

Whitepaper

De papieren illusie van cyberveiligheid

Waarom 100% veiligheid niet bestaat en wat je wel kunt doen

In een tijd waarin we voor vrijwel alles afhankelijk zijn van digitale systemen, lijkt het behalen van een ISO-certificering of het afvinken van compliance-eisen voor velen de ultieme geruststelling. Het biedt een tastbaar bewijs dat de informatiebeveiliging op orde is. Toch schuilt hierin een gevaarlijke misvatting. Een certificaat toont aan dat processen op papier bestaan, maar het garandeert niet dat een organisatie daadwerkelijk weerbaar is wanneer een crisis uitbreekt. Dit fenomeen noemen we de 'papieren illusie'.

Tegelijkertijd zien we dat het dreigingslandschap in Nederland steeds complexer wordt. Het Cybersecuritybeeld Nederland 2025 waarschuwt voor de grote verscheidenheid aan aanvallen door statelijke actoren en cybercriminelen, waarbij de grens tussen beide steeds vaker vervaagt. In deze whitepaper ontleden we de mythe van 100% veiligheid, onderzoeken we waarom het testen van de werking van beveiligingsmaatregelen cruciaal is, en bieden we een concreet actieplan om van schijnveiligheid naar echte digitale weerbaarheid te bewegen.

In dit whitepaper lees je meer over de volgende onderwerpen

- Waarom een ISO-certificaat of vinkje een organisatie niet gelijk veilig maakt
- Hoe je ontdekt of de beveiliging binnen je organisatie echt werkt
- Waarom testen met ketenpartners net zo belangrijk is als binnen de organisatie
- Hoe een sterke infrastructuur een crisisteam de ruimte geeft om te handelen
- Wat je morgen kunt doen om als organisatie digitaal weerbaarder te worden

De illusie van 100% veiligheid

Het is een comfortabele gedachte: de IT-infrastructuur is dichtgetimmerd, de Service Level Agreements (SLA's) met leveranciers zijn getekend en de auditor heeft het ISO 27001-certificaat afgegeven. Het management haalt opgelucht adem, in de veronderstelling dat het digitale fort onneembaar is. De realiteit is echter weerbarstiger.

Cybercriminelen opereren in een wereld zonder bureaucratie. Waar organisaties gebonden zijn aan strenge privacywetgeving en complexe aanbestedingsprocedures, delen aanvallers moeiteloos informatie en tools op het dark web. Zoals cybersecurity-expert Kelvin Rorive stelt in de TReNT-podcast *Oefenen met je ketenpartners*: "Criminelen zijn beter georganiseerd dan de organisaties die ze aanvallen. Ze hebben geen last van wetten, regels of aanbestedingen".

Deze asymmetrie in de digitale wapenwedloop betekent dat 100% veiligheid simpelweg niet bestaat. Een certificaat is een momentopname en toont slechts aan dat je als organisatie hebt nagedacht over risico's en procedures. Het is echter geen schild dat een aanval afweert. Wanneer we de nadruk te veel leggen op compliance in plaats van op daadwerkelijke weerbaarheid, ontstaat er schijnveiligheid. Organisaties wanen zich veilig, terwijl de voordeur in de praktijk nog op een kier staat.

Onderaan dit whitepaper vind je een link naar de podcast *Oefenen met je ketenpartners*.

Opzet, bestaan én werking

Om de kloof tussen theorie en praktijk te overbruggen, is het essentieel om onderscheid te maken tussen de opzet, het bestaan en de werking van beveiligingsmaatregelen.

- **Opzet:** het ontwerp van de maatregel (bijvoorbeeld een beleid voor back-ups).
- **Bestaan:** de implementatie van de maatregel (de back-upsoftware is geïnstalleerd).
- **Werking:** de effectiviteit van de maatregel in de praktijk (kunnen we de back-up daadwerkelijk en tijdig herstellen tijdens een ransomware-aanval?).

Veel audits en certificeringen focussen zich primair op opzet en bestaan. Maar zoals Rorieve benadrukt: ethical hackers slagen er regelmatig in om binnen een week binnen te dringen bij organisaties die op papier alle vinkjes op orde hebben. De echte test van digitale weerbaarheid ligt in de werking.

Dit geldt des te meer in het licht van supply chain-risico's. De afhankelijkheid van toeleveranciers is een van de grootste kwetsbaarheden voor Nederlandse organisaties. Uit recent onderzoek blijkt dat hoewel bijna alle Nederlandse bedrijven vertrouwen op de cybersecuritymaatregelen van hun leveranciers, bijna de helft deze leveranciers nooit regelmatig controleert. Je kunt als organisatie je eigen zaken perfect op orde hebben, maar als een kritieke partner in de keten omvalt, stagneert ook jouw bedrijfsvoering. De Cyberbeveiligingswet (de Nederlandse implementatie van de Europese NIS2-richtlijn), die momenteel al actief is, legt dan ook sterk de nadruk op deze ketenverantwoordelijkheid.

Oefenen is de sleutel

Als 100% veiligheid een illusie is en certificaten onvoldoende garantie bieden, wat is dan het antwoord? Het antwoord ligt in het continu testen en oefenen van crisisscenario's.

Een crisisplan in een bureaula is waardeloos als het team niet weet hoe het in de praktijk moet samenwerken. Tijdens een cybercrisis staat de organisatie onder extreme druk. Beslissingen moeten snel en op basis van onvolledige informatie worden genomen. In zo'n situatie moet een crisisteam functioneren als een goed geoliede machine.

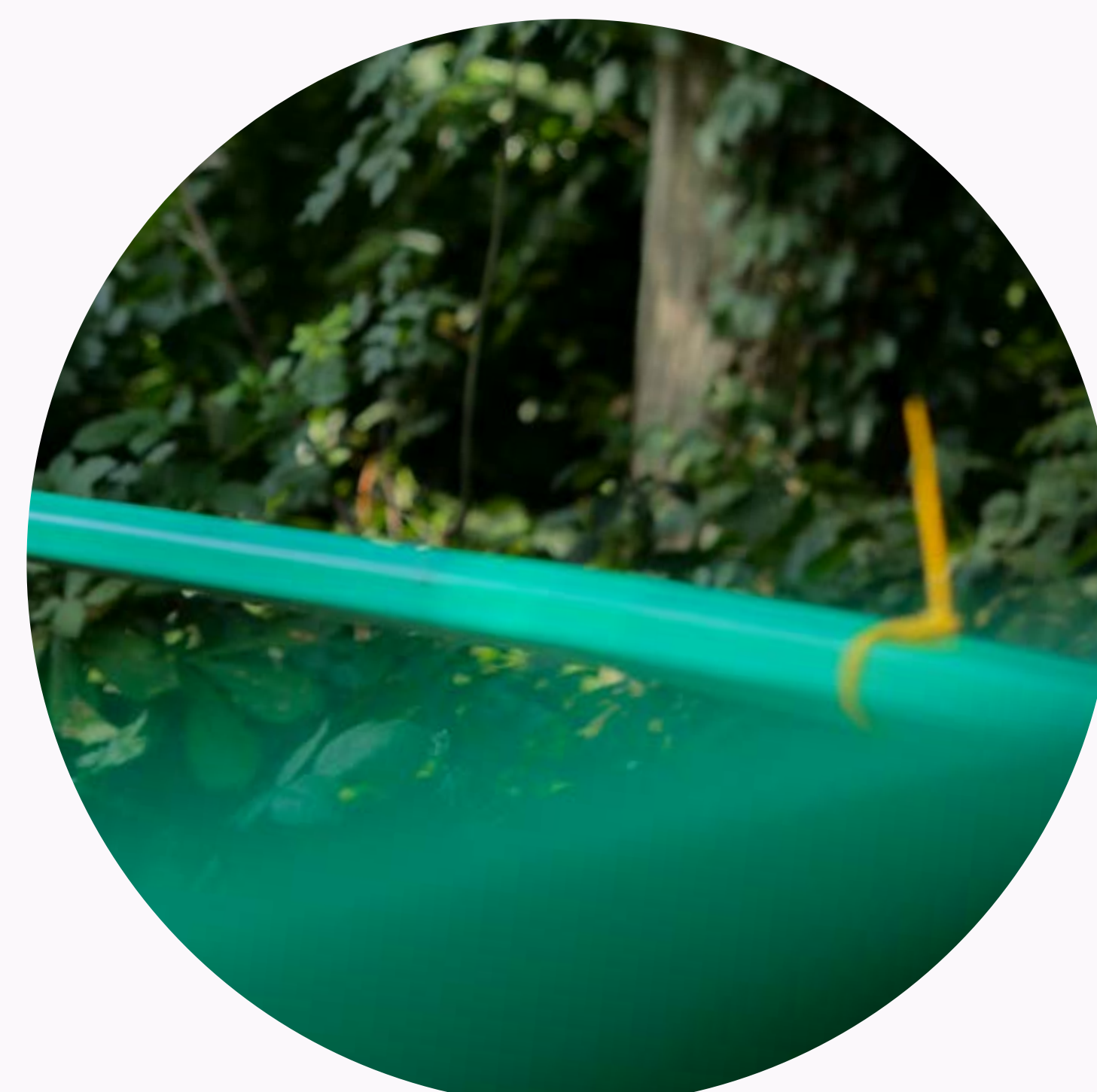
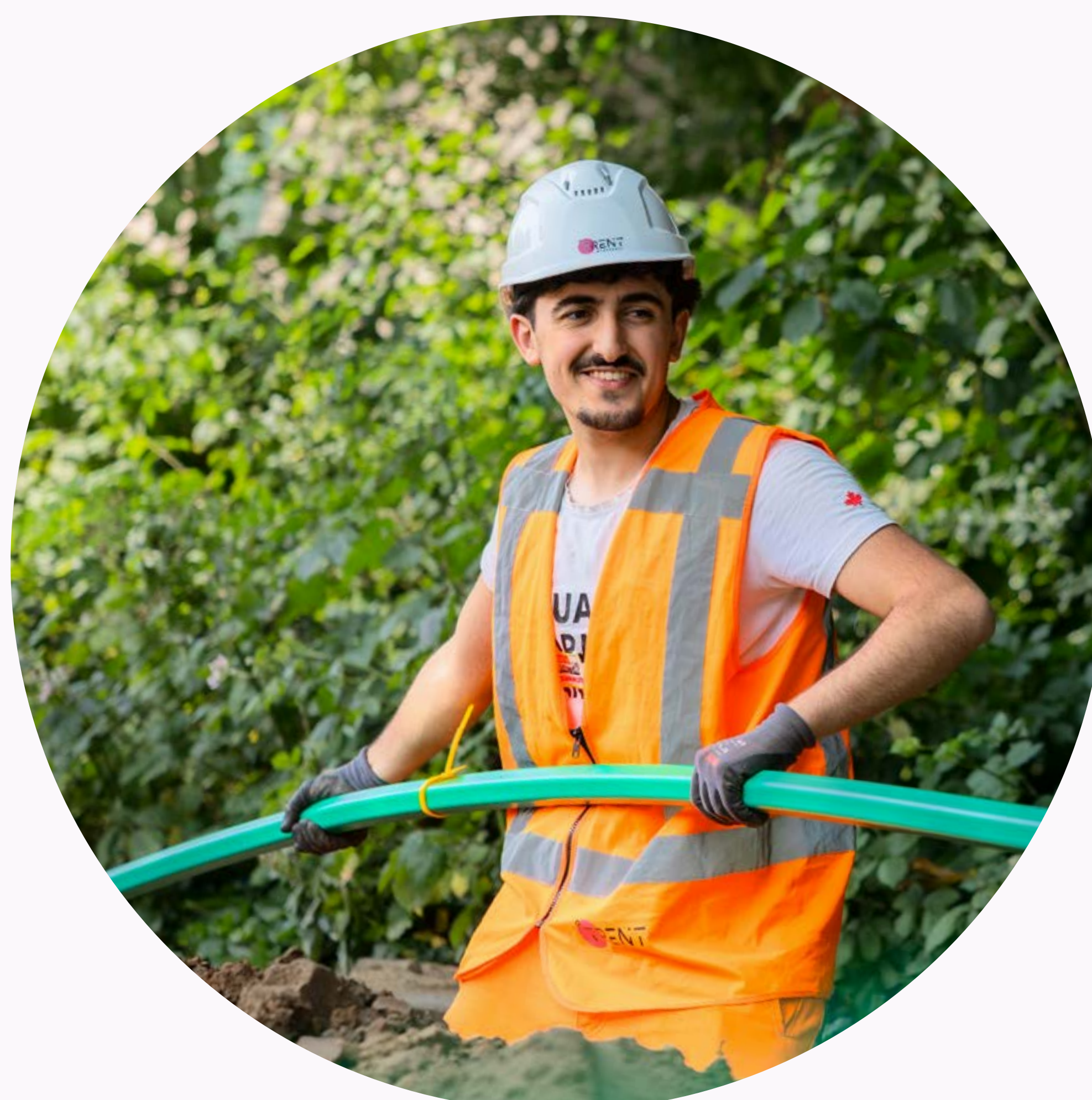
Dit vereist niet alleen dat de rollen duidelijk zijn belegd – zoals de voorzitter die het overzicht bewaart, de communicatie-expert die de reputatieschade beperkt, en de 'logger' die als motor van het team alle besluiten vastlegt – maar ook dat de teamleden elkaar door en door kennen. Bovendien mag het oefenen niet stoppen bij je eigen voorkeur. Het simuleren van een crisis samen met kritieke IT-leveranciers en ketenpartners legt vaak pijnlijke blinde vlekken bloot. Zo kan tijdens een simulatie blijken dat de veronderstelde back-upvoorziening bij de leverancier helemaal niet in het contract was opgenomen. Door dit in vreedstijd te ontdekken, voorkom je catastrofale gevolgen tijdens een daadwerkelijke aanval.

De basis voor weerbaarheid

Hoewel de menselijke factor en het oefenen van processen cruciaal zijn voor de werking van digitale weerbaarheid, kan een organisatie pas effectief reageren als de fysieke basis – de opzet en het bestaan – robuust en betrouwbaar is.

Hier speelt de keuze van de digitale infrastructuur een doorslaggevende rol. Een eigen glasvezelnetwerk, zoals dark fiber, biedt een fundamenteel veiliger uitgangspunt dan gedeelde verbindingen. Omdat een dark fiber-verbinding fysiek gescheiden is en niet wordt gedeeld met andere partijen, elimineert het de risico's die inherent zijn aan publieke netwerken.

Met een eigen dark fiber-verbinding behoud je als organisatie de volledige regie over je eigen datastromen en capaciteit. Dit sluit naadloos aan bij de behoefte aan datasoevereiniteit en controle, thema's die door geopolitieke spanningen en wetgeving zoals NIS2 steeds urgenter worden. Wanneer de basisinfrastructuur stabiel, schaalbaar en maximaal beveiligd is, creëert dit de noodzakelijke rust en ruimte voor het bestuur en het crisisteam om zich te focussen op het oefenen van processen en het optimaliseren van de samenwerking in de keten.



Actieplan

De verschuiving van schijnveiligheid naar echte digitale weerbaarheid is geen eenmalig project, maar een continu proces. Om deze transitie in gang te zetten, kun je vandaag nog starten met de volgende drie stappen:

- 1. Ken je ecosysteem en ketenrisico's:** Breng in kaart wie je meest kritische ketenpartners en toeleveranciers zijn. Vertrouw niet blindelings op hun certificaten, maar ga het gesprek aan over hun daadwerkelijke weerbaarheid en hoe zij omgaan met incidenten.
- 2. Organiseer een eerste (keten)simulatie:** Begin klein, maar begin. Simuleer een realistisch scenario, zoals een ransomware-aanval waarbij een belangrijk systeem uitvalt. Evalueer achteraf niet alleen de technische respons, maar vooral de communicatie en besluitvorming binnen het crisisteam en met externe partners.
- 3. Beoordeel je digitale fundament:** Onderzoek in hoeverre je huidige connectiviteit en infrastructuur de controle en veiligheid bieden die nodig is in het huidige dreigingslandschap. Overweeg of een eigen dark fiber-oplossing de noodzakelijke robuuste basis kan vormen voor je langetermijnstrategie.

Digitale weerbaarheid vereist de moed om voorbij de papieren werkelijkheid te kijken. Door te investeren in een sterk fysiek fundament en tegelijkertijd onophoudelijk te oefenen met de menselijke en organisatorische aspecten van een crisis, bouw je aan een organisatie die niet alleen op papier veilig is, maar in de praktijk werkelijk veerkrachtig blijkt.



Beluister de podcast met Kelvin Rorive

