

Claassen: "Wat kunnen we nog zonder ICT? De continuïteit van activiteiten bleek afhankelijk van connectiviteit. We hebben de leden dan ook razendsnel van de informatie voorzien die nodig was om het hybride werken te kunnen opzetten." Dit was nu bij uitstek een taak voor de Branchevereniging voor IT en Communicatietechnologie BTG. De eerste brug is die tussen gebruikers en aanbieders van

kennisinstellingen, netwerkoperators en netwerkproducenten en -bouwers bij elkaar rond 'strategische tafels'. De partijen die er belang bij hebben en de partijen met expertise, vraag en aanbod, komen samen. Zo'n expertgroep deelt inzichten en stelt zo vast waar de gaten in kennis en praktische barrières zitten." Het kan ook gaan om young professionals en executives, 'green meets grey' die samen oplossingen formuleren. "Deze

BTG en MKB

Ruim tweehonderd grote bedrijven - van ASML tot Jumbo - en (semi) overheidsorganisaties van ministeries en academische ziekenhuizen tot de Belastingdienst, Rijkswaterstaat Schiphol en de havens van Rotterdam en Amsterdam vormen de achterban van BTG. Dat zijn allemaal grote organisaties. Een nieuw BTG-initiatief wil de best practices van deze grote organisatie op het gebied van duurzame ICT ook aan het MKB beschikbaar stellen via masterclasses.



...sing?
A "We hebben op dit moment een testbed gebouwd dat het principe van 100 procent veilige datatransmissie bewijst. De stap hierna is een opstelling bij één van onze klanten. Vervolgens maken we er een product van. Eén van de zaken waar we aan werken, is het vergroten van de maximale transmissieafstand. Behalve aan het netwerk werken we ook aan nieuwe 'quantumbestendige' versleutelingsmethoden, want die zijn zeker mogelijk. Die combinatie van quantum veilige hardware en software komt in het testbed terug. We werken daarbij samen met Q*bird en Juniper Networks. Het testbed staat open voor klanten uit bijvoorbeeld overheden, bedrijfsleven, vitale infrastructuur en de energiesector. Organisaties die kennis en ervaring met deze quantum veilige datatransmissie willen opdoen, kunnen zich melden."

ADVERTENTIE

De meeste cyberaanvallen hadden voorkomen kunnen worden

Ondanks dat 2023 nog niet eens halverwege is, hebben we al veel impactvolle cyberaanvallen gezien op Nederlandse organisaties. Een kwalijke zaak, zeker wanneer later blijkt dat het nagenoeg altijd voorkomen had kunnen worden. Toch merken wij dat nog (te)veel organisaties het belang van een adequaat en doordacht IT-securitybeleid nog niet inzien. Of wellicht niet willen inzien.

De redenen hiervoor zijn uiteenlopend, maar hebben vaak te maken met een gebrek aan kennis, budget of het idee dat er "toch niets aan te doen is" of "wij zijn echt geen doelwit hoor". Zeker die laatste twee doen ons pijn. Daarom herinneren wij klanten er altijd aan dat hackers geen motief nodig hebben voor hun acties. En ja, ook daar is zeker tegen te verdedigen. Desondanks is het wel belangrijk om te benadrukken dat cyberveiligheid een constant proces is, geen project. En wat hier perfect op aansluit, is onze Endpoint Protection oplossing.

Endpoint protection is gericht op het beschermen van apparaten die toegang hebben tot netwerken en gegevens, zoals laptops, desktops, smartphones en tablets. Deze beveiligingsmethode maakt gebruik van verschillende technologieën, waaronder antivirussoftware, firewalls en intrusion detection- en preventiesystemen, om bedreigingen te detecteren en te blokkeren voordat deze schade kunnen veroorzaken.

In tegenstelling tot een standaard firewall of antivirus is onze oplossing veel meer gericht op gedrag. Het voordeel hiervan is dat het actief acteert op dreiging van binnen- en buitenaf. Ter illustratie, probeert een legitieme gebruiker in te loggen op een omgeving waar hij of zij nog nooit eerder heeft ingelogd? Dan wordt dit gezien als verdacht gedrag. Omdat wij geloven dat technologie alleen niet voldoende is, combineren wij onze Endpoint Protection oplossing met 24/7 monitoring door onze eigen, gespecialiseerde medewerkers. Dit is zeer waardevol. Je haalt op deze manier niet enkel de software in huis, maar ook kennis en ervaring.

Wij zien dat steeds meer organisaties zoeken naar een dynamische en doorlopende oplossing tegen de ongekende hoeveelheid aan cyberdreigingen. Herkent u zich hierin en wil u 's avonds ook beter slapen? Neem dan contact op met de Cyber Security experts van Rootsec.



ROOTSEC