

Waarom een IT-securitystrategie op preventie zinloos is

22-02-2017 11:13



Door Rob Pronk
Regional director Northern Europe bij LogRhythm

Ze installeerden voor 1,6 miljoen dollar aan malwaredetectiesystemen, maar werden enkele maanden later toch slachtoffer van een enorm datalek dat hen een half jaar later al een slordige 129 miljoen dollar kostte. De impact van de cyberaanval was voor de Amerikaanse retailer Target enorm. Van veertig miljoen klanten waren de creditcard- en betaalkaartgegevens gestolen. Kort na de diefstal daalde het Target-aandeel met elf procent en in het eerstvolgende kwartaal daalde de winst met zestien procent. De juridische kosten zijn daar nog niet in meegerekend.

Het IT-landschap in de retail is steeds gevarieerder en complexer geworden. Zo heeft het Internet of Things zijn intrede gedaan, en maken medewerkers gebruik van eigen devices en op cloud-gebaseerde applicaties die vaak onder de radar blijven. Door die complexiteit enerzijds en de geraffineerdheid van hackers anderzijds is een strategie waarbij puur ingezet wordt op het voorkomen van aanvallen zinloos. Uit onderzoek van Trustwave blijkt namelijk dat van alle aanvallen 71 procent ongedetecteerd blijft. Bedrijven die een aanval wel weten te onderscheppen, doen dat gemiddeld pas na 87 dagen. En dan duurt het nog een week voordat ze daarop weten te reageren. Tegen die tijd is er al een hoop schade aangericht. Denk aan alle persoonsgegevens, intellectueel eigendom of commerciële informatie die in verkeerde handen kunnen zijn gevallen.

Dergelijke cijfers klinken misschien schokkend, maar vormen wel de nieuwe werkelijkheid. Volgens Gartner verkeren bedrijven in 2020 in een staat van permanente bedreiging, waarbij ze niet in staat zijn geavanceerde aanvallen af te wenden. Gartner-VP Neil MacDonald gelooft dan ook dat er een verschuiving plaatsvindt in de securityfocus. Waar nu het merendeel van de kosten vooral aan preventie wordt besteed, zal dat in de toekomst meer en meer in snelle detectie en respons worden gestoken. Want nu gebeurt het nog regelmatig dat dure software wel een verdachte activiteit meldt, maar dat die niet wordt opgevolgd.

Natuurlijk moet antivirussoftware up-to-date zijn en zijn firewalls heel belangrijk, maar bedrijven moeten méér doen. Vanwege de enorme hoeveelheid informatie die we tegenwoordig tot onze beschikking hebben, gaat het nogal eens mis bij het identificeren wat een bedreiging en wat gewoon ruis is. Target kreeg bijvoorbeeld wel degelijk een melding van een mogelijk lek, maar die raakte zoek tussen alle andere meldingen.

Door te kiezen voor Security Intelligence wordt het mogelijk slimme analyses te maken. Security Intelligence stelt organisaties in staat bedrijfsgegevens te verzamelen. Een effectief Security Intelligence-platform zorgt waar mogelijk voor automatisering en helpt organisaties belangrijke data te 'vangen' en daar vervolgens correlaties, visualisaties en analyses op toe te passen. Een enkele gebeurtenis, zoals een gebruiker die inlogt vanaf een filiaal in Amsterdam, kan op zichzelf onschuldig lijken. Maar als diezelfde gebruiker tien minuten daarvóór nog dertig kilometer verderop was ingelogd, moeten de alarmbellen gaan rinkelen. Het correleren van data met contextinformatie, maakt de kans op het juist identificeren van een aanval groter en de tijd die het kost om een bedreiging te detecteren en erop te reageren, juist korter.

Het principe van Security Intelligence is in de basis zeer eenvoudig en bestaat uit vijf opeenvolgende processen: detecteren van de bedreiging, kwalificeren van de bedreiging, onderzoeken van de impact ervan, het beperken of elimineren van de dreiging of aanval en het herstellen van de schade. Slechts één ineffectieve stap kan echter al zorgen voor een flinke afname van de algehele effectiviteit. Denk daarom aan een krachtig Security Intelligence-platform. Dit maakt een gestroomlijnde workflow mogelijk en stelt de organisatie in staat om snel en adequaat een aanval in de kiem te smoren.