proximus NXT
Nederland

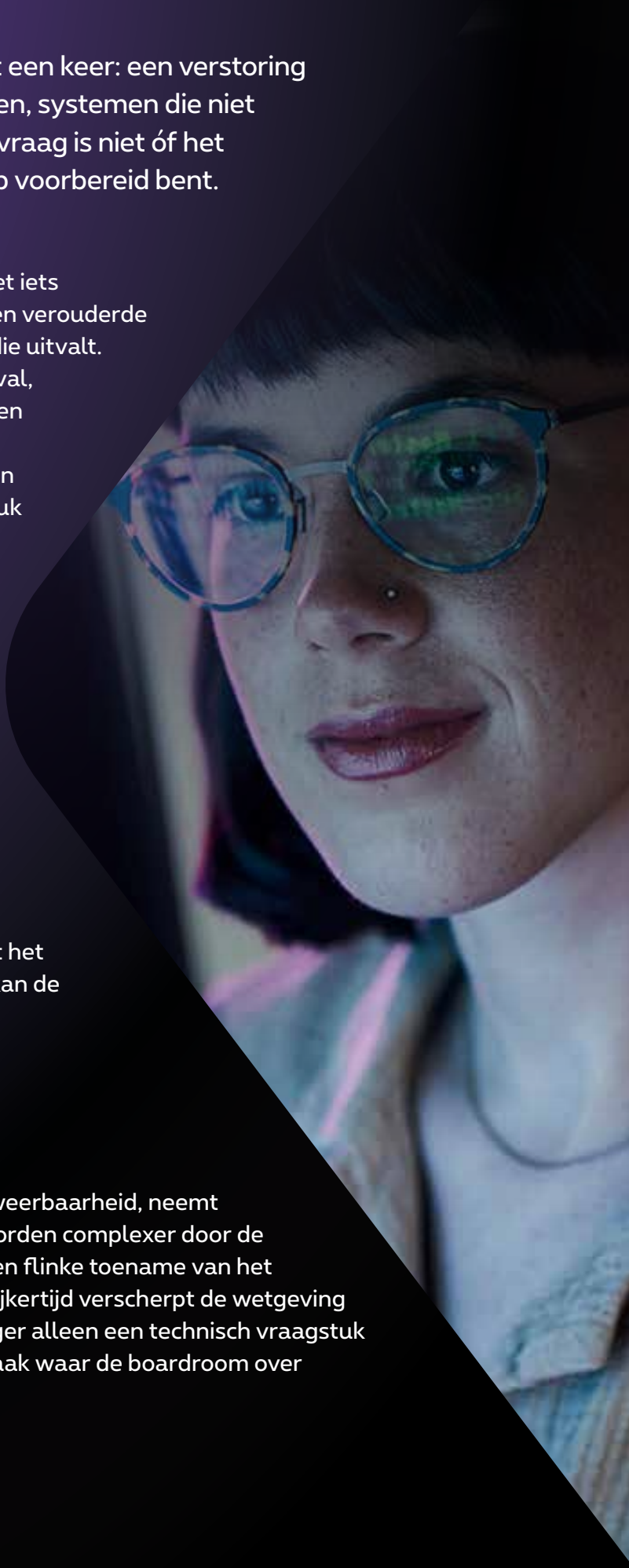
Hoe voorkom je IT-verstoringen?

Een praktische gids voor digitale weerbaarheid in een complexe wereld

De risico's van IT-uitval

Het overkomt elke organisatie vroeg of laat een keer: een verstoring van de IT-infrastructuur. Servers die uitvallen, systemen die niet bereikbaar zijn, processen die stilliggen: de vraag is niet óf het gebeurt, maar wanneer en hoe goed je erop voorbereid bent.

IT-uitval kent vele oorzaken. Het kan beginnen met iets ogenschijnlijks onschuldigs: een stroomstoring, een verouderde switch die het begeeft of een internetverbinding die uitvalt. Maar het kan ook gaan om een gerichte cyberaanval, ransomware die je systemen gegijzeld houdt, of een technische storing bij een leverancier waarvan je afhankelijk bent. Zelfs menselijke fouten, zoals een verkeerd ingestelde configuratie of een per ongeluk verwijderd bestand, kunnen je organisatie tot stilstand brengen.



Grote impact...

De impact kan groot zijn. Operationele processen vallen stil, de omzet loopt terug, klanten verliezen vertrouwen en je reputatie staat op het spel. Voor organisaties die kritieke infrastructuur beheren, zoals ziekenhuizen, energieleveranciers, waterbedrijven, financiële instellingen en centrale en lokale overheden, gaat het om meer dan bedrijfscontinuïteit: een verstoring kan de maatschappij vergaand ontwrichten.

...en groeiende urgentie

De urgentie om aan de slag te gaan met digitale weerbaarheid, neemt ondertussen alleen maar toe. IT-landschappen worden complexer door de integratie van cloud, hybride infrastructuren en een flinke toename van het aantal met het internet verbonden devices. Tegelijkertijd verscherpt de wetgeving (zie kader). Digitale veiligheid is daarmee niet langer alleen een technisch vraagstuk voor de IT-afdeling, maar een strategische noodzaak waar de boardroom over meebeslist.

Nieuwe wetgeving verhoogt de druk

Recente en aankomende wet- en regelgeving stelt concrete eisen aan digitale weerbaarheid en maakt bestuurders persoonlijk aansprakelijk.

NIS2: deze Europese richtlijn verplicht organisaties in kritieke sectoren om cybersecurity-maatregelen te nemen en incidenten te rapporteren.

DORA (Digital Operational Resilience Act): gericht op financiële instellingen. DORA stelt eisen aan hoe je IT-risico's beheerst, incidenten rapporteert en leveranciers managet.

BIO2 (Baseline Informatiebeveiliging Overheid): de Nederlandse norm voor overheidsorganisaties, met strenge eisen aan onder meer encryptie en wie toegang heeft tot welke systemen.

Wet weerbaarheid kritieke entiteiten (Wwke): verplicht kritieke organisaties om weerbaarheidsmaat-regelen te treffen tegen fysieke en digitale dreigingen.

ABRO (Algemene Beveiligingseisen voor Rijksoverheid Opdrachten): beveiligingseisen specifiek voor leveranciers die werken voor de Rijksoverheid.

ABDO (Algemene Beveiligingseisen voor Defensieopdrachten): vergelijkbaar met ABRO, maar gericht op defensie-gerelateerde opdrachten.

Voor bestuurders betekent dit dat zij aantoonbaar moeten kunnen maken dat hun organisatie passende maatregelen heeft getroffen, anders kunnen ze bij een ernstig incident persoonlijk aansprakelijk worden gesteld voor nalatigheid. Concrete vragen die bestuurders aan IT zouden moeten stellen: hebben we onze kritieke systemen in kaart? Is ons incident response-plan recent getest? Kunnen we binnen 24 uur een cyberincident rapporteren? Zijn onze belangrijkste leveranciers doorgelicht op security? En: hebben we een actueel disaster recovery-plan dat daadwerkelijk werkt?

Oorzaken van IT-uitval

Om digitale uitval te voorkomen, moet je eerst begrijpen waar de zwakke plekken zitten. De oorzaken zijn divers en vaak met elkaar verweven.

Infrastructurele kwetsbaarheden

De basis van elke IT-omgeving (servers, netwerkapparatuur, stroomvoorziening en internetverbindingen) lijkt bij veel organisaties goed geregeld, maar verbergt bij nadere beschouwing vaak onverwachte kwetsbaarheden. Met name zogenoemde **single points of failure** (kwetsbare schakels waarvan alles afhankelijk is) zijn verraderlijk: als één cruciale component uitvalt, staat alles stil. Voorbeelden uit de praktijk: een back-upsysteem dat ongemerkt al jaren niet meer functioneert, een enkele internetverbinding waarop alle bedrijfsprocessen draaien, of een stroomvoorziening zonder noodstroom. Vaak blijft dit soort kwetsbaarheden onzichtbaar, tótdat er een storing is.

In de praktijk zien we dit regelmatig bij assessments: organisaties denken dat hun infrastructuur robuust is, maar bij nader onderzoek blijkt bijvoorbeeld dat redundante verbindingen door hetzelfde tracé lopen, of dat back-upsystemen niet getest zijn. Door vanuit een frisse blik naar je volledige infrastructuur te kijken (van de fysieke laag tot applicaties) komen dit soort risico's aan het licht vóórdat ze tot uitval leiden.

Toenemende cyberrisico's

De aard van cyberaanvallen is fundamenteel veranderd. Waar veel organisaties lange tijd simpelweg een firewall op de grens van hun netwerk zetten en zich veilig waanden, zien we nu steeds vaker ketenaanvallen waarbij hackers via meerdere, ogenschijnlijk onschuldige stappen binnendringen. Eenmaal in het netwerk kunnen aanvallers zich verspreiden van systeem naar systeem, tot ze toegang hebben tot je meest waardevolle assets; zoals klantdata, financiële informatie of intellectueel eigendom.

Ransomware, waarbij cybercriminelen je data versleutelen en vervolgens losgeld eisen, blijft een prominente dreiging. Supply chain attacks zijn subtieler: aanvallers injecteren kwaadaardige code in softwareupdates of manipuleren hardware voordat die je organisatie bereikt. Je vertrouwt op je leveranciers, maar wat als die leverancier zelf gecompromitteerd is?

Een nieuwe dimensie is verder de rol van kunstmatige intelligentie bij cyberaanvallen. Waar je vroeger diepgaande technische kennis nodig had om malware te schrijven, kunnen nu ook relatief onervaren aanvallers met behulp van AI geavanceerde aanvallen uitvoeren. De drempel om kwaad te doen is daarmee al met al dramatisch verlaagd.

Wij helpen organisaties om zich hier systematisch tegen te wapenen. Dat begint met het in kaart brengen van je aanvalsoppervlak: welke systemen zijn kritiek? Waar zitten potentiële ingangen? En hoe zijn ketens beveiligd? Op basis daarvan adviseren we over moderne security-architecturen als Zero Trust, waarbij je niet langer vertrouwt op netwerkgrenzen maar simpelweg élke toegangspoging verifieert. Ook toetsen we regelmatig of je maatregelen nog up-to-date zijn.

Groeiende complexiteit

IT-landschappen zijn in een razend tempo geëvolueerd. Hybride infrastructuren combineren on-premises datacenters met publieke en private clouds. Multi-cloud-strategieën verspreiden workloads over verschillende leveranciers. Dat biedt flexibiliteit, maar vergroot ook het aanvalsoppervlak.

IoT-devices vormen een vaak onderschat risico. Van slimme thermostaten tot sensoren in productielijnen: elk met het internet verbonden apparaat is een potentiële ingang voor aanvallers. Een berucht voorbeeld is dat van een casino dat werd leeggeroofd via de temperatuursensor in een aquarium. De sensor was verbonden met het bedrijfsnetwerk, en dat netwerk had toegang tot kritieke systemen.

Ook de integratie van OT (Operational Technology) en IT vergroot kwetsbaarheden. Productieomgevingen, industriële besturingssystemen en kritieke infrastructuur worden steeds vaker verbonden met bedrijfsnetwerken. Dat maakt ze efficiënter, maar ook kwetsbaarder voor aanvallen.

De toenemende afhankelijkheid van externe diensten brengt verder ook risico's met zich mee waar je weinig controle over hebt. Als een cloudprovider uitvalt, of als een belangrijke SaaS-applicatie niet bereikbaar is, dan ligt ook jouw organisatie stil.

Interne factoren

Niet alle oorzaken komen van buitenaf. Veel organisaties worstelen met een kennistekort; de ontwikkelingen gaan zo snel, dat IT-teams ze nauwelijks kunnen bijbenen. Best practices worden niet altijd gevolgd; niet uit onwil, maar uit gebrek aan tijd, kennis of middelen.

Een ander veel voorkomend probleem: onduidelijke processen bij incidenten. Wie mag beslissen om de stekker eruit te trekken als er een cyberaanval gaande is? Wie belt de autoriteiten? Wie informeert het management? Als die vragen niet van tevoren beantwoord zijn, gaat kostbare tijd verloren op het moment dat elke seconde telt.

Dit is waar governance en procesbegeleiding cruciaal worden. Wij voeren regelmatig interviews met organisaties om te inventariseren: heb je beleidsdocumenten rondom IT-continuïteit? Is er een plan voor disaster recovery? Wie heeft welke rol bij een incident? Door dit systematisch te doen, aan de hand van bewezen methodieken of security maturity models, krijg je helder waar de gaten zitten. En, belangrijker nog: hoe je die dicht.

Hoe voorkom je IT-uitval?

Digitale weerbaarheid vraagt om een systematische, gelaagde aanpak. Het gaat niet alleen om technische maatregelen, maar ook om processen, governance en een cultuur waarin preventie centraal staat.

Ken je risico's

De eerste stap naar digitale weerbaarheid is een grondige risico-inventarisatie. Breng in kaart wat je hebt, waar het staat, hoe het met elkaar verbonden is, en wat de impact is als het uitvalt.

Identificeer daarbij om te beginnen je 'kroonjuwelen': de meest waardevolle en kritieke assets van je organisatie. Welke systemen, data en processen zijn absoluut kritiek voor de bedrijfsvoering? Wat is de impact als ze uitvallen: financieel, operationeel en qua reputatie? En hoe waarschijnlijk is het dat dit gebeurt?

Op basis van deze analyse maak je een afweging: waar investeer je in extra beveiliging en redundantie, en waar accepteer je bewust een restrisico? Honderd procent veiligheid bestaat niet, maar door te focussen op de voornaamste risico's en de grootste impact, maak je rationele keuzes.

TIP: breng je infrastructuur in kaart

Wij gebruiken diverse discovery-tools die je netwerk en cloud scannen: welke apparatuur draait er? Hoe zijn systemen verbonden? Zijn patches up-to-date? En waar zitten kwetsbaarheden? Gecombineerd met interviews en een analyse van je bestaande documentatie ontstaat een actueel beeld, als basis voor gerichte beveiligingsmaatregelen. Dit doen we niet alleen vanuit IT-perspectief, maar integraal: inclusief governance, risicomanagement en compliance.

Zorg voor zichtbaarheid en controle

Inzicht krijgen is één ding, het behouden is iets anders. Observability (continu inzicht in wat er gebeurt in je infrastructuur) is cruciaal. Je kunt maatregelen nemen wat je wilt, maar als je niet ziet wat er gebeurt, ben je blind.

Dit vraagt om monitoring en het vastleggen van alle systeemactiviteiten over je hele infrastructuur. Gebruik Security Information and Event Management (SIEM) om patronen te herkennen en afwijkingen te detecteren. En hanteer het 'Assume Breach'-principe: ga ervan uit dat aanvallers al binnen zijn, en richt je processen daarop in. Wat doe je dan? Hoe beperk je de schade? En hoe voorkom je dat ze zich verder verspreiden? Door deze vragen vooraf te beantwoorden, kun je snel en adequaat reageren wanneer er écht iets gebeurt.

In de praktijk betekent dit dat we samen met organisaties kijken naar de juiste tooling én naar de processen eromheen.
Wie monitort wat? Hoe snel worden afwijkingen opgepikt?
Wie krijgt welke alerts? En wat gebeurt er vervolgens?
Door dit te toetsen (soms via gesimuleerde scenario's) weet je zeker dat je monitoring ook daadwerkelijk werkt wanneer het nodig is.

Operational AI: van reactief naar proactief

Traditionele monitoring laat zien wát er gebeurt. Operational AI gaat een stap verder: deze slimme systemen herkennen patronen, detecteren afwijkingen automatisch, en voorspellen waar problemen kunnen ontstaan. Zo kun je sneller reageren op incidenten of ze zelfs voorkomen.

Investeer in moderne security-architectuur

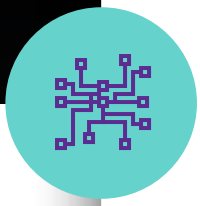
De conventionele security-aanpak (een firewall op de rand van je netwerk met daarachter vrije toegang) werkt niet meer. Moderne aanvallen omzeilen deze netwerkgrens of komen van binnenuit.

Zero Trust Network Access (ZTNA) biedt een effectief alternatief.

Het principe: vertrouw niemand, verifieer alles. Bij elke poging om toegang te krijgen tot een systeem, applicatie of dataset wordt gecontroleerd: wie ben je, waar kom je vandaan, met welk apparaat, en mag je hier überhaupt bij? En als je erbij mag, wat mag je dan precies doen: lezen, schrijven, bewerken?

Identity & Access Management (IAM) speelt hierin een centrale rol.

Niet alleen bij de grens van je netwerk, maar bij elke stap die een gebruiker zet. Dit voorkomt dat aanvallers zich door je netwerk verspreiden: toegang tot één systeem betekent niet automatisch toegang tot alle andere.



Netwerksegmentatie en micro-segmentatie compartimenteren je infrastructuur in kleinere zones.

Als één zone gecompromitteerd raakt, blijft de schade beperkt. Zeker bij de scheiding van OT- en IT-domeinen (productieomgevingen en bedrijfsnetwerken) is dit essentieel. Een cyberaanval op kantoor mag niet leiden tot stilstand van de fabriek.

Proximus NXT komt van origine uit de wereld van network en security. Dit betekent dat we niet alleen adviseren over deze architecturen, maar ze ook daadwerkelijk kunnen ontwerpen en implementeren; van de onderliggende netwerkinfrastructuur tot de security-lagen erboven. We kijken daarbij naar de hele keten: niet alleen binnen je datacenters, maar ook naar de verbindingen ertussen, je cloud-omgevingen en je eindgebruikers. Deze end-to-end benadering is essentieel voor effectieve beveiliging.

Bescherm je data op alle niveaus

Data vormt de kern van je organisatie. Beschermen doe je op drie niveaus: data in use (terwijl je ermee werkt), data in transit (tijdens overdracht), en data at rest (opgeslagen).

Encryptie vormt een fundamentele beveiligingslaag.

Versleutel data niet alleen tijdens overdracht, maar ook waar het staat; op servers, in databases en in back-ups. Ook bij een geslaagde inbraak blijft je data zo onleesbaar voor aanvallers.

Een opkomend thema is quantum-safe encryptie.

Kwantumcomputers zullen in de toekomst krachtig genoeg zijn om de huidige encryptie te kraken. Voor de meeste organisaties is dit nu nog toekomstmuziek, maar sectoren die data jarenlang moeten bewaren (zoals de zorg, financiële dienstverlening of overheden) moeten nu al

Regel daarnaast je data governance: wie heeft toegang tot welke data?

Niet iedereen hoeft immers overal bij te kunnen: een HR-medewerker heeft andere toegang nodig dan iemand van IT, een stagiair andere rechten dan een directeur. Beperk toegang tot wat strikt noodzakelijk is.

Proximus NXT implementeert quantum-safe verbindingen tussen datacenters en denkt actief mee over toekomstbestendige encryptie-strategieën. Dit gaat verder dan alleen de IT-laag: het raakt aan de fysieke infrastructuur, de optische verbindingen en de hele connectivity-keten. Door deze integrale blik kunnen we adviseren over databeveiliging op alle niveaus, van applicatie tot glasvezel.

Bouw weerbaarheid in

Digitale weerbaarheid betekent ook: redundantie op alle lagen, met dubbele voedingen, reserveverbindingen en gerepliceerde systemen. Als het ene pad uitvalt, neemt het andere het over; automatisch, zonder onderbreking.

Zorg er verder voor dat systemen up-to-date blijven: installeer beveiligingsupdates tijdig en los bekende kwetsbaarheden op voordat aanvallers ze kunnen misbruiken. Dit klinkt vanzelfsprekend, maar wordt vaak verwaarloosd door tijdgebrek of angst om productie te verstoren.

Je back-upstrategie is je laatste redmiddel. Zorg voor regelmatige back-ups, test of je ze ook kunt terugzetten, en bewaar kopieën offline (niet aangesloten op het netwerk) of ‘air-gapped’ (volledig geïsoleerd). Zo blijven ze veilig bij een ransomware-aanval die je hele infrastructuur versleutelt.

Redundantie ontwerpen vraagt om grondige kennis van je infrastructuur. Wij helpen organisaties om single points of failure te identificeren en op te lossen; niet alleen op IT-niveau, maar ook in de onderliggende netwerk- en connectivity-infrastructuur. Want een redundante applicatie-setup helpt weinig als beide verbindingen door hetzelfde kabelkanaal lopen.

Het belang van samenwerking

De complexiteit van moderne IT-landschappen maakt het bijna onmogelijk om digitale weerbaarheid alleen te realiseren. Ontwikkelingen gaan te snel, kennis is te gespecialiseerd, en de dreiging te divers. Veel organisaties missen simpelweg de expertise of de tijd om alle facetten van security, cloud, netwerken en compliance bij te houden.

In de praktijk blijkt dat organisaties die met een gestructureerde methodiek werken, doorgaans sneller en effectiever herstellen van incidenten. Dat komt door de heldere processtappen, duidelijke verantwoordelijkheden en regelmatige toetsing van de aanpak.

Een externe partner kan hierbij helpen door structuur aan te brengen en prioriteiten helder te krijgen. Dat begint vaak met een onafhankelijk risico-assessment: een frisse blik op je infrastructuur, zonder interne politiek of legacy-denken. Via discovery tools en interviews wordt helder waar de grootste knelpunten zitten.

Van daaruit volgen advies, roadmap en (indien gewenst) implementatie. Wij werken met bewezen methodieken, security maturity-modellen en onze eigen FLOW-methodiek. Deze structuur zorgt ervoor dat trajecten niet verzanden, maar stap voor stap tastbare resultaten opleveren. Wat ons onderscheidt is dat we dit integraal kunnen doen: van governance en risicomanagement tot de daadwerkelijke technische implementatie van netwerk, security en cloud-oplossingen. We kijken daarbij naar de hele keten: niet alleen naar de applicatielaag, maar ook naar de onderliggende netwerk- en connectivity-infrastructuur. Dit omvat alles van optische verbindingen tussen datacenters tot quantum-safe encryptie voor toekomstbestendige beveiliging.

Een belangrijk punt: wij kunnen ook volledig onafhankelijk opereren. Soms doen we alleen het assessment en de roadmap, zonder dat we zelf implementeren. Onze klanten waarderen deze onafhankelijkheid, omdat ze weten dat onze adviezen niet gekleurd zijn door commerciële belangen.

Onze ervaring op het gebied van network en security betekent dat we complexe, hybride omgevingen overzien en gericht kunnen adviseren over waar risico's ontstaan; niet alleen binnen je datacenters, maar ook in de verbindingen ertussen, je cloud-omgevingen en bij je eindgebruikers.

Onze ervaring in diverse sectoren (van centrale en lokale overheid tot defensie, van healthcare tot financial services en industriële omgevingen) stelt ons bovendien in staat om hierbij sectorspecifieke regelgeving en best practices mee te nemen. We weten welke eisen NIS2 stelt aan energiebedrijven, wat DORA betekent voor banken, en hoe BIO2 doorwerkt bij overheidsorganisaties. Deze kennis leidt tot concrete maatregelen die aansluiten bij jouw context.

Oefen je respons:

van papier naar praktijk

Een **disaster recovery-plan** op papier is niet genoeg. De organisaties die het beste omgaan met verstoringen, zijn degenen die regelmatig oefenen. Test je processen: wie neemt welke beslissingen? Wie belt de autoriteiten? Hoe communiceer je naar klanten? Wanneer mag de stekker eruit?

Net als bij de brandweer en defensie geldt ook hier: oefenen, oefenen, oefenen. Zo weet je dat je plannen werken wanneer elke seconde telt. En je ontdekt ondertussen waar aannames niet klopten en waar processen schuren.

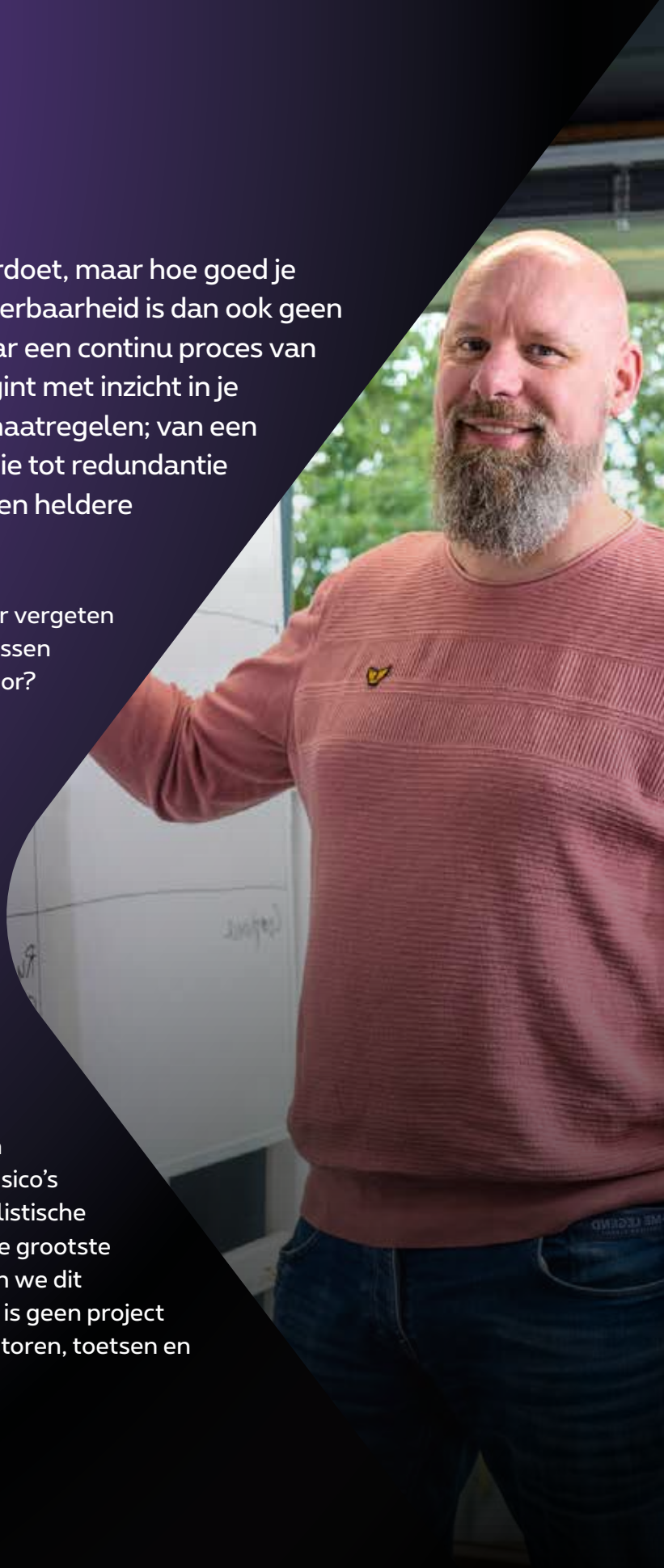
Wij begeleiden organisaties bij dit soort oefeningen. Door scenario's door te spelen ontdek je of je plannen kloppen en of iedereen weet wat zijn of haar rol is. Dit geeft niet alleen vertrouwen, maar legt ook bloot waar je processen aanscherping nodig hebben.

Conclusie

De vraag is niet of een verstoring zich voordoet, maar hoe goed je organisatie erop voorbereid is. Digitale weerbaarheid is dan ook geen eenmalig project met een einddatum, maar een continu proces van meten, verbeteren en anticiperen. Het begint met inzicht in je kwetsbaarheden en groeit via gelaagde maatregelen; van een moderne security-architectuur en encryptie tot redundantie in je infrastructuur, regelmatige back-ups en heldere toegangscontroles.

Veel organisaties investeren in technologie, maar vergeten hun besluitvorming te testen. Wie mag wat beslissen als het erop aankomt? Welke processen gaan voor? Zonder oefening blijven zelfs de beste plannen theorie. De organisaties die het beste omgaan met verstoringen, zijn niet per se degenen met de meeste technologie. Het zijn degenen die regelmatig oefenen, heldere processen hebben en weten wie wat mag beslissen in een crisis.

De complexiteit van moderne IT-omgevingen maakt externe expertise vaak onmisbaar. Begin met een grondige inventarisatie van waar je staat. Laat je infrastructuur scannen, voer interviews om je governance en processen in kaart te brengen, en identificeer samen met specialisten je grootste risico's en je kroonjuwelen. Van daaruit bouw je een realistische roadmap. Wat pakken we eerst aan? Waar ligt de grootste impact? Welke quick wins zijn er? En: hoe houden we dit vervolgens levend? Want digitale weerbaarheid is geen project dat 'af' is, maar een doorlopend proces van monitoren, toetsen en bijsturen.



Over Proximus NXT

Proximus NXT (met vestigingen in de hele Benelux) is gespecialiseerd in het bouwen en beheren van veilige, betrouwbare en altijd beschikbare IT-infrastructuren. We combineren diepe technische expertise op het gebied van connectivity, netwerk, security en cloud met een praktische aanpak die past bij jouw organisatie.

Wat ons onderscheidt:

- **End-to-end connectiviteit:** Van optical verbindingen tussen datacenters tot quantum-safe encryptie, van SD-WAN tot hybride cloud-oplossingen: wij kijken naar de hele keten, niet alleen naar de applicatielaag.
- **Security & network DNA:** We komen van origine uit network en security, waardoor we moderne architecturen als Zero Trust niet alleen adviseren maar ook volledig kunnen implementeren.
- **Onafhankelijk advies:** We kunnen trajecten ook volledig onafhankelijk uitvoeren: alleen assessment en roadmap, zonder implementatieverplichtingen.
- **Brede sector-ervaring:** Van centrale en lokale overheid tot healthcare, financial services en industriële omgevingen: we kennen de specifieke regelgeving en uitdagingen per sector.
- **Integrale aanpak:** Niet alleen technologie, maar ook governance, risicomanagement en compliance. Van beleidsdocumenten tot disaster recovery-oefeningen.

Met onze FLOW-methodiek brengen we structuur aan in complexe trajecten: van eerste gesprek en risico-assessment tot advies, roadmap, implementatie en doorlopend beheer. We begeleiden organisaties bij compliance met NIS2, DORA, Wwke, BIO2, ABRO en ABDO. En we zorgen ervoor dat digitale weerbaarheid niet blijft steken in plannen, maar werkelijkheid wordt in je dagelijkse operatie.

Onverhoopt toch een IT-uitval?
Raadpleeg DEZE CHECKLIST om te zien wat je moet doen.

Wil je weten waar je organisatie staat en welke stappen het meest urgent zijn?

Neem contact op voor een vrijblijvend gesprek.

contact