Whitepaper

Wat als je elkaar niet meer kan bereiken?

De realiteit van digitale afhankelijkheid
bij gemeenten en veiligheidsregio’s

De overheid draait op digitale voorzieningen. Dit geldt voor communicatie, samenwerking en essentiële dienstverlening. In het dagelijks werk is die afhankelijkheid vanzelfsprekend geworden. Zolang alles werkt, is dat nauwelijks zichtbaar. Maar als het misgaat, wordt duidelijk hoe groot die afhankelijkheid is. Veel organisaties gaan ervan uit dat telecom en digitale voorzieningen beschikbaar blijven. Toch is dat geen vanzelfsprekendheid. Bij langdurige verstoringen, zoals stroomuitval of andere grootschalige incidenten, komt die afhankelijkheid direct onder druk te staan.

Binnen crisisbeheersing speelt de 72-uurs realiteit een cruciale rol. Na die eerste periode verandert het speelveld. De focus verschuift van acute respons naar continuïteit: kunnen organisaties hun dienstverlening blijven leveren en als overheid blijven functioneren? Het gaat daarbij om het in stand houden van essentiële dienstverlening, het kunnen nemen van besluiten en het blijven samenwerken tussen organisaties. Communicatie is daarvoor een voorwaarde. Juist dan wordt zichtbaar hoe kwetsbaar organisaties zijn als digitale voorzieningen niet meer vanzelfsprekend beschikbaar zijn.

In dit whitepaper verkennen Veiligheidsregio Twente en IT Platform Twente, ondersteund door TReNT Glasvezel, wat dit in de praktijk betekent. In hoeverre zijn aannames over beschikbaarheid van netwerken realistisch, en wat vraagt dat van de manier waarop je continuïteit organiseert? Met praktijkervaringen en de inzet van een gezamenlijke regionale infrastructuur laten we zien hoe je als regio minder afhankelijk wordt en meer regie houdt wanneer het erop aankomt.

In dit whitepaper lees je meer over de volgende onderwerpen

- De 72-uurs realiteit
- Het sneeuwbaleffect van langdurige uitval
- De Twentse benadering van samenwerking op regionaal niveau
- Rollen van de drie betrokken organisaties uitgelegd

De afhankelijkheid van digitale infrastructuur

Binnen gemeenten en veiligheidsregio's is digitalisering diep doorgedrongen in de dagelijkse operatie. Meldkamers, crisiscoördinatie, datacenters, sensoren, camera's en drones leveren cruciale informatie voor situational awareness en besluitvorming. Zo worden drones ingezet bij natuur- en industriebranden om snel inzicht te krijgen in de omvang, locatie en ontwikkeling van incidenten. Die informatie is essentieel voor de eerste inzet, maar volledig afhankelijk van verbindingen, stroom en netwerken.

Deze afhankelijkheid maakt organisaties efficiënt en slagvaardig, maar vergroot tegelijkertijd de kwetsbaarheid. Wanneer één schakel uitvalt, stroom, telecom of netwerk raakt dat direct meerdere processen tegelijk.

De 72-uurs realiteit
Binnen crisisbeheersing wordt vaak gesproken over de zogenoemde 72-uurs realiteit. Burgers worden geacht zichzelf gedurende die periode te kunnen redden. Voor overheden en hulpdiensten geldt het tegenovergestelde: juist in deze periode moet de overheid blijven functioneren. Besluiten moeten worden genomen, informatie moet worden gedeeld en samenwerking moet mogelijk blijven.

Daar wringt een ongemakkelijke waarheid. Veel organisaties gaan ervan uit dat hun communicatie en IT-infrastructuur ook bij calamiteiten beschikbaar blijft, vaak dankzij de Noodcommunicatievoorziening (NCV) of back-upnetwerken. Wat daarbij regelmatig over het hoofd wordt gezien, is dat een groot deel van deze infrastructuur bestaat uit straatkasten, knooppunten en tussenstations met geen of slechts beperkte noodstroomvoorzieningen.

Bij een langdurige stroomuitval vallen deze onderdelen daardoor vaak sneller uit dan verwacht. Het gevolg is dat verbindingen waarop men denkt te kunnen vertrouwen, in de praktijk maar beperkt beschikbaar blijven.

Het sneeuwbaleffect van langdurige uitval
Tegelijkertijd kennen bestaande systemen duidelijke grenzen. Het C2000-netwerk, essentieel voor hulpdiensten, maakt mede gebruik van openbare infrastructuur van telecomproviders. Bij grootschalige stroomuitval vallen zendmasten en knooppunten uit zodra de noodaccu’s na enkele uren leeg zijn. Daardoor verliest het C2000-netwerk de verbinding en is het niet meer operationeel bij langdurige stroomuitval.

Monitoring van kritieke infrastructuur, zoals gemalen of dijken, is vaak afhankelijk van mobiele netwerken en komt daarmee eveneens onder druk te staan.

Zo ontstaat een kettingreactie waarin afhankelijkheden elkaar versterken. Wat begint als een stroomstoring, groeit uit tot een bredere verstoring van communicatie, informatievoorziening en uiteindelijk bestuurlijke slagkracht.

Regie op eigen infrastructuur
Juist in die context wordt duidelijk hoe belangrijk het is om regie te houden op infrastructuur. Binnen de Veiligheidsregio Twente wordt communicatie niet gezien als een ondersteunend proces, maar als een absolute randvoorwaarde. Daarom is er bewust gekozen voor aanvullende maatregelen die verder gaan dan standaardoplossingen. Er wordt gewerkt met eigen infrastructuur, redundante verbindingen en noodvoorzieningen die ervoor zorgen dat communicatie zo lang mogelijk overeind blijft. Zo zijn er mogelijkheden om vaste telefonie lokaal in stand te houden en kan via eigen netwerken, bijvoorbeeld met portofoons en repeaters, communicatie in het veld blijven plaatsvinden, onafhankelijk van het internet of het mobiele netwerk. Deze aanpak vraagt om meer dan technische maatregelen alleen. Het vereist samenwerking op regionaal niveau.

De rollen van de drie betrokken organisaties uitgelegd

1 Veiligheidsregio Twente

2 IT Platform Twente

3 TReNT Glasvezel

Een samenwerking op regionaal niveau

Veiligheidsregio Twente

De Veiligheidsregio Twente (VRT) is verantwoordelijk voor de veiligheidsbeheersing in de regio. Haar missie en visie zijn gericht op "samen werken aan een veilig Twente" . De VRT fungeert als een stabiele factor in tijden van verandering en richt zich op het verhogen van het fysieke veiligheidsniveau van de inwoners van Twente. Dit gebeurt door middel van twee hoofddisciplines: *risicobeheersing* en *crisisbeheersing*. Bij risiscobeheersing richt de organisatie zich op de preventie van rampen en crises. Crisisbeheersing omvat de voorbereiding op, de respons tijdens, en het herstel na afloop van rampen en crises in Twente.

IT Platform Twente

Binnen Twente speelt het IT Platform Twente een centrale rol in het organiseren van een samenwerking op regionaal niveau. Dit samenwerkingsverband verbindt gemeenten en publieke organisaties rondom hun digitale infrastructuur. Het doel daarvan is niet alleen efficiëntie, maar vooral weerbaarheid.

Door gezamenlijk te investeren in infrastructuur, kennis en analyses ontstaat een gedeeld beeld van risico’s en afhankelijkheden. Het platform maakt het mogelijk om verder te kijken dan de grenzen van individuele organisaties en om digitale weerbaarheid als een gezamenlijke verantwoordelijkheid te benaderen.

In die samenwerking komt een belangrijk inzicht naar voren: kwetsbaarheden ontstaan vaak niet doordat systemen ontbreken, maar doordat aannames niet expliciet zijn gemaakt. Door die aannames zichtbaar te maken en met elkaar te bespreken, ontstaat ruimte voor bewuste keuzes.

TReNT Glasvezel

TReNT vervult binnen deze context een cruciale rol als infrastructuurpartner. Als regionale partij faciliteert TReNT de fysieke glasvezelverbindingen die de basis vormen voor betrouwbare communicatie tussen gemeenten en de veiligheidsregio.

Door inzet van eigen glasvezelinfrastructuur en ringstructuren wordt de afhankelijkheid van commerciële telecom verkleind. Organisaties krijgen daarmee meer controle over hun verbindingen en kunnen beter borgen dat essentiële communicatie ook onder extreme omstandigheden beschikbaar blijft.

Deze combinatie van regionale samenwerking, eigen infrastructuur en gedeelde verantwoordelijkheid vormt de kern van de aanpak in Twente.

Conclusie

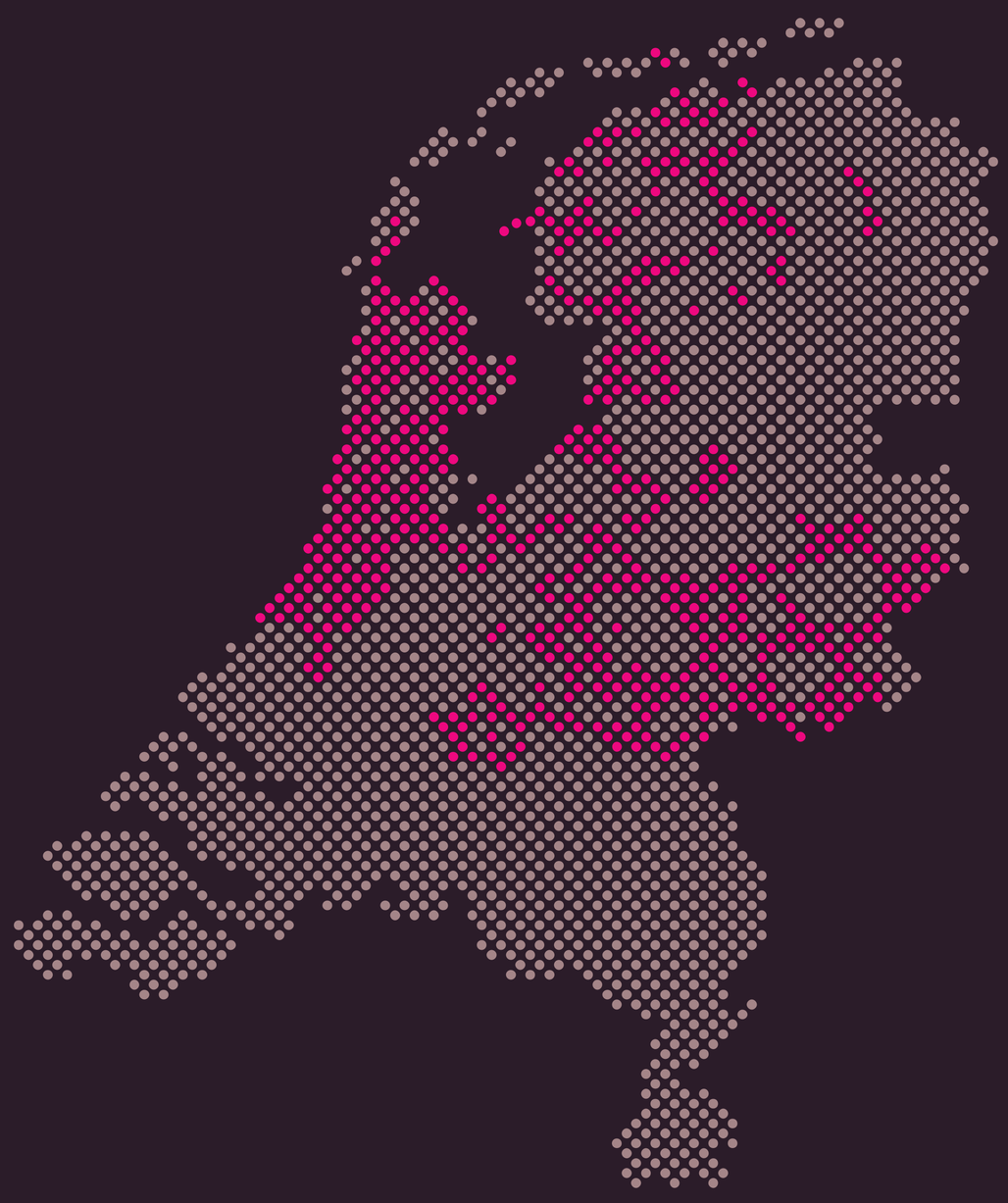
Niet alle risico’s zijn uit te sluiten en niet elke digitale afhankelijkheid is volledig te beheersen. De essentie ligt daarom niet in het creëren van een perfecte situatie, maar in het ontwikkelen van bewustzijn en regie. Dat begint bij inzicht: weten waar kwetsbaarheden zitten, begrijpen welke aannames worden gedaan en expliciet bepalen welke risico’s acceptabel zijn en welke niet.

Het echte risico schuilt niet in uitval op zichzelf, maar in het ontbreken van dat inzicht. Zolang organisaties onvoldoende zicht hebben op hun eigen aannames, ontstaat het gevaar van onbewust onbekwaam handelen. Juist dat is in een crisissituatie geen optie meer.

Binnen de samenwerking tussen Veiligheidsregio Twente, IT Platform Twente en TReNT wordt deze bewustwording actief georganiseerd. Door gezamenlijke infrastructuur, gedeelde analyses en realistische scenario’s ontstaat meer grip op digitale afhankelijkheden. Niet omdat uitval volledig te voorkomen is, maar omdat verrassing op het moment dat het erop aankomt geen optie mag zijn.

TRENT GLASVEZEL

Betrouwbare connectiviteit voor
bedrijfskritische ICT-toepassingen.



www.trentglasvezel.nl