'De maatschappij is gewend geraakt aan thuiswerken', aldus Bas de Stigter, technisch directeur bij Kop ICT.

KOP ICT TILT THUISWERKEN NAAR HET VEREISTE SECURITYNIVEAU

VEILIG DOOR DE TUNNEL

In de afgelopen jaren heeft het bedrijfsleven een forse slag gemaakt op het gebied van cybersecurity. Vervolgens greep corona om zich heen en werd thuiswerken de norm, met alle beveiligingsrisico's van dien. De hybride werkplek lijkt een blijvertje, maar met de juiste maatregelen hoeven organisaties zich geen zorgen te maken over hun dataverkeer. Kop ICT zet de oplossingen uiteen, tot op het hoogste securityniveau.

"Los van alle ellende heeft covid-19 ook positieve dingen voortgebracht," meent Bas de Stigter, technisch directeur bij Kop ICT. "De maatschappij is gewend geraakt aan thuiswerken, dat naar mijn idee niet zomaar zal verdwijnen, al draait het in veel gevallen waarschijnlijk uit op een combinatie met een paar dagen per week op kantoor, bij klanten of op een andere locatie zitten. De vermindering van de filedruk en de reistijd dragen bij aan een enorme efficiëntieslag en dan praat ik nog niet eens over internationaal communiceren met klanten of collega's in het buitenland via videobellen, in plaats van dat je 'even' op het vliegtuig stapt. Ik ken zelfs een ondernemer die in de coronatijd besloot om de huur van zijn pand op te zeggen en zijn mensen thuis laat werken. Indien nodig reserveert hij tijdelijk een vergaderruimte. Deze transformatie stelt natuurlijk wel eisen aan de kwaliteit van de internetverbindingen bij particulieren thuis. In sommige gevallen viel daar een behoorlijke stap te maken in snelheid, stabiliteit en veiligheid."
De eerste twee factoren blijken niet in alle situaties even vanzelfsprekend. "Vooral in het buitengebied liggen nog uitdagingen. Glasvezel maakt er weliswaar een opmars, maar het gaat langzaam. De internetverbindingen schieten er vaak nog tekort."

Tekst: Aart van der Haagen Fotografie: Raphaël Drent

VERSLEUTELD EN ONTSLEUTELD

Kop ICT, onderdeel van de gerenommeerde multi-dienstverlener Kop Groep (inclusief Kop Beveiliging, Kop Telecom en Kop Digitaal), maakt een onderscheid in drie 'smaken' als het aankomt op snel, stabiel en veilig internet thuis voor zakelijke toepassingen. "In sommige gevallen leggen we een complete verbinding aan. Meestal echter gebruiken we de bestaande en zetten we daar een VPN-box bovenop, dat een hoofdrol speelt in de beveiliging. Het legt een link met een datacentrum, waar een zware centrale firewall alle in- en uitgaande bitjes checkt die over de lijn vliegen. 'Door de tunnel,' zeggen wij ook wel. Elk afzonderlijk bitje wordt bij de verzending versleuteld en bij aankomst op de bestemming ontsleuteld, waardoor een hacker die de informatie zou onderscheppen er in principe niets mee kan. KPN noemt dit EVI: extra veilig internet. Het opereert dus los van de privéverbinding bij de klant thuis, wat voor de werkgever een geruststellende gedachte vormt, die immers niet wil dat data binnenshuis verspreid worden. Daarnaast is er de zekerheid dat de snelheid en stabiliteit geen hinder ondervinden van internetgebruik door andere gezinsleden, zoals kinderen die gamen of online-lessen volgen."

PLUG AND PLAY

De versleutelde verbinding met het datacentrum maakt volgens de Stigter ook deel uit van de derde optie die Kop ICT aanbiedt: een extra verbinding via een 4G- of 5G-oplossing. "Dat is niets meer of minder dan een antenne bij de gebruiker op locatie, die de data geheel beveiligd door de lucht stuurt," legt De Stigter uit. "Ideaal voor mensen die in het buitengebied wonen of die zich tijdens quarantaine terugtrekken in een vakantiehuisje. We sturen heel eenvoudig per post een kastje op dat direct begint te werken zodra je het in het stopcontact steekt. Plug and play. Desgewenst verhuren we het zelfs vanaf 59 euro per maand. Dezelfde techniek passen we toe wanneer we in opdracht van de klant een back-upverbinding bij de gebruiker thuis aanleggen. Die staat standaard aan en treedt automatisch in werking op het moment dat het internet er onverhoopt uit ligt. Ook vangt hij pieken in de belasting op, bijvoorbeeld wanneer meerdere gezinsleden tegelijk veel data verbruiken. Daarmee is de stabiliteit gegarandeerd. Overigens onderscheiden wij ons in de markt met een 24/7 bereikbare helpdesk, waarbij de gebruiker - dus ook thuis - altijd een fysieke medewerker aan de lijn krijgt die actie onderneemt om een probleem zo snel mogelijk te verhelpen."

'VERTROUWEN IS GOED, CONTROLE IS BETER'

TOEVERTROUWEN

Externe data-opslag en samenwerken in de vorm van cloudoplossingen nemen steeds meer een vlucht, maar aan wat voor partij vertrouw je al die gegevens toe? "Het laatste dat je wilt is dat de partij die het beheert de beveiliging tegen hackers niet goed op orde heeft," zegt De Stigter. "Wij werken samen met één vaste partner op dit gebied. Het betreft een Nederlands datacentrum met de hoogste graad in ISO- en NEN-certificering, zorgvuldig door ons uitgekozen na een intensief selectieproces. We zijn zelfs ter plaatse gaan kijken. Eigenlijk zoals je dat vroeger ook deed wanneer je een grote hoeveelheid papiergeld ergens in een kluis wilde laten bewaren. Met volledig getoetste verbindingen en cloudoplossingen kunnen en mogen we deze services aanbieden in sectoren die op grote schaal met privacy- en andere gevoelige data werken, zoals zorg, onderwijs, financiële dienstverlening en overheden. Indien gewenst of op grond van ISO-normering vereist laten we audits uitvoeren door ethisch hackers. Overigens kunnen we bij medewerkers thuis ook een quickscan doen op het gebied van security."

CYBER ALARM MONITOR

Voor opdrachtgevers die het hoogste niveau van beveiliging verlangen - level 5 - heeft Kop ICT de scanning alarm monitor (SAM) paraat. "Vergelijk het met een woonhuis dat op alle fronten afgeschermd is tegen inbrekers, met hoogwaardige sloten en dergelijke. Toch weet er iemand binnen te dringen die met je kostbare spullen aan de haal gaat. Dat gebeurt dan nog onder tijdsdruk, waar een hacker juist geduldig zijn kans afwacht en 'in de kelder kruipt.' Die heeft maar één doel: informatie naar buiten krijgen. De SAM checkt het uitgaande dataverkeer extra en slaat alarm wanneer deze buiten de normale gebruikers om verstuurd worden. Op dat moment ontvangen zowel de klant als wij een melding. In geval van hoge prioriteit nemen we contact op en treffen we een noodprocedure; in het uiterste geval het onderbreken van de internetverbinding om het weglekken van waardevolle en/of gevoelige data te voorkomen of in ieder geval te beperken. Vertrouwen is goed, controle is beter." Eigenlijk geldt dat credo voor de gehele internetverbinding in relatie tot thuiswerken. Kop ICT weet inmiddels als geen ander hoe je data veilig door een tunnel laat gaan.

www.kopict.nl