DIGITALE TRANSFORMATIE

‘WIJ BIEDEN EEN IN DE HELE KETEN BEVEILIGDE OPLOSSING’

Jouk Lier,
directeur van BLU Networks

Gaandeweg nemen we afscheid van veel rotsen in de branding. Binnenkort wordt ISDN door KPN uitgefaseerd en zullen veel tevreden gebruikers om moeten kijken naar een goed, betrouwbaar en veilig, wellicht cloudgebaseerd, alternatief. “Wij bieden een goed beveiligde infrastructuur”, zegt Jouk Lier van BLU Networks.

door: Hans Steeman

Het Nederlandse bedrijf BLU Networks is een wholesale aanbieder van netwerkdiensten op de eigen infrastructuur en ISDN vormt een belangrijk deel van de bedrijfsactiviteiten. De uitfasering van ISDN is dan ook een onderwerp waarop actie moet worden ondernomen, is de mening van directeur Jouk Lier van BLU Networks uit Meppel. Hij heeft een helder verhaal voor klanten die in de toekomst te maken zullen krijgen met het einde van ISDN. “Kijk verder dan de goedkoopste aanbieder, denk goed na en maak een verantwoorde keuze.”

“De huidige digitale transitie is niet echt nieuw”, zegt Lier. “Al meer dan tien jaar is het mogelijk met een thin client en terminal sessies remote te werken. Indertijd draaiden de diensten in het eigen beschermde datacentrum en werd er met een simpele terminal remote op ingelogd. Met de digitale transitie van nu gaat het veel verder. Ineens gaat alles naar de cloud. Dat is nu het toverwoord. Maar de cloud is niet alleen een krachtig hulpmiddel, er zijn ook veel valkuilen in. Bedrijfsdata wordt bij een derde partij in beheer gegeven maar het is niet altijd duidelijk hoe het met de beveiliging is gesteld. Uiteraard zijn er partijen die veiligheid hoog in het vaandel hebben staan en concepten als ‘bring your own key’ ondersteunen, maar dan nog weten eindgebruikers niet waar hun data wordt opgeslagen en welke mensen er al dan niet bij kunnen. Amerikaanse bedrijven zullen de neiging hebben data binnen hun landsgrenzen op te slaan. Dan lopen bedrijven het risico dat de veiligheidsdiensten graag even meekijken. Uiteraard is er ook in Europa of Nederland lawfull interceptie, maar dat wordt gebruikt als de juiste gerechtelijke organen daar opdracht voor geven. Dat is toch net even anders.”


Jouk Lier

Gerenommeerde aanbieders

BLU Networks werkt volgens Lier met de netwerkinfrastructuur van grote gerenommeerde aanbieders waaronder Europese carriers zoals BT en Colt. “Ze werken binnen de Europese grenzen en hebben veiligheid en betrouwbaarheid hoog in het vaandel staan. Iemand die via ons op SIP-gebaseerde telefoondiensten afneemt, heeft de maken met een veilige en goed dichtgetimmerde infrastructuur.”

Kostenaspect

Te veel bedrijven kijken te vaak naar goedkoopste oplossing, vindt Lier. Een paar tientjes uitsparen en een standaard internetaanbieder gebruiken voor de VoIP-diensten lijkt aanlokkelijk maar is

‘Bedrijven nemen vaak uit kosten-overwegingen grote bedrijfsrisico’s’

“Onze focus richt zich helemaal op het leveren van telefonie en datadiensten. Al het verkeer dat we daarvoor gebruiken, is via Transport Layer Security (TLS) beveiligd en daarmee afgesloten voor pottenkijkers. Alle data in de cloud is volledig versleuteld. Niemand, ook de opsporingsdiensten niet, kan eraan komen. Apart genoeg lijken particulieren het soms beter te begrijpen. Als zij vertrouwelijkheid willen, kiezen ze diensten zoals Telegram en WhatsApp. Daar is een end-to-end versleuteling standaard in de clients en hebben de overheden geen greep op de informatie. Waarom gebruiken bedrijven dan nog onbeveiligde VoIP-diensten?”

volgens hem gevaarlijk. “Zonder encryptie is iedereen in staat om gesprekken te onderscheppen als die bijvoorbeeld via open hotspots worden gemaakt. Om het risico van fake hotspots met keyloggers nog maar even te benoemen. Als bedrijven zakelijke data via hotspots ontsluiten, en dat is zeker tijdens reizen en roamen financieel aanlokkelijk, is minimaal het gebruik van een VPN noodzakelijk. Wij faciliteren dat standaard, maar veel gebruikers benutten het niet. En dat terwijl de Europese roamingtarieven zijn

‘Ons verkeer is helemaal beveiligd tegen pottenkijkers’

verdwenen en kosten al lang niet meer het probleem hoeven te zijn. Een mobiele verbinding is het veiligst. Een internetverbinding met VPN is een goed alternatief. Maar zelfs als bedrijven dit alles goed regelen, blijven er risico’s. Bij een interconnect van een SIP-verbinding is alles goed te versleutelen. Zodra het verkeer echter naar een traditionele telecomprovider gaat, verdwijnt die weer en ligt alles weer open”, aldus Lier. “Het is soms beangstigend om te zien hoe bedrijven voor een dubbeltje op de eerste rang willen zitten en daarmee grote bedrijfsrisico’s nemen. Wij kunnen met OneSpace een heel veilige oplossing bieden die over de hele keten is beveiligd. Sterker nog, zelfs in China waar VPN’s steeds vaker niet kunnen worden gebruikt, blijft onze op WebRTC gebaseerde spraakdienst gewoon beveiligd werken dankzij de verpakking van de data in het HTTPS-protocol.”

Community

De diensten van BLU draaien op platformen die door programmeurs in de Oekraïne worden gebouwd. De ontwikkeling van het WebRTC platform vindt plaats in Odessa, legt Lier uit. “Odessa is een stad met 1,1 miljoen inwoners en maar liefst 18 universiteiten op development-niveau. Zij hebben jaarlijks meer dan 300.000 studenten. Getallen waar we in Nederland niet aankomen. Het is deze community die volledig gecommitteerd is aan een veilige oplossing. Geen kortetermijnactiviteiten, maar de drive om langdurig een betrouwbaar product te leveren. Wij zijn trots om zo’n solide basis te kunnen gebruiken bij het leveren van veilige diensten”, besluit Lier. «

www.blunetworks.nl info@blunetworks.nl 088 118 6444