Van binnenuit beveiligen: hoe organisaties hun netwerk toekomstbestendig maken

Door Peter Brandenburg, GTM Networking Lead NTT DATA Nederland

De afgelopen jaren heb ik bij veel organisaties van dichtbij gezien, hoe snel hun digitale omgeving aan het veranderen is. Nieuwe technologieën zoals AI, cloud en data-intensieve toepassingen worden in razend tempo omarmd. Dat brengt prachtige kansen, maar ik merk in gesprekken ook steeds dezelfde onzekerheid: *hoe houden we het veilig?*

Wat me vooral opvalt, is dat bijna iedereen meer investeert in security dan ooit en toch groeit de dreiging. De cijfers liegen er niet om: volgens het World Economic Forum ziet ruim 70% van de bedrijven het aantal cyberaanvallen toenemen, ondanks stijgende securitybudgetten. Dat contrast zet mij, en veel van onze klanten, aan het denken. Want als méér tools niet automatisch leiden tot minder risico's, wat dan wel?

Voor mij is de conclusie helder: veiligheid draait niet langer om nóg meer technologie, maar om een slimmer fundament. Niet de tools, maar het netwerk zelf moet de eerste verdedigingslinie worden.

Beveiliging van binnenuit: een nieuw fundament

Ook in Nederland zien we dezelfde trend. Organisaties versnellen hun digitale transformatie, maar veel netwerken zijn nog opgebouwd rond oude perimeter-architecturen: een harde buitenkant, een zachte kern. Dat model werkt niet meer in een wereld waarin medewerkers, data en applicaties verspreid zijn over cloud, thuisnetwerken en mobiele devices. Een moderne organisatie heeft een netwerk nodig dat zichzelf begrijpt, ziet wat er gebeurt, patronen herkent en zichzelf verdedigt.

Bij NTT DATA Nederland noemen we dat Secure Networking: een geïntegreerde aanpak waarin connectiviteit, security en automatisering samenkomen in één intelligent systeem. Maar hoe komen organisaties daar? Hoe transformeer je een traditioneel, vaak complex netwerk naar een toekomstbestendige, zelfverdedigende infrastructuur?

Die transitie begint met **vijf strategische stappen die iedere organisatie**, ongeacht omvang of sector, kan zetten om het netwerk van binnenuit te versterken.

Vijf strategische stappen naar een veilig netwerk

1. **Gebruik wat u al heeft, slim en bewust**

Veel organisaties benutten slechts een fractie van de beveiligingsmogelijkheden die al in hun infrastructuur aanwezig zijn, zoals netwerksegmentatie, encryptie en toegangscontrole. Door deze basis te optimaliseren ontstaat direct winst in beveiliging, zonder grote investeringen.

2. **Omarm Zero Trust als bedrijfsstrategie**

Zero Trust is geen technologie, maar een manier van denken: *Never trust, Always verify, Assume breach*. Iedere gebruiker, applicatie en verbinding wordt continu gevalideerd, essentieel in hybride werkomgevingen.

3. **Verleg beveiliging naar de cloud**

Data en medewerkers zijn overal. Cloud-native modellen zoals Secure Service Edge (SSE) en software-defined networking maken het mogelijk om beleid, identiteit en bescherming uniform te beheren van datacenter tot edge.

4. **Maak uw netwerk inzichtelijk**

Zonder inzicht is er geen controle. Observability vertaalt netwerkdata naar bruikbare inzichten: van prestaties tot afwijkingen en dreigingen.
Met analytics en AI ontstaan dashboards die niet alleen tonen *wat er gebeurt*, maar ook *wat er gaat gebeuren*.

5. **Automatiseer met AI Ops**

AI Ops gebruikt machine learning om onregelmatigheden te detecteren, incidenten te voorspellen en automatisch te herstellen. Het resultaat: minder incidenten, snellere oplossingen en meer ruimte voor innovatie.

Waarom dit relevant is voor Nederlandse organisaties

Nederland is digitaal vooruitstrevend, maar onze infrastructuren zijn vaak complex, gefragmenteerd en verouderd. De combinatie van hybride werken, toenemende compliance-eisen en groeiende dreigingen laat zien: security moet geïntegreerd zijn in de kern van het netwerk. Voor sectoren als industrie, financiële dienstverlening en zorg gaat het om meer dan bescherming. Het gaat om vertrouwen, continuïteit en reputatie.

De kracht van NTT DATA Nederland

Bij NTT DATA Nederland helpen we organisaties om hun netwerk van binnenuit te transformeren. Met Secure Networking en Software-Defined Infrastructure Services (SDIS) combineren we technische diepgang met een businessgerichte aanpak. Wij bieden onder meer:

- **End-to-end zichtbaarheid en voorspellend risicobeheer**
  Niet alleen realtime, maar ook predictive analytics.
- **Zero Trust en identity-based security in alle lagen**
  Inclusief microsegmentatie en policy enforcement.

- **AI-gedreven automatisering en proactieve threat detection**
  Van monitoring naar actie.
- **Flexibele, schaalbare infrastructuur via SDIS**
  Direct meebewegend met businessbehoeften.
- **Lifecycle management gericht op kostenoptimalisatie en compliance**
  Continu verbeteren én aantoonbaar voldoen aan regelgeving.

Onze aanpak is pragmatisch, meetbaar en gericht op waard creatie: minder risico, lagere kosten en hogere wendbaarheid.

De toekomst vraagt niet om méér beveiligingstools, maar om een slimmer netwerk. Een netwerk dat zichzelf beschermt, leert en meegroeit met de organisatie.
De transitie naar Secure Networking begint vandaag.

Jouw netwerk. Jouw regie.