingen niet slecht, alleen zijn de cybercriminelen sneller, slimmer en effectiever geworden in hun aanpak.

Met meer dan 10 jaar aan ervaring binnen de cybersecurity zijn onze experts gewend aan verschuivingen binnen de markt. Zo kregen wij de afgelopen tijd vanuit onze klanten steeds vaker vragen over de mogelijkheid van een proactieve(re) manier van beveiligen. Daarom hebben wij onze dienst genaamd “Endpoint Protection” geïntroduceerd. Een endpoint is bijvoorbeeld een laptop, werkstation, server of IoT-apparaat. Endpoint Protection voeren wij uit vanuit het Security as a Service (SaaS) principe, oftewel een oplossing in de vorm van een licentiemodel dat past bij elke organisatie ongeacht omvang.

Endpoint Protection is een constante en actieve monitoring en beveiliging van uw endpoints tegen virussen, malware, ransomware, phishing, datadiefstal en interne dreigingen. Het kan het beste gezien worden als een offensieve laag van extra beveiliging die aanvallen op uw endpoints detecteert, blokkeert of dreigingen voorkomt. Een essentiële laag, want maar liefst 70% van alle cyberaanvallen beginnen bij een de gebruiker.

Onze Endpoint Protection, beschikt dankzij Artificial Intelligence (AI) over een slim stel hersenen. Dit stelt de software in staat om ook nieuwe varianten van virussen en/of hackmethodes te herkennen omdat ze kijkt naar patronen en afwijkend gedrag. Dreigt een gebruiker een gevaarlijk bestand te openen of heeft een hacker zich toegang verschaft tot uw systemen? Dan grijpt onze Endpoint Protection meteen in.

Onze 24/7 helpdesk bewaakt en optimaliseert dit proces continu om zo de hoogste kwaliteit en precisie te behouden. Cybercriminelen zijn immers op elk tijdstip actief en het geeft de klant een veel veiliger gevoel. Inmiddels hebben wij deze oplossing met veel succes uitgerold bij diverse bedrijven en overheden. We houden de instap erg laagdrempelig. Al vanaf 25 endpoints per maand verzekert u zich van veiligheid en service van de bovenste plank voor elk bedrijf, ongeacht de grootte.

ROOTSEC