

KPN biedt certificaatbeveiliging als beheerde dienst

KPN International heeft de certificaatbeveiliging van TrustAlert via Comsenso als een beheerde dienst toegevoegd aan zijn aanbod van internationale beveiligingsoplossingen. "Onze klanten willen een managed oplossing."

KPN International is een businessunit van KPN, die via zijn eigen, zeer uitgebreide netwerken klanten wereldwijd netwerk- en bandbreedteoplossingen biedt. KPN heeft een glasvezelnet in 22 Europese landen en werkt in ruim 180 landen samen met lokale aanbieders om een vergelijkbaar net te kunnen bieden.

TrustAlert ontwikkelde twee jaar geleden Resept, waarmee kortlopende PKI-certificaten kunnen worden uitgegeven als ASP-dienst. Daarmee kunnen elektronische transacties beveiligd worden. Met Resept loste TrustAlert een belangrijk probleem op van de klassieke PKI-certificaten: er zat te veel beheerwerk vast aan de langlopende certificaten, waardoor de kosten te hoog waren. Doordat alleen kortlopende certificaten worden uitgegeven die heel beperkt geldig zijn, voor één dagdeel bijvoorbeeld of voor één transactie of sessie, hoeft er geen complexe gebruikersdatabase te worden bijgehouden.

Rutger Gerritz, Vice President Product Management International Network Services van KPN International, bena-

drukt dat TrustAlert niet de enige oplossing is die hij voor deze dienst aan zijn klanten aanbiedt. "We bieden ook Verisign bijvoorbeeld. We willen de klant ook niet beperken. Klanten pikken het niet als je maar één leverancier biedt. Maar de TrustAlert-oplossing is een prettige aanvulling. Het is een niche, maar als je al je telecomzorgen wilt onderbrengen, is dit een prima oplossing."

KPN International biedt onder meer diensten als upgraden van het netwerk en convergentie van data en voice. Gerritz: "Wij hebben hier ongeveer tweehonderd medewerkers en hebben zeventienhonderd klanten. Wij zijn een bedrijf binnen dit bedrijf. Daarbij kiezen wij voor het segment net onder de zeer grote organisaties. Dat is een heel groot segment, waarin wij vorig jaar ruim vijftig nieuwe klanten vonden." Het bedrijf neemt in zijn portfolio diensten mee van partners en resellers. Gerritz: "Er is een behoefte aan dit soort oplossingen. Tien jaar geleden ontwikkelden we alles zelf. Nu werken we zoveel mogelijk samen. In veel

gevallen is dat sneller en minder riskant. Klanten verwachten de beste oplossing en één aanspreekpunt. De verantwoordelijkheid ligt bij ons. We streven naar een heel korte 'time to market'. Dat kan met deze werkwijze. In het verleden duurde dat te lang."

Gerritz: "Medewerkers reizen meer, ze internationaliseren. Er moet dus wereldwijd beveiligde toegang mogelijk zijn. En dat moet voor hen geregeld worden. Dat is een kwestie van organiseren en uitbesteden. Inbellen via een modem gebeurt vrijwel niet meer. De oplossing hiervoor is connectiviteit en beveiliging. Daar moeten beveiligde tunnels voor worden opgezet." Hij merkt dat zijn klanten zich steeds beter bewust zijn van het belang van beveiliging. De IT-manager moet echter een afweging maken tussen de beveiliging, het gebruiksgemak en de kosten. Het managen van beveiliging is arbeidsintensief en dus duur. Je moet ervoor zorgen dat certificaten worden uitgegeven. Er moeten tokens bij. Je moet ervoor zorgen dat oude werknemers uit het systeem worden verwijderd, dat nieuwe erin gaan. Wij gebruiken onze hotspots daarvoor en bieden dit daarbij extra als oplossing aan. In het verleden was connectiviteit het belangrijkste, maar dat wordt nu steeds meer beveiliging. Voor de eindgebruikers is dat toch uiteindelijk van groter belang."

Tanja de Vrede/t.vrede@sdu.nl

