Bernard Schep, Regional Sales Manager Benelux A10 Networks

‘Er komt een vloedgolf aan devices op ons af’

De nieuwe werkplek heeft netwerkbeveiliging nog uitdagender gemaakt dan het al was. Tel daar de apparatenexplosie bij op die 5G gaat veroorzaken, en je krijgt een ingewikkelde puzzel. De sleutel ligt volgens A10 Networks niet bij het eindpunt, maar bij de provider.

Tekst Michiel van Blommestein

In 2024 zal het aantal IoT-apparaten met een mobiele verbinding zijn uitgedijd tot 4,1 miljard wereldwijd. Tot zover stipt een nieuwe rapport van A10 Networks niet veel verrassends aan. Maar wat erbij komt is dat de bandbreedte van deze apparaten in één keer enorm toeneemt als 5G eenmaal wordt uitgerold. Bovendien krijg je veel meer direct verkeer tussen mobiele apparaten. En daarom moeten dienstverleners zich snel gaan aanpassen, zo zegt Bernard Schep, Regional Sales Manager Benelux en Nordics bij A10 Networks. “Bij direct verkeer gaat het niet meer via een centraal punt. In zekere zin valt de radiotoren weg die het allemaal coördineert en inspecteert.” Door mobility wordt ook steeds vaker toegang tot de backbone gezocht via particuliere netwerken. “Serviceproviders worden in toenemende mate verantwoordelijk gehouden”, zegt hij. “Thuisnetwerken maken immers uiteindelijk deel uit van het netwerk van de provider. Je genereert geïnfecteerd verkeer vanuit botnets.”

De deuren moeten dus aan de netwerkkant dicht. Build a wall, dus. ”Maar dan niet letterlijk”, lacht Schep. “Zonder het te weten wordt je apparaat geïnfecteerd. Als gebruiker en als bedrijf zal je merken dat je applicatieprestaties slechter worden. Je ziet het niet, je weet het niet.” Een manier waarop A10 het probleem bestrijdt is door een detector te zetten op versleuteld verkeer. “Als dat op het punt staat het bedrijfsnetwerk te verlaten, dan decrypten we het eerst en voeren het verkeer eerst langs allerlei security-systemen. Alleen als het verkeer echt veilig is, encrypten we het weer en geven we het verder door.

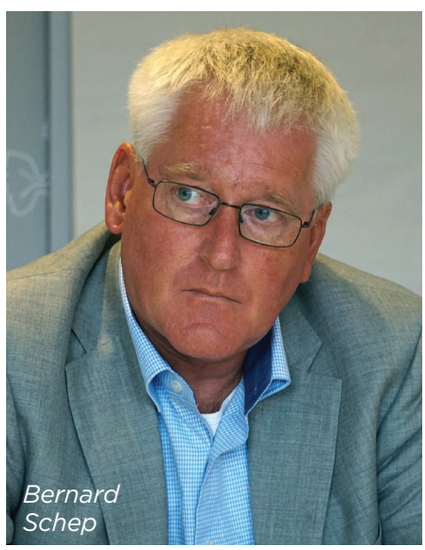
‘Serviceproviders worden in toenemende mate verantwoordelijk gehouden’

Dit noemen we SSL-inspectie. Je kunt dan als serviceprovider beter garanderen dat jouw verkeer geen schade toebrengt en geen kritische bedrijfsinformatie naar buiten verdwijnt.”

Single sign-on

Het mechanisme wordt steeds belangrijker, want er zijn nogal wat slimme apparaten binnen bedrijven en huishoudens. “Er komt een vloedgolf van apparaten onze kant op”, zegt Schep. Bovendien wisselen steeds meer apparaten regelmatig van netwerk. Denk aan laptops en tablets van thuiswerkers. “We hebben daar ‘single sign-on’-oplossingen voor. Onafhankelijk van de infrastructuur en onafhankelijk van waar vandaan iemand je cloud benadert, weet je wie toegang heeft met welke rechten.”

Het is echter niet zo dat A10 alles kan bieden. “Je kunt niet alles zelf doen. Het is ook onze kracht dat we een groot partnernetwerk hebben met andere leveranciers. We integreren onze producten onderling, en tijdens de ontwikkeling wordt daar ook rekening mee gehouden.” Als voorbeeld noemt Schep de grote firewall-leveranciers. “Dat zijn partijen die heel goed zijn in het detecteren van vriend en vijand, wat ze moeten doorlaten en wat blokkeren”, zegt hij. “Maar zij zijn minder geschikt voor grootschalige encryptie en decryptie. Als je dat op de firewall probeert, krijg je een forse daling van de capaciteit en mogelijk te maken met aanzienlijke vertragingen. Die taak kunnen wij van hen overnemen.” «


Bernard Schep

www.a10networks.com | bschep@a10networks.com | 065 151 8486