SONICWALL, ALS HET OP VERTROUWEN AANKOMT

Zero Trust is dé manier om indringers buiten te houden

Met het steeds ambulanter worden van medewerkers krijgt netwerkbeveiliging te maken met nieuwe uitdagingen. Naast username en wachtwoord zijn steeds meer andere aspecten relevant. Een goede beveiliging houdt ook rekening met het te verwachten gedrag van een medewerker. Dan komt Zero Trust om de hoek kijken. ChannelConnect sprak met senior channel accountmanager Dennis Dielemans van SonicWall over de oplossing die zij in petto hebben. *Tekst: Hans Steeman*

Het beveiligen van netwerken wordt steeds actueler. Vroeger zaten alle werknemers met hun laptop of desktop-pc in een veilige kantooromgeving met een bekabelde verbinding. De moderne werkplek is dankzij wifi draadloos, niet langer locatiegebonden en kan ook andere vormen hebben zoals de smartphone of een tablet. Om dit in veilige banen te leiden, is er meer aandacht voor beveiliging nodig. Aan het woord is Dennis Dielemans, senior channel accountmanager van SonicWall, een Amerikaanse onderneming gespecialiseerd in netwerkbeveiliging. Dielemans: "SonicWall is channel only en onze meer dan 500 channelpartners in de Benelux beleveren de eindgebruiker. De hechte samenwerking met onze channelpartners zorgt ervoor dat alle kennis die nodig is om tot een succesvolle implementatie te komen, altijd beschikbaar is."


Dennis Dielemans

> **'Verhoogde beveiliging betekent vaak ook een extra barrière voor gebruiker'**

Het portfolio van SonicWall is breed en de kern draait om de firewall. Met hun Next Gen Firewall zorgt men voor de bescherming van netwerken, data, servers en werkplekken tegen cyberaanvallen. Maar omdat de firewall niet langer als afdoende wordt ervaren komt daar nu Cloud Edge-security bij. Met Cloud Edge-security wordt een Zero Trust-model geïntroduceerd.

Vertrouwen is goed, zekerheid is beter

"Bij Zero Trust kijken we naar meerdere parameters", legt Dielemans uit. "Gebruikersnaam/wachtwoord, tijdstip, geolocatie en werkdomein. Een medewerker die altijd vanaf kantoor werkt en zich ineens midden in de nacht met een Aziatisch IP-adres aanmeldt is per definitie verdacht. Een ingelogde gebruiker die informatie ophaalt uit een netwerk of dat segment waar hij niets mee van doen heeft is ook verdacht. Het zijn dit soort aspecten die bij Zero Trust getoetst worden. Een gebruikersnaam/wachtwoord combinatie resulteert in een identiteit, Zero Trust controleert of die identiteit aannemelijk is en het gedrag vertoont dat bij zijn rol hoort zoals tijdstip en geografische locatie.

Dielemans: "Verhoogde beveiliging betekent vaak ook een extra barrière voor gebruiker. Je moet bijvoorbeeld vaker inloggen met steeds complexere wachtwoorden. Dit verlaagt de productiviteit. Bij Zero Trust kunnen we die efficiency voor een stuk reduceren door hulpmiddelen in te zetten zoals sterke authenticatie en Single Sign On."

De oplossing van SonicWall is helemaal in de cloud gebouwd (cloud native) en wordt de klant als service aangeboden. Contracten lopen per gebruiker per jaar of maand en per afgenomen dienst. Door de cloudstrategie is de implementatie voor reseller eenvoudig uit te rollen. ■