# Een netwerk is zo sterk als de zwakste schakel

## Vergroot de beschikbaarheid van je netwerk

**Ben jij verantwoordelijk voor de continuïteit van jullie bedrijfsnetwerk? En wil je tips en adviezen om de betrouwbaarheid ervan te vergroten? In dit whitepaper delen signetbreedband en Eurofiber hun kennis en ervaring.**



signet breedband

eurofiber

*“Als één schakel in ons proces stilvalt, ligt onze business plat. We moeten daarom altijd kunnen vertrouwen op een veilige en stabiele internetverbinding.”*
*– Mark Loos, Directeur IPHandlers*

# Netwerkbeschikbaarheid is cruciaal

Wanneer een bedrijfsnetwerk uitvalt, is dat lang niet altijd zomaar ‘vervelend’. Staat de productie stil, dan kost het al snel veel geld. Kunnen de vrachtwagens niet laden, lossen en rijden? Dan is de levering niet tijdig bij de klant, die zelf ook niet verder kan. Netwerkbeschikbaarheid is cruciaal, ook voor het mkb. Maar wat is netwerkbeschikbaarheid? Welke factoren hebben daarop invloed? Wat kan je zelf doen en wat regel je via een leverancier? En hoe overtuig je het management van het belang? In dit whitepaper delen de netwerkspecialisten van signetbreedband en Eurofiber hun kennis en ervaring.

# 1. Uitdagingen voor de IT-manager

Als IT-manager ben je betrokken bij tal van processen binnen het bedrijf. IT is namelijk niet meer alleen een technisch ondersteunend proces, het kruipt steeds dichter tegen de bedrijfsprocessen aan. Netwerkbetrouwbaarheid staat zelden hoog op de agenda. Er zijn altijd bedrijfskritische vraagstukken en processen die als eerste om aandacht vragen. Toch is netwerkbetrouwbaarheid zelden een kwestie van geld, maar van prioriteit.

**Redundante oplossing te duur**

Een redundant netwerk is zo sterk als de zwakste schakel. De internettoegang is meestal goed geregeld, maar mkb-bedrijven kiezen vaak voor één firewall in plaats van een redundant uitgevoerde firewall. Dit vanwege de kosten. De infrastructuur daarachter is doorgaans wel redundant, omdat switches relatief goedkoop zijn. Een volledig redundante infrastructuur sneuvelt in veel gevallen in de offertefase. Zo'n investering is namelijk lastig te verantwoorden aan het management. Zeker als een netwerk nog nooit is uitgevallen.

**De uptime gaat omlaag**

Als je netwerkbeschikbaarheid niet goed regelt, gaat de maximale uptime omlaag. Bedrijven vertrouwen vaak op de provider, maar die heeft niet altijd alles zelf in de hand. Stel dat een verbinding uitvalt door een doorgraving van een glasvezelkabel. Dan belt de provider een aannemer die de oorzaak moet achterhalen. Dat kan al snel een paar uur duren.

**Een kwestie van gevoelde prioriteit**

Zolang het IT-netwerk draait, voelen de meeste bedrijven geen noodzaak extra maatregelen te nemen. Die kosten geld en leveren niet direct iets tastbaars op. Dat kan leiden tot een kloof tussen degene die moet investeren (het management) en degene die de noodzaak ziet (de IT-manager).

De impact van een netwerkstoring kan groot zijn. Als dat gebeurt, wordt het voor de IT-manager vaak makkelijker om maatregelen erdoor te krijgen. Valkuil is dat een bedrijf door haast of stress niet de beste keuzes maakt. Denk dus vooraf na over het belang van connectiviteit en netwerkbeschikbaarheid.

**Learnings**

- Netwerkbetrouwbaarheid is zelden een kwestie van geld, maar meestal van prioriteit.
- De keuze voor een redundante infrastructuur sneuvelt vrijwel altijd in de offertefase.
- Zolang het netwerk draait, wordt de noodzaak zelden gevoeld door het management.
- De impact van een netwerkstoring kan (enorm) groot zijn.
- Denk daarom vooraf na over het belang van connectiviteit en netwerkbeschikbaarheid.

# 2. Wat is netwerkbeschikbaarheid?

De simpele definitie kan zijn: de beschikbaarheid van een bedrijfsnetwerk voor het storingsvrij uitvoeren van taken. Maar de netwerkbeschikbaarheid hangt af van wat jij ziet als jouw netwerk én wat daarover is afgesproken. Het netwerk van een administratiekantoor met vijf medewerkers is anders dan dat van een productiebedrijf met meerdere locaties. Het ene netwerk is bedrijfskritischer dan het andere.

***99% uptime = maximaal 4 dagen downtime per jaar***

*In de Service Level Agreement (SLA) met de provider maak je afspraken over netwerkbeschik-baarheid. Die percentages spreken vertrouwen uit. Maar een uptime van 99% (vaak het minimum dat providers aanbieden) betekent dat het netwerk er maximaal vier dagen per jaar uitligt. Een uptime van 99,5% staat gelijk aan een maximale downtime van ruim 50 minuten per week. Dit komt neer op bijna twee volle dagen op jaarbasis. Dat sluit vaak niet aan op de business requirements. Je kunt bij providers daarom ook een uptime garantie afsluiten tot wel 99,99%, wat neerkomt op maximaal 1 uur downtime per jaar.*

Vroeg of laat is (on)geplande downtime onvermijdelijk. In alle zeven lagen van het OSI-model kan iets fout gaan: van fysieke infrastructuur tot applicatie. En van patchkast tot point of presence (POP), de fysieke locatie waar communicatie-apparaten een verbinding tot stand brengen. Een storing kan ook veroorzaakt worden doordat op een of meerdere plekken wijzingen in het netwerk plaatsvinden. Goed communiceren is hierbij cruciaal; IT blijft immers mensenwerk.

*Oorzaken van netwerkuitval zijn heel divers:*

**Fysieke oorzaken**

De meeste netwerkstoringen worden veroorzaakt in de omgeving van het bedrijf (the last mile), vooral door graafwerkzaamheden. Dergelijke storingen zijn soms moeilijk op te lossen. Stel dat een kapotte glasvezeltube 144 kabels bevat, dan moeten die individueel aan de juiste andere kant worden gelast.
Andere fysieke oorzaken zijn een stroomstoring, brand en waterschade. Maar ook een inpandige kabelbreuk is een risico. Bijvoorbeeld als iemand een deur tegen een kabel drukt of wanneer een patchkabel vervuild raakt.

**Fouten in de configuratie**

Ook fouten in de configuratie kunnen een netwerk-storing veroorzaken. Stel dat je een netwerk hebt waarbij achter twee redundante core-switches zes verschillende netwerken zitten. Dan kan het met spoed handmatig wijzigen van één poort ervoor zorgen dat het standaard netwerk het weer doet en de vijf andere netwerken eruit liggen. Dan kan het even duren voordat de oorzaak van zo'n storing is achterhaald. De meest basale oorzaak van downtime is defecte apparatuur; check regelmatig de werking ervan en vervang indien nodig.

**Learnings**

- Sommige netwerken zijn bedrijfskritischer dan andere; daarom heeft iedereen zijn eigen definitie van netwerkbeschikbaarheid.
- Van fysieke infrastructuur tot applicatie; overal in het netwerk kan iets misgaan.
- Veel netwerkstoringen komen door graafwerk-zaamheden in de buurt.
- Inpandig is kabelbreuk een reëel risico.
- Kleine configuratiefouten kunnen ook een netwerkstoring veroorzaken.
- Bij een uptime van 99% kan een netwerk er theoretisch gezien tot vier dagen per jaar uitliggen.

***"Alle kritische componenten in onze netwerkoplossing zijn redundant uitgevoerd. Zo zijn 140 locaties voorzien van een mobiel back-up verbinding. Internet is cruciaal voor ons bestel- en distributieproces. Even zonder betekent geen telefonie én geen bestellingen."***
*– John Junggeburt, Director Central Services*
*Alliance Automotive Group Benelux*


# 3. De impact van netwerkuitval

Netwerkuitval kan veel impact hebben. Wat de precieze gevolgen zijn hangt van vele factoren af. Voor elke branche is dat weer net even anders.

**Logistiek**

Een logistiek bedrijf heeft externe koppelingen met leveranciers. En in het magazijn zijn vaak grote wifi-netwerken aanwezig. Door een storing in één van de netwerken kunnen bijvoorbeeld vrachtwagens niet meer laden of lossen, omdat Warehouse Management Software (WMS) en de handscanners niet werken. Vrachtwagens staan stil, wat een kostenpost is.
Ook geeft het problemen in de verdere keten van de klant. Netwerkuitval in het magazijn ontstaat vaak na herinrichting. Denk aan wifi-access points die onder een stalen rek worden gehangen en daardoor niet meer goed werken.

**Industrie**

Bij een industrieel bedrijf kunnen de activiteiten vaak alleen in en rond het pand gebeuren, daar waar de productie plaatsvindt. Valt het netwerk op kantoor uit, dan kunnen mensen thuiswerken, als hun applicaties in de cloud staan. Maar het lokale netwerk van de fabriek is cruciaal voor de productieprocessen. Bij uitval is de economische schade meestal groot. Zo'n netwerk moet daarom voldoen aan de hoogste uptime- en performance-eisen, door het inbouwen van redundantie.

**Zakelijke dienstverlening**

Voor zakelijke dienstverleners doet netwerkwise de lokale hoofdvestiging er tegenwoordig vaak minder toe, omdat gewerkt wordt met externe datacenters en clouddiensten. Die moeten overal en altijd goed én veilig bereikbaar zijn voor medewerkers en klanten. Dat stelt hoge eisen aan de kritische netwerken. Stel dat er een storing is in het datacenter in Amsterdam. Dan is het fijn als er nog een datacenter is als back-up. Is dit goed ingeregeld, dan worden medewerkers minder afhankelijk van het hoofdkantoor en zijn netwerken bedrijfszekerder. Dat geldt ook voor kantoren met meerdere kantoren of vestigingen. Voorheen stonden de servers on-premise op het hoofdkantoor. Alle nevenkantoren moesten daarnaartoe verbinden. In de moderne IT-infra-structuur is ook het hoofdkantoor 'slechts' een nevenkantoor.

# 4. Maatregelen voor een hoge netwerkbeschikbaarheid

Wil je een netwerk met een zo hoog mogelijke beschikbaarheid? Dat kan op allerlei manieren. Hoe meer zekerheid je nodig hebt, hoe hoger de investering in hardware, softwarelicenties, beheer en onderhoud. Hieronder de belangrijkste maatregelen die je in samenwerking met de provider kan nemen:

**Segmentatie van netwerken**
Met netwerksegmentatie scheiden we de kritische en niet-kritische delen in kleinere segmenten. Daartussen zit een beveiligd koppelvlak. Dit minimaliseert het risico dat twee kritische netwerken tegelijkertijd uitvallen. Bij een storing is de oorzaak sneller duidelijk en hoef je niet te richten op niet-kritische onderdelen. Dit verkort het trouble shooting-traject en vergroot de uptime.

**Aparte omgevingen voor IT en OT**
De laatste decennia zijn de omgevingen voor Information Technology (IT) en Operational Technology (OT) steeds meer naar elkaar toegegroeid. Dit vergroot de gevoeligheid voor netwerkstoringen, vooral nu hackers ook via het internet de OT-omgeving kunnen binnen-dringen. Door te segmenteren blijft de OT-omgeving zo ver mogelijk gescheiden van het internet en is alleen je IT-omgeving verbonden. Omdat elk segment is gescheiden, hebben hackers toegang tot maar één segment en niet tot het volledige netwerk. Issues in segmenten zijn ook makkelijker te traceren.

**Redundantie**
Is je bedrijf sterk afhankelijk van een bepaald netwerk? Laat dit dan redundant uitvoeren. Dat kan op verschillende manieren: van 4G-backup tot een drievoudig redundant MPLS-netwerk met noodstroom en voeding vanuit meerdere datacenters. Een redundant netwerk kan op je wensen en behoeften worden ingericht.

Een slimme keuze is een volledig fysiek gescheiden IT-netwerkstructuur. Hierbij liggen de kabels niet in dezelfde geul of hetzelfde pad. Dit voorkomt uitval door graafwerkzaamheden of onderhoud aan één van de verbindingen. Vervolgens worden zoveel mogelijk componenten dubbel uitgevoerd. Daarmee zorg je voor een fail-over (HA-oplossing). Valt één van de componenten uit, dan neemt een andere component het automatisch over.

Welke componenten belangrijk zijn? Dat hangt ervan af waar de servers staan: on-premise, in de cloud of in een extern datacenter. Een volledig redundante netwerkoplossing bestaat uit zowel WAN- als LAN-redundantie. Zo blijft de verbinding werken bij uitval van zowel de externe infrastructuur als van een verbinding of apparatuur.

**Componenten dubbel uitvoeren**
Kies je voor een redundante infrastructuur en twee datacenters, dan worden ook de switches en de routers dubbel uitgevoerd. Dit voorkomt dat de actieve netwerk-apparatuur een single point of failure wordt. Denk ook aan dubbele firewalls en het dubbel uitvoeren van de hardware in de IT-omgeving.

***"We beseffen ons maar al te goed hoeveel data er over onze lijn gaat. Dat we gebruikmaken van een dubbele verbinding via verschillende providers geeft ons een geruststellend gevoel."***
*– Marcel Verdonk, IT-Manager BenQ Europe*

**Twee datacenters voor directe synchronisatie**
Het summum van redundantie zijn twee of meer datacenters op twee fysiek gescheiden locaties die de data direct synchroniseren. Die moeten ook een fysiek gescheiden infrastructuur hebben, zodat een kabelbreuk door graafwerkzaamheden geen impact heeft.

**Voorzieningen in het externe datacenter**
Draait het netwerk in een datacenter? Daar is in een noodstroomvoorziening en een fail-over procedure voorzien, waarbij een tweede server de taken van de primaire server overneemt. Zorg ook voor de redundantie van de volledige infrastructuur naar een ander datacenter. Je hebt dan geen last van een storing in één van de datacenters. Blijf je voorlopig werken met een on-premise netwerk, deels of volledig? Dan is een UPS-noodstroomvoorziening of zelfs een noodstroomaggregaat aan te bevelen, bijvoorbeeld in productieomgevingen.

***Tip: kies voor een provider in de regisseursrol***
*Zo'n provider garandeert dat de verbindingen ook echt volledig redundant zijn. Je weet dan zeker dat deze verbindingen niet in dezelfde geul of hetzelfde pad liggen. Dit voorkomt gelijktijdige uitval, in geval van bijvoorbeeld graafschade of onderhoud.*

**4G of 5G geschikt voor redundantie**
Een mobiele netwerkverbinding is een geschikte oplossing voor redundantie, maar dan vaak alleen als back-up-oplossing omdat bandbreedte en legacy een rol spelen. Met een 4G-/5G-oplossing kun je prima de primaire behoeften van sommige belangrijke applicaties opvangen. Maar als je met veel gebruikers tegelijk werkt of wilt (video)bellen, zijn er betere oplossingen voorhanden.

**Monitoring**
Met monitoring volg je de prestaties en status van alle netwerken binnen het bedrijf. Je kunt dan reageren voordat een melding een probleem wordt.
Zo'n monitoring-tool is relatief betaalbaar en eenvoudig zelf in te richten. De provider kan je helpen als je de monitoring zelf wilt inrichten.

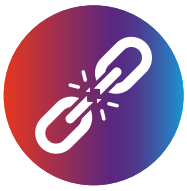
Wat jullie nodig hebben? Dat hangt af van het type organisatie, de mate van risico's en de impact daarvan. Weeg dit zorgvuldig af, zodat je niet een onnodig dure oplossing hebt, maar de redundantie wel écht goed is geregeld. En voorkom dat ergens in het netwerk tóch een single point of failure zit.

Nu kun je de investeringen afwegen tegen de mogelijke risico's en gevolgen van een netwerkuitval.

**Learnings**
- Is je organisatie sterk afhankelijk van een netwerk? Laat dit redundant uitvoeren.
- Een redundant netwerk kan op je wensen en behoeften worden ingericht; een provider kan je hierbij helpen.
- Met netwerksegmentatie worden de kritische en niet-kritische delen gescheiden in kleinere segmenten.
- Monitoring van het netwerk helpt netwerkuitval te voorkomen.
- Een mobiele netwerkverbinding is een geschikte back-up oplossing voor redundantie.

# 5. Wat kun je zelf doen als IT-manager?

Een netwerk is zo sterk als de zwakste schakel. Het is dus cruciaal dat je inzicht hebt in de totale IT-netwerkomgeving, de risico's en de impact van een eventuele netwerkuitval. Op basis daarvan kun je het management gericht adviseren. Hieronder 10 tips voor IT-managers voor het verhogen van de netwerkbeschikbaarheid:



**1. Voer een single point of failure-analyse uit**

Analyseer met het IT-team iteratief alle onderdelen van het netwerk. Teken het netwerk zorgvuldig uit en bekijk waar de single points of failure (SPOF's) zitten. Doe dit zo doemdenkerig mogelijk! Bekijk daarna per SPOF hoe kritisch deze is en wat het kost als dit onderdeeltje defect gaat. Eén apparaat heeft de potentie om veel gebruikers uit te schakelen. Deel het netwerk daarom op in kleine blokjes. Dit voorkomt ook een broadcast storm, waarbij een verzonden bericht steeds verder rondzingt in het netwerk totdat dit uitvalt. Zelf kom je een heel eind met het formuleren van de SPOF's. Maar je krijgt het plaatje pas echt compleet samen met een partij die het connectiviteitsplatform volledig overziet.

**2. Zorg voor goede actuele documentatie**

Wanneer je een goed beeld hebt van hoe je netwerk in elkaar steekt, is het raadzaam om deze zo goed mogelijk te beschrijven. Goede documentatie als belangrijke informatiebron is bijvoorbeeld cruciaal bij het overdragen van kennis en verantwoordelijkheden. Heb je de documentatie opgezet, houd deze dan ook actueel. Zo houd je ten alle tijden grip op je IT-omgeving.

**3. Maak een risicoanalyse**

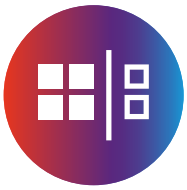
Wat kost het als het netwerk van je bedrijf of afdeling acht uur uitvalt? Wat is de schade qua omzet, extra opslagruimte en boetes? Welke gevolgen heeft het voor medewerkers, leveranciers en klanten? Kijk bij de risicoanalyse ook naar het gebied waar je pand staat. Wordt in de omgeving veel gebouwd of worden veel wegen aangelegd, dan is het risico op een storing groter. Zitten er misschien anderen op het bedrijfsnetwerk? Bijvoorbeeld dat bedrijf dat ook in jullie pand zit en en zelf de IT regelt? Waar werken zij mee? En hóe werken zij? Elk onderdeel van een netwerk heeft de potentie om een heel netwerk plat te leggen. De provider kan een berekening maken van de gemiddelde storingstijd en van de gemiddelde reparatietijd. De kosten van de redundantie-maatregelen moeten opwegen tegen de schade bij uitval.

**4. Praat met de managers in het bedrijf**

Vraag het management naar de belangrijkste processen die móeten blijven draaien. Welke IT-onderdelen zijn cruciaal? Hoeveel downtime kan het bedrijf of de afdeling zich permitteren? Welke gevolgen heeft het als zo'n kritisch onderdeel uitvalt? Maak daarvan indien mogelijk een kostenberekening.


**5. Maak een interne SLA**

Het loont om een interne SLA te maken voor specifieke afdelingen. Daarin leg je vast aan welke afspraken de IT-afdeling moet voldoen om te garanderen dat een storing binnen een bepaalde tijd is verholpen. In een interne SLA kun je vervolgens aangeven welke maatregelen nodig zijn en de kosten relateren aan de beschikbaarheid van een specifieke afdeling.



**6. Segmenteer kritische en niet-kritische onderdelen**

Van sommige netwerkonderdelen is het niet gelijk een ramp als dat er een paar uur uit ligt. Denk aan een deel van het kantoornetwerk. Ligt de fabriek plat als een onderdeel uitvalt? Dan zijn de gevolgen al snel groot. Door te segmenteren scheid je de kritische en niet-kritische delen in kleine, beveiligde onderdelen. Hierdoor is je kritische netwerkomgeving dus beter beschermd.

**7. Voorstel van jouw provider**

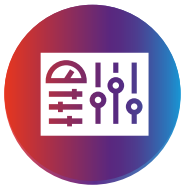
Heb je het IT-netwerk en de kritische en niet-kritische onderdelen in kaart gebracht? Ga dan in gesprek met de netwerkprovider. Die denkt mee, stelt kritische vragen en doet een voorstel voor maatregelen. De provider kijkt ook naar de verbindingen en back-up-mogelijkheden op jullie locatie. Een goed advies is een advies dat 100% aansluit op jullie situatie, wensen en eisen. Ook als dat betekent dat de provider een derde partij inschakelt omdat dat het best is voor de connectiviteit.

**8. Vraag goed door**

Kies je voor een redundant netwerk? Vraag dan goed door naar de technische en de procesmatige aspecten van connectiviteit. En naar de impact op de netwerkbeschikbaarheid voor je organisatie. Welke kwaliteit levert de provider op de secundaire verbinding? Voert hij de apparatuur redundant uit? Welke service en support krijg je? Wie bel je bij een storing? En wanneer voert de provider onderhoud uit?

**9. In gesprek met de leveranciers**

Vooral productiebedrijven en logistieke bedrijven hebben te maken met netwerkkoppelingen naar externe leveranciers. Het is belangrijk dat óók zij hun netwerken redundant uitvoeren. Blijf daarover in gesprek met de leveranciers, vooral als ze wijzigingen doorvoeren in de verbindingen.



**10. Blijf in controle over het totale IT-netwerk**

De IT-infrastructuur is een momentopname, want je bedrijf ontwikkelt zich ongetwijfeld door. Check regelmatig de werking van de netwerkcomponenten en de noodstroomvoorzieningen. Dit helpt netwerkuitval te voorkomen.
En bedenk dat ook nieuwe hardware –op den duur- defect kunnen raken.

# 6. Over signetbreedband en Eurofiber

signetbreedband werkt samen met Eurofiber aan een optimale netwerkbeschikbaarheid. signetbreedband als netwerkonafhankelijke connectiviteits-specialist, Eurofiber als een belangrijke netwerk-partner.

Bedrijven die de allerhoogste eisen stellen aan de netwerkbeschikbaarheid, kunnen kiezen voor een volledig redundant netwerk zónder single points of failure. Met volledig gescheiden glasvezelverbindingen die naar gescheiden POP-locaties gaan, duplicatie van de actieve componenten en goede fail-over procedures. Is de continuïteit van het netwerk voor jouw bedrijf essentieel en kun je je het niet permitteren om een paar uur per jaar offline te zijn, dan adviseren we om alles in het eigen domein redundant uit te voeren. Dit voorkomt dat daar alsnog single points of failure ontstaan. Kortom, met deze oplossing elimineer je alle risico's.

Maar is dit voor jouw bedrijf nodig en wegen de kosten van de redundantie-maatregelen op tegen de schade bij uitval? Dit is voor ieder bedrijf anders. Het is namelijk afhankelijk van veel verschillende factoren waaronder het risico op netwerkuitval, de impact hiervan op je bedrijf. Bovendien speelt de lokale beschikbaarheid van netwerken een rol. signetbreedband snapt dit als geen ander en adviseren je over de meest slimme, kostenefficiënte en duurzame oplossing voor jouw bedrijf.

**Eurofiber:**

- Glasvezelnetwerk in eigendom.
- Volledig ondergronds netwerk op minimaal 60 centimeter diepte.
- Continue monitoring op het netwerk om vroegtijdige degradatie (verzwakkingen) op te sporen.
- Voert preventief onderhoud aan zowel netwerk als apparatuur in datacenters.

**signetbreedband:**

- Samenwerking met meer dan 50 verschillende netwerkpartners.
- Sinds 1996 dé specialist op het gebied van connectiviteit.
- Volledige connectiviteitsoplossingen onder één dak.
- Advies op maat en persoonlijke service.

Heb je naar aanleiding van dit whitepaper vragen? Of wil je meer informatie? Neem contact met ons op. We helpen je graag verder!


signet breedband

**Locatie Eindhoven**
Achtseweg Zuid 153W
5651 GW Eindhoven

088 599 99 99
info@signetbreedband.nl
www.signetbreedband.nl

**locatie Arnhem**
Amsterdamseweg 54
6814 CP Arnhem

eurofiber

**Eurofiber**
Safariweg 25-31
3605 MA Maarssen
030 242 8993
info@eurofiber.com
www.eurofiber.com