NDIX STAAT VOOR CONNECTIVITEIT WAAR JE OP KUNT VERTROUWEN

Afgeschermd netwerk en 24/7 dienstverlening garanderen veiligheid en betrouwbaarheid

Het gebruik van publieke cloud services, remote datacenters en nevenvestigingen trekt een wissel op de beveiliging van bedrijfsdata. Een veilige dataverbinding, bij voorkeur privaat, is dan cruciaal. NDIX is in dit gat gesprongen en helpt klanten aan private verbindingen met de hoogste beveiliging mogelijk. *Tekst: Hans Steeman*

De afgelopen jaren is de manier waarop bedrijven met data omgaan flink veranderd. Steeds vaker worden voormalige on-premise IT-omgevingen ondergebracht bij een externe serviceprovider. Ook is het voor grotere concerns nodig alle vestigingen met elkaar te verbinden (peering). Om dit alles in veilige banen te leiden zijn versleutelde verbindingen (VPN's) via het internet eigenlijk niet veilig genoeg. Veel beter is een private verbinding. Het Nederlands/Duitse bedrijf NDIX uit Enschede faciliteert dit. ChannelConnect sprak met Dylan van Dijk, innovation- en risk manager bij NDIX en Dennis Seppenwoold, project- en key account manager bij NDIX, over het ontstaan van NDIX en de oplossing die zij hun klanten van het netwerk kunnen bieden.

Al 20 jaar actief

Zo'n 20 jaar geleden kwam het idee op om private verbindingen te gaan exploiteren. Hackers kunnen geen toegang tot private verbindingen krijgen, waardoor deze dus intrinsiek veilig zijn. Dylan van Dijk: "In die tijd was dat een dure maar wel een veilige manier van verbinden met een gegarandeerde bandbreedte. Bandbreedte en hoge kosten gingen hand in hand met veiligheid en betrouwbaarheid." Vanuit de universiteit Twente kwam het idee om op netwerklaag 2 (OSI-model) via een beheerd netwerk een ethernetverbinding beschikbaar te stellen. Hierop kunnen klanten hun VLAN's gebruiken. Sinds die start is er veel veranderd. Uitgangspunt is inmiddels darkfiber dat NDIX exploiteert. In Nederland zijn er 90 switch locaties. Naast Nederland is men ook in een deel van Duitsland (Nordrhein-Westfalen en Nedersaksen) actief.

Colocatie ruimte bij Equinix Nederland (bron: Equinix)

De klanten van NDIX krijgen op hun locatie een darkfiber vezel aangeleverd en kunnen die zelf belichten. Is er nog geen glasvezelaansluiting aanwezig, dan moet via een lokale serviceprovider eerst een verbinding met de meest nabije switch locatie worden aangelegd. Seppenwoold: "We leveren de klanten een private darkfiber vezel en garanderen daarop een bandbreedte. Hoeveel data men daarover verstuurt is niet belangrijk, de klant betaalt enkel voor de beschikbaar gestelde bandbreedte."

> **'We leveren de klanten een private darkfiber vezel met garandeerde bandbreedte'**

Het glasvezelnetwerk wordt door NDIX beheerd en ondersteund met een marktplaats voor diensten. De switch locaties waar het verkeer samenkomt worden streng bewaakt en elke poging om aan een verbinding te rommelen of het netwerk te benaderen wordt direct gedetecteerd. Daarmee kan gegarandeerd worden dat hackers nooit fysiek toegang krijgen tot een klantvezel. Hacken via het internet is principieel niet mogelijk, omdat er geen verbinding met internet is.
Speciaal voor gebruikers van Microsoft Azure en Amazon AWS verzorgt men directe aansluitingen op deze domeinen via Microsoft Azure ExpressRoute en Amazon AWS Direct Connect. Zo wordt de klant met maximale veiligheid verbonden met het domein van de serviceprovider. Er zit geen internet of derde partij tussen hem en de cruciale bedrijfsdata. Ondersteuning van het Border Gateway Protocol (BGP) realiseert directe toegang tot andere datacentra. Bedrijfslocaties kunnen via een Ethernetpad (peering) met elkaar verbonden worden. ■