eurofiber

E-BOOK:
CHECK DE MOGELIJKHEDEN DIE DE CLOUD BIEDT

Een **snelle, veilige, betrouwbare infrastructuur** voor de **zorg?**

LIFELINE

Hoe speel je in de zorg in op de razendsnel veranderende klantvraag?

Organisaties in de Zorg hebben een groeiende behoefte aan connectiviteit voor allerlei nieuwe toepassingen, zoals beeldschermzorg, robots aan het bed en Internet of Things oplossingen om slimme Zorg te leveren. Betrouwbare connectiviteit is cruciaal.

De technologische revolutie waar we ons momenteel in bevinden, zorgt voor een razendsnel veranderende klantvraag. Klanten stellen steeds hogere eisen en verwachten dat u gebruik maakt van de nieuwste technologische mogelijkheden. En die mogelijkheden ontwikkelen zich ook nog eens in razend tempo: de nieuwe, flexibele generatie markttoetreders zet namelijk continu nieuwe diensten als service concept in de markt.

Voor uw organisatie is het van groot belang snel te reageren op al deze veranderingen. Maar hoe doet u dit? Hoe maakt u uw organisatie flexibel en wendbaar?

De cloud maakt het gemakkelijker, laagdrempeliger en goedkoper om met uw organisatie te versnellen en te experimenteren. In dit ebook nemen we u mee in deze nieuwe wereld.

Wat is de cloud precies, wat zijn de voordelen voor uw organisatie en waarom is beveiliging nog belangrijker dan in ons traditionele IT-landschap? Ontdek de mogelijk heden van de cloud en hoe u veilig en direct toegang krijgt tot meerdere cloud platformen.

Eurofiber Nederland

1

De opmars van de cloud
- Wat is de cloud eigenlijk?
- De voordelen voor uw organisatie
- Besparing op IT-kosten.

2

Overstappen naar de cloud
- De 3 gebruikersmodellen: publieke, private en hybride cloud
- De servicemodellen van de cloud Software as a Service SaaS Platform as a Service PaaS Infrastructure as a Service IaaS

3

Aandachtspunten bij cloud migratie
- Zorg voor een volledige inventarisatie
- Verbindingen met de cloud
- Exit-strategie

4

Veilige connectie
- Via het publieke netwerk
- Via een privé-netwerk
- Wat is Ethernet VPN?

5

Securitybeleid
- De financiële gevolgen van een cyberaanval
- Security in de cloud
- Verbindingen onderbelicht aspect van cybersecurity
- Netwerk monitoring

6

Secure Cloud Connect van Eurofiber
- Efficiënte totaaloplossing
- Op maat voor uw organisatie
- Optimale beschikbaarheid en support

1. De opmars van de cloud

De meeste organisaties in Nederland maken in meer of mindere mate gebruik van de cloud. Volgens onderzoek van onderzoeksbureau Giarte naar de cloud, blijkt dat inmiddels 86% van organisaties ervaring heeft met de cloud. Er zijn echter vele soorten cloud toepassingen.

Wat is de cloud eigenlijk?

De cloud staat voor een netwerk dat met al de computers die erop aangesloten zijn een 'wolk van computers' vormt. Hierop draait dan een veelheid aan applicaties. Gebruikers zijn op deze manier geen eigenaar meer van software en hebben ook geen zorgen over het onderhoud. De gebruiker beschikt over een 'eigen' virtuele infrastructuur, schaalbaar in omvang en mogelijkheden, waarmee hij online gebruik kan maken van applicaties, software en data die worden aangeboden vanuit datacenters.

De voordelen voor uw organisatie

Nederlandse organisaties en IT-managers verwachten dus veel van de cloud. Terecht? Zeker! De cloud biedt zeer veel flexibiliteit en schaalbaarheid. Het op-en afschalen van bijvoorbeeld gebruikers van een applicatie is vaak letterlijk een kwestie van een paar muisklikken. Hierdoor is uw IT bij dal-en piekmomenten een prettig hulpmiddel in plaats van een financieel en operationeel obstakel.

Hetzelfde geldt voor het in gebruik nemen van nieuwe applicaties of diensten, deze zijn on demand beschikbaar. Wat de snelheid en wendbaarheid van uw organisatie ten goede komt bij bijvoorbeeld de ontwikkeling van een nieuw product of dienst. En uiteindelijk stelt de cloud een organisatie in staat om snel te groeien: de extra ITcapaciteit is direct beschikbaar als het nodig is. Zonder investeringen in bijvoorbeeld het bijplaatsen van extra servers en lange doorlooptijden.

Besparing op IT-kosten

Ongemerkt wordt veel tijd en geld besteed aan beheer en onderhoud van de eigen IT-omgeving. Bij de cloud doet de cloud provider de kapitaal en arbeidsintensieve investeringen: van de aanschaf van netwerkservers en applicaties tot aan het nemen van securitymaatregelen. Ook bijkomende zaken als het onderhouden van een team hooggekwalificeerde IT'ers komt op het bord van de cloud provider.

Neemt u een cloud dienst af, dan betaalt u alleen voor wat uw organisatie en uw medewerkers gebruiken. Er zijn verschillende soorten afrekenmodellen: per maand, per gebruiker of per afgenomen resources. Dit levert een besparing op uw IT-kosten op. Om het in financiële termen uit te drukken: CAPEX (Capital Expenditure, investeringen) wordt OPEX (Operational Expenditure, lopende uitgaven).

Natuurlijk moet u ook bij de cloud uw uitgaven scherp in de gaten houden. Controleer periodiek welke cloud diensten uw gebruikersgroepen afnemen.

2. Overstappen naar de cloud

De behoefte aan het snel inspelen op veranderingen en het terugdringen van kosten zijn belangrijke argumenten om over te stappen naar de cloud. U moet een aantal keuzes maken om tot een optimale cloud omgeving te komen. Maakt u hierbij gebruik van de publieke, private of hybride cloud?

De 3 gebruikersmodellen:

Publieke, private en hybride cloud. Vanwege de verschillende eisen van organisaties, zijn er ook verschillende gebruikersmodellen: publieke, private en hybride cloud. Kies de cloud die het best voldoet aan uw eisen.

Publieke cloud

De naam zegt het al: de publieke cloud is voor iedereen toegankelijk. Deze cloud bestaat uit een gevirtualiseerde IT- omgeving waarbij verschillende organisaties elk een eigen IT-omgeving, inclusief besturingssysteem, gebruiken. De cloud provider werkt met een aantal standaardconfiguraties voor netwerkservers, cybersecurity, applicaties en gegevensopslag. Het beheer en onderhoud van de IT is voor rekening van de cloud provider.

Voordelen

- Relatief lage investering
  Door de standaardconfiguraties kan de cloud provider een behoorlijk aantal klanten bedienen. Wat zorgt voor een relatief lage prijsstelling.
- Snel doorvoeren van nieuwe ontwikkelingen
  De publieke platformen hebben de capaciteit om nieuwe ontwikkelingen snel te implementeren, zodat u direct profiteert van nieuwe mogelijkheden.
- Schaalbaarheid
  Voor tijdelijke projecten kunt u snel extra opslagruimte of rekenkracht inzetten.
- Veel expertise over informatiebeveiliging
  Cloud providers hebben vaak een hoge volwassenheid op het gebied van informatie-beveiliging. Denk aan maatregelen op het vlak van fysieke beveiliging, toegangscontrole, gegevensopslag en continue training van gespecialiseerd personeel.

Nadelen

- Beperkte mogelijkheden voor maatwerk
  Er is een groot aanbod aan applicaties en diensten beschikbaar. Maar deze moeten maar net helemaal aansluiten bij de specifieke IT-behoeften van uw organisatie.
- Privacy overwegingen
  Bij de publieke cloud is het niet inzichtelijk op welke systemen en in welke landen de gegevens zich bevinden. Soms eist de overheid van organisaties dat zij bepaalde gegevens altijd in eigen beheer houden.

Alle voor- en nadelen op een rijtje

Private cloud

Wanneer we de gevirtualiseerde IT-omgeving uitsluitend voor het eigen bedrijf gebruiken, dan spreken we over een private cloud. Bij private cloud staan de applicaties en diensten bij de cloud provider in een beheerd datacenter of in het eigen datacenter. Net als bij de publieke cloud. Echter een private cloud is een volledig afschermde IT-omgeving met eigen servers voor applicaties en gegevensopslag.

Uw eigen IT-afdeling zorgt voor het beheer en onderhoud (of desgewenst een speciaal team van de cloud provider).

Voordelen

- Op maat gemaakt
  De applicaties en diensten zijn afgestemd op de behoeften van uw organisatie.
- Privacy overweging
  U weet altijd exact waar uw data is opgeslagen. Voor bijvoorbeeld financiële instellingen is dat van cruciaal belang: de wet-en regelgeving eist dat zij precies weten waar de (klant)gegevens staan én hoe de beveiliging is geregeld.

Nadelen

- Hogere investeringen
  Door het maatwerk dat bij een private cloud komt kijken, is deze oplossing mogelijk duurder dan de publieke cloud. Denk aan extra investeringen voor hardware, fysieke beveiliging en continuïteit. Ook moet er rekening gehouden worden met hogere kosten voor het opschalen van extra capaciteit.

Hybride cloud

De hybride cloud is een combinatie van de publieke en private cloud. De hybride cloud biedt u kortgezegd 'best of both worlds'. Zo gebruikt u het standaardaanbod van de publieke cloud, zoals Microsoft Azure, Amazon Web Services of Google Cloud Platform.

Daarnaast maakt u gebruik van maatwerkoplossingen om aan privacywetgeving te voldoen of om eigen sector, of bedrijfsspecifieke software te blijven toepassen. Deze handige combinatie zorgt ervoor dat de hybride cloud steeds populairder wordt.

Voordelen

- Financieel aantrekkelijke standaard configuraties met de snelheid en flexibiliteit van de publieke cloud.
- Maatwerkoplossingen voor specifieke applicaties en systemen zoals in de private cloud.

Nadelen

- Hogere investeringen dan voor de publieke cloud.
- Complexiteit van het combineren van de publieke en private cloud.

Welke cloudvorm past bij uw organisatie?

De servicemodellen van de cloud
Wanneer u heeft besloten welke vorm van de cloud het best past bij uw organisatie, maakt u ook de keuze in hoeverre u het beheer van de IT-omgeving uit handen geeft. Aan de basis van de cloud staat 'Everything as a Service', ook wel XaaS. Hieronder vallen een aantal servicemodellen:

Software as a Service SaaS
Misschien wel de meest bekende 'as a Service' variant is software (SaaS).
In plaats van het eenmalig aankopen van software betaalt u de software naar gebruik. De meeste SaaS oplossingen worden direct online gebruikt zonder dat er een download of installatie nodig is. Ook heeft SaaS als voordeel dat de leverancier het beheer en opslag van de applicatie verzorgt.
Tegenwoordig is er een breed scala aan applicaties via het internet te gebruiken: van kantoorsoftware (Microsoft Office 365, Salesforce.com) tot boekhoudpakketten (AFAS Software, Exact), HRsoftware (WorkDay) en ERP-applicaties (SAP, Oracle).

Platform as a Service PaaS
Wanneer organisaties een platform online afnemen waarop ze maatwerk applicaties kunnen ontwikkelen, dan spreken we over Platform as a Service (PaaS). Een PaaS-platform bestaat uit gedeelde hardware voor server en gegevensopslag inclusief de benodigde virtualisatie-software en besturingssystemen. Het onderhoud en beheer zijn voor rekening van de cloud provider. In tegenstelling tot SaaS dient u bij PaaS meer beheer-derstaken zelf uit te voeren. Dit vergt meer kennis en ervaring. De meest bekende PaaS aanbieders zijn Amazon (EC2), Microsoft (Azure), Oracle en Google (App Engine).

Infrastructure as a Service IaaS
Een IaaS oplossing biedt uw organisatie een virtuele hosting omgeving met controle over onder andere gegevensopslag, netwerk apparatuur en besturingssysteem. U betaalt alleen voor wat u daadwerkelijk gebruikt. Groot voordeel is dat de extra capaciteit vrijwel onmiddellijk beschikbaar is en u niet zelf hoeft te investeren in hardware en de locatie van een server. Bekende IaaS partijen zijn Amazon (AWS), Microsoft (Azure), Google Cloud Platform en Oracle (NetApp).

Wat, waar onder-brengen?

Als u de stap naar de cloud gaat maken of uw cloud omgeving gaat uitbreiden brengt dit een aantal uitdagingen met zich mee. Welke applicaties, data en platformen gaat u waar onderbrengen?

3. Aandachtspunten bij cloud migratie

Nu u een beter beeld heeft van de cloud is het tijd om de eigen IT-omgeving goed te inventariseren. Migreren naar de cloud is een complex proces. U heeft immers te maken met verschillende applicaties en systemen die overgezet moeten worden.

"Betrek diverse zorg collega's bij een inventarisatie"

Denk daarom van te voren goed na hoe u dit proces gaat inrichten. Welke applicaties gaan in de cloud? En gaat u meerdere clouds gebruiken? Dan krijgt u wellicht te maken met uiteenlopende leveranciers van SaaS, PaaS en IaaS. Gaat uw afdeling deze partijen vervolgens zelf aansturen of besteedt u dit liever uit?

Zorg voor een volledige inventarisatie

Bij de migratie naar de cloud start u met de inventarisatie van uw huidige IT- omgeving. Maar let op: een goede inventarisatie gaat verder dan een lijst maken van applicaties en systemen. Uw medewerkers en de verschillende afdelingen gebruiken meer IT- oplossingen dan de IT- afdeling vaak beseft. Denk bijvoorbeeld aan cloud diensten die ze privé al gebruiken, zoals Dropbox of Google Drive. Neem maatregelen om de wildgroei aan deze schaduwIT tegen te gaan. Dit doet u bijvoorbeeld door duidelijk te communiceren welke voorkeursleveranciers er zijn. Betrek uw medewerkers en afdelingen ook bij de inventarisatie om inzicht te krijgen in de verschillende verwachtingen en belangen die meespelen. Zo komt u er achter waarom uw gebruikers geen gebruik maken van de door de organisatie aangeboden IT-oplossingen.

Misschien is het zelfs tijd voor andere leveranciers?

- Hoeveel vestigingen en werkplekken heeft u momenteel?
- Welke soft-en hardware gebruiken de medewerkers en afdelingen van uw organisatie?
- Is er overlap tussen verschillende applicaties en systemen?
- Kan de software ook vanuit de cloud worden afgenomen?
- Moet een aantal applicaties (maatwerksoftware of verouderde bedrijfskritische pakketten) toch op een eigen server blijven draaien?
- Of zijn er goede alternatieven in de cloud voorhanden?
- Wie verzorgt het beheer van uw IT-omgeving?
- Heeft uw IT afdeling voldoende kennis om te migreren?
- Hoe wilt u de regie gaan voeren over de keten?
- Wat is uw beleid op het gebied van privacy & security?

Verbindingen met de cloud
Als u een inventarisatie maakt, is het ook tijd om kritisch te kijken naar de huidige infrastructuur. Betrouwbare verbindingen zijn een cruciaal onderdeel van de cloud. Neem daarom ook uw internet en netwerkverbindingen onder de loep. Voldoen die straks in de praktijk als het gaat om bandbreedte?

Exit-strategie
Het laatste aandachtspunt is die van een succesvolle exitmogelijkheid. Wie van de ene naar de andere cloud provider over wil stappen, zal dat van te voren goed moeten regelen. Bijvoorbeeld door in het contract met de cloud provider op te nemen dat de bedrijfsdata gemakkelijk en snel naar een nieuwe partij zijn over te hevelen. Zónder dat daar extra kosten bij komen kijken.

Denk aan:
- Hoeveel aparte internet en netwerkverbindingen zijn er?
- Kunt u altijd bij uw gegevens?
- Is er rekening gehouden met redundantie?
- Geeft de netwerkleverancier ook de nodige garanties op de continuïteit van zijn dienstverlening?
- Is de netwerkleverancier in het bezit van certificeringen die de kwaliteit garanderen?
- Wat zijn de adviezen van de cloud providers op het gebied van verbindingen qua bandbreedte en kwaliteitseisen?
- Hoe gaat u de connectiviteit naar deze platformen of applicaties organiseren?
- Hoe belangrijk zijn deze voor de continuïteit van uw organisatie?
- Hoe waarborgt u de security van uw ITomgeving?

4. Veilige connectie

Een betrouwbare en veilige netwerkverbinding is van cruciaal belang voor toegang tot uw cloud omgeving. U kunt op twee manieren verbinding maken met de cloud: via het publieke internet of via een privé netwerk. In dit laatste geval maakt u gebruik van de diensten van een netwerk-leverancier. In dit hoofdstuk lichten we de voor- en nadelen van deze verbindingen toe, zodat u een juiste keuze kunt maken voor een verbinding.

"Kies je in de zorg voor een publiek- of privé netwerk"

Via het publieke netwerk

Het publieke internet lijkt de eenvoudigste manier voor organisaties om met de cloud te verbinden. Helaas kleven er behoorlijk wat nadelen aan deze oplossing:

- Er is geen controle over de verschillende 'tussenstations' waar de bedrijfsdata en –applicaties overheen gestuurd worden. Een echte Quality of Service (QoS) op de verbinding is bij het publieke internet niet af te geven.
- De schaalbaarheid is beperkt. Snel opschalen bij pieken in het gebruik van cloud applicaties is er niet bij. U heeft dus een redelijke bandbreedte nodig om benodigde extra capaciteit op te kunnen vangen.
- De beveiliging is niet waterdicht. Als u een beveiligde cloud verbinding wilt realiseren zult u extra moeten investeren in een beter beveiligde verbinding.
- Aansluitend zult u het netwerk nog moeten verbinden met een cloud provider naar keuze.

Via een privé netwerk

Als u kiest voor een privé netwerk voor toegang tot de cloud, verloopt uw dataverkeer via een privé verbinding over een gesloten netwerk. De verbinding met de cloud wordt in feite onderdeel van uw bedrijfsnetwerk. Er zijn hierin twee mogelijke manieren van aanpak. U kunt een privé netwerk volledig zelf inrichten of gebruik maken van een netwerkleverancier. In beide gevallen heeft u hoogwaardige breedband verbindingen nodig.

Wanneer u het zelf inregelt, is er uitgebreide expertise en specialistische kennis nodig. Er moeten verbindingen worden gerealiseerd, rackruimte gehuurd en ingericht worden in datacenters waar de verschillende cloud platformen draaien. Ook is er kennis nodig over de verschillende netwerklagen, BGP protocollen en IP routering om met de cloud platformen te koppelen. Waarna u de cloud omgeving kunt gaan bouwen en inrichten.

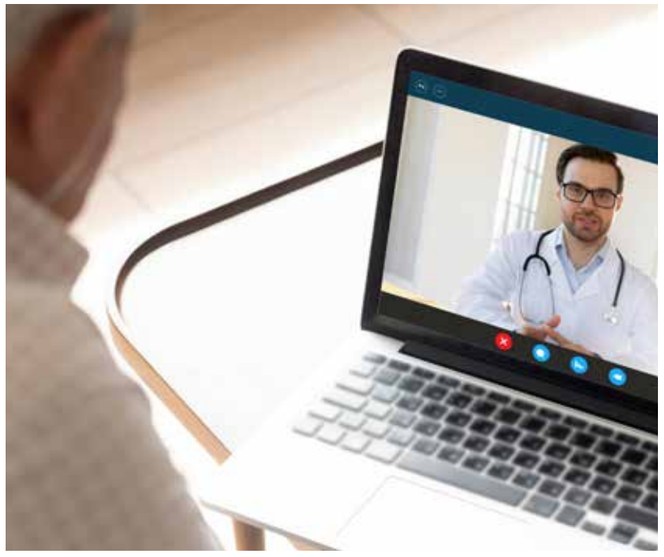
Het alternatief is dat u gebruik maakt van de diensten van een netwerkleverancier voor een IaaS connectiviteits oplossing. Deze levert u privé verbindingen met de datacenters van de diverse cloud providers over hun vooraf ingerichte infrastructuur, dit biedt u een aantal voordelen:

- Goede toegangsbeveiliging tot uw applicaties en data in de cloud. Namelijk het netwerk wordt opgezet op basis van private Ethernet of IP VPNverbindingen en is volledig gescheiden van het publieke internet. (lees meer over VPN in het kader op deze pagina)
- Een één op één relatie met de netwerk-leverancier, met een Service Level Agreement (SLA) specifiek voor de afgesloten dienstverlening.
- Sommige netwerkleveranciers bieden een end-to-end koppeling via hun netwerk met aangesloten cloud providers, geheel ingeregeld op een cloud exchange of directe koppelingen met de diverse cloud providers. Deze complete oplossing biedt daarbij redundantie naar de cloud, zeer hoge beschikbaarheid en niet onbelangrijk, een dienst tegen relatief lage kosten. Het enige waar u zorg voor moet dragen is de inrichting van uw cloud omgeving. Deze oplossingen passen volledig in het cloud model van ontzorgen, schaalbaarheid en flexibiliteit. En u hoeft zelf niet de special-istische netwerk kennis in huis te hebben om direct met cloud providers te koppelen of een datacenter infrastructuur in te richten.

Wat is VPN?
VPN staat voor Virtual Private Network: een virtueel datanetwerk tussen locaties, dat gescheiden is van het publieke internet. Met VPN-verbindingen creëert u een gesloten organisatienetwerk tussen uw hoofdkantoor, vestigingen en datacenters. Het netwerk is eenvoudig uit te breiden en stimuleert efficiënt werken.

De voordelen van een VPN
- U kunt meerdere diensten over uw VPN-verbinding transporteren, zoals internet, telefonie en video. Door ook uw datacenters via het netwerk te ontsluiten, is het mogelijk om applicaties en platformen centraal aan te bieden.
- Voor uw organisatienetwerk kunt u per verbinding de behoefte aan bandbreedte bepalen. Zo bent u flexibel tijdens piekmomenten.
- U kunt uw hoofdkantoor, vestigingen en in-of externe datacenters via enkelvoudige of redundante verbindingen aan elkaar koppelen. Het belang van de locatie bepaalt wat voor verbinding u nodig heeft.

"Toekomst-bestendige oplossingen"



5. Securitybeleid

De cloud en de verbindingen ernaartoe vragen om een modern en toekomstbestendig securitybeleid. Een beleid dat alle nieuwe verbindingen en opslagmogelijkheden zo goed mogelijk beschermt tegen cybercriminelen. De gevolgen van een cyberaanval kunnen een ramp zijn voor uw organisatie. Hoe zorgt u ervoor dat u uw organisatie zo veilig mogelijk inricht?

"Juist voor de zorg geldt: veiligheid voor alles"

De financiële gevolgen van een cyberaanval

Op het moment dat een cybercrimineel uw organisatie binnendringt, heeft dit grote gevolgen. Cybersecurity specialist Kaspersky heeft onderzocht dat de kosten na een cyberaanval bij bedrijven uiteenlopen van 120.000 dollar tot wel 1.23 miljoen dollar*.

Een deel van die kosten zijn direct gerelateerd aan de naweeën van de cyberaanval, zoals het dichten van het lek en het inhuren van security-experts. De grootste kosten ontstaan echter door omzetverlies en reputatieschade. Uw organisatie wordt in een negatief daglicht gesteld.

En dat is nog niet alles. Mogelijk ontvangt u claims van derden. En daarnaast kunt u ook nog een flinke boete opgelegd krijgen door de overheid. In de Europese Unie verplicht de Algemene Verordening Gegevensbescherming een datalek binnen 72 uur te melden. Doet u dit niet, of doet u dit te laat, dan kan de boete oplopen tot 20 miljoen euro, dan wel 4 procent van de wereldwijde jaaromzet van de onderneming**.

Wat de kosten voor uw organisatie zullen zijn, is natuurlijk erg afhankelijk van het soort en de omvang van uw organisatie en ook de vorm van de cyberaanval. Wij adviseren u dan ook om u vooraf te laten adviseren door een security specialist.

Security in de cloud

Als u een cloud dienst afneemt, liggen veel cybersecuritymaatregelen op het bord van de cloud provider. Zij nemen security zeer serieus en investeren er flink in. Die investeringen variëren van fysieke beveiliging, toegangscontrole, gegevensopslag tot en met continue training van gespecialiseerd personeel.

Daarmee gaan veel cloud providers verder dan een organisatie zelf zou kunnen. Natuurlijk moet u zelf ook maatregelen nemen om de kans op een cyberaanval te verkleinen. Zoals het inrichten van een Cyber Threat Management platform of het afnemen van een Security Operations Service. Zorg ook voor een passend antivirussysteem op al uw apparaten en laat updates regelmatig uitvoeren. En, misschien wel het belangrijkst: zorg ervoor dat uw medewerkers weten hoe zij veilig werken.

Leer ze wat wel en niet mag als het gaat om de toegang tot applicaties en data en leer hen hoe ze sterke wachtwoorden instellen. Organiseer bijvoorbeeld met regelmaat awareness sessies waarin ze leren omgaan met de risico's van cybercriminaliteit.

Verbindingen onderbelicht aspect van cybersecurity
De verbinding met de cloud is een onderbelicht element bij de beveiliging. Toch is het een essentiële schakel: alle applicaties en data lopen immers via de verbinding met de cloud provider. Dé ingang voor cybercriminelen om toe te slaan.

Houdt uw verbindingen daarom continu in de gaten door middel van monitoring. Zo kunt u verstoringen in het netwerk direct detecteren. Bij Ethernet en IP VPN-verbindingen is deze monitoring tweeledig: de leverancier heeft zicht op zijn eigen netwerk en u als klant heeft overzicht over het gehele stuk, inclusief uw eigen netwerk en de apparatuur die zich daarin bevindt. Als er storingen optreden, kan eenvoudig worden nagegaan of het een storing betreft naar aanleiding van (geplande) werkzaamheden of dat er iets anders aan de hand is. Bij alle netwerkapparatuur worden monitoringtools geleverd waarin onder meer latency, retransmissies en bit errors worden gemeten.

Beheer uw netwerkcomponenten en –poorten actief, zodat u bij latency veranderingen en onderbrekingen van het signaal direct alarmbellen ziet afgaan. Dit zijn indicaties dat er mogelijk ongewenste apparatuur in het netwerk is geplaatst. De grote aanbieders van de cloud hebben inmiddels oplossingen ontwikkeld voor directe en beveiligde toegang via een netwerkverbinding.

*Bron Kaspersky: https://usa.kaspersky.com
**Bron: https://autoriteitpersoonsgegevens.nl

"Cybersecurity in de zorg is vaak nog onderbelicht"

Om te kunnen voldoen aan de AVG is encryptie onontbeerlijk. Encryptie versleutelt data, zodat als het onverhoopt verloren of gestolen wordt, kwaadwillenden er niets aan hebben. Ze kunnen de data dan immers niet ontcijferen. Afhankelijk van de toepassing, kunt u op verschillende netwerklagen encryptie toepassen en dataverkeer versleutelen.

6. Secure Cloud Connect van Eurofiber

Om als organisatie wendbaar en flexibel te zijn, gaat u steeds meer vanuit de cloud werken. Met Secure Cloud Connect heeft u altijd veilig en direct toegang tot meerdere cloud platformen. Met deze complete end-to-end oplossing krijgt u direct toegang tot de platformen van uw keuze via een veilig privé-netwerk.

Efficiënte totaaloplossing

We verbinden uw organisatie via een virtueel privénetwerk (VPN) met uw cloud providers, waarbij het netwerk volledig van het publieke internet is gescheiden.

Daarnaast krijgt u direct toegang tot het platform van uw keuze door middel van onze cloud koppelingen. Eurofiber levert een end-to-end dienstverlening vanaf uw kantoorlocatie en/ of data-center locatie, naar publieke cloud service providers zoals: Microsoft Azure, Microsoft Office 365, Amazon Web Services (AWS) en Google Cloud Platform.

Andere cloud platformen zijn beschikbaar op verzoek. Met Secure Cloud Connect beheert u alleen uw applicaties in de cloud, de rest regelen wij voor u.

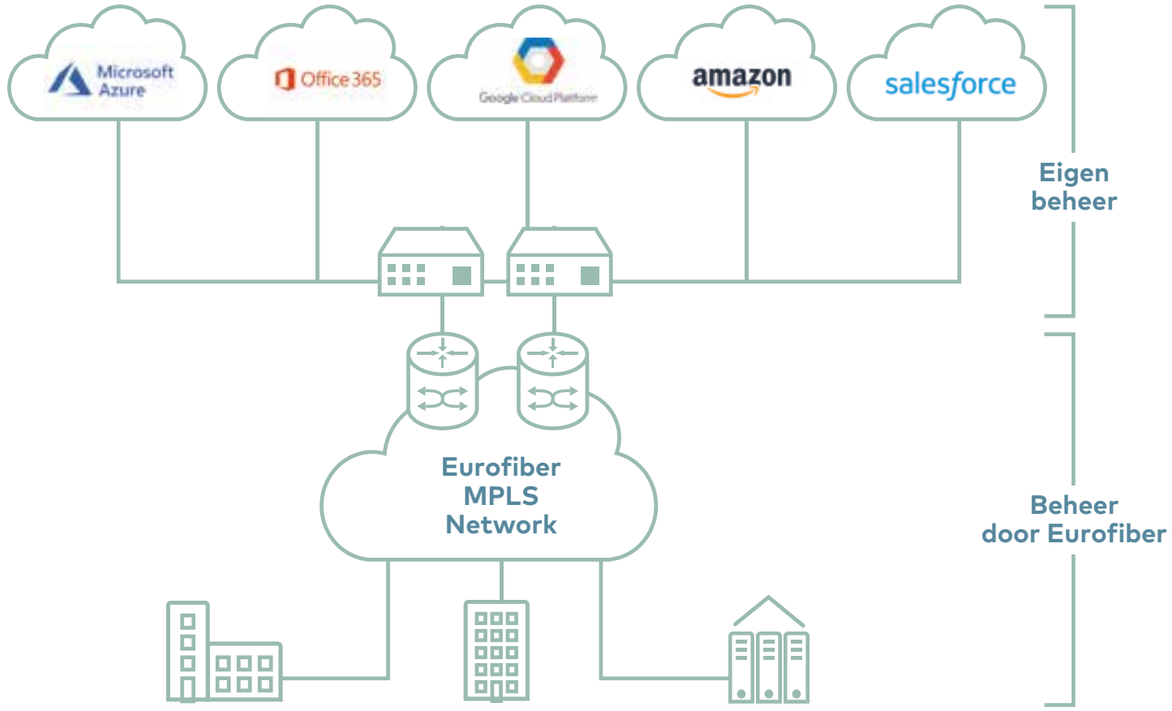
Op maat voor uw organisatie

We bieden u altijd een complete oplossing die optimaal aansluit op de situatie van uw organisatie. Wij adviseren u graag over het inrichten van uw netwerk: Internet, VPN-netwerk tussen uw hoofd- en nevenkantoren, datacenters en integratie van cloud service providers.

U kunt uw netwerk flexibel inrichten per locatie naar bandbreedte, service level en enkele- of redundante uitvoering. Secure Cloud Connect ondersteunt alle band-breedtes van de diverse cloud service providers van 50 Mb/s tot 10 Gb/s, zowel single als redundante aansluitingen.

Optimale beschikbaarheid en support

Om uw organisatie betrouwbaar toegang te bieden tot uw cloud providers, leveren we Secure Cloud Connect altijd over de glasvezel infrastructuur van Eurofiber en het Eurofiber private laag-2 netwerk. Daarnaast kunt u rekenen op 24 x 7 ondersteuning door ons Network Monitoring Center (NMC).



Het glasvezelnetwerk van Eurofiber Nederland

Eurofiber Nederland levert high end-connectiviteits-diensten op basis van glasvezel voor de zakelijke markt. Eurofiber loopt voorop in het implementeren van nieuwe technologie en het continu verhogen van de kwaliteit van het glasvezelnetwerk.

Eurofiber Nederland

Eurofiber exploiteert sinds 2000 hoogwaardige digitale open infrastructuur. Met ons eigen glasvezelnetwerk en datacenters bieden we bedrijven, overheden en non-profit organisaties een toekomstvaste, slimme en open infrastructuur. Klanten hebben de vrijheid om zelf de diensten, toepassingen en aanbieders te kiezen die ze nodig hebben. Zo kunnen ze het innovatiepotentieel in de digitalisering ten volle te benutten.

Naast het uitgebreide glasvezelnetwerk in Nederland en België en eigen datacenters in Nederland bieden we ook oplossingen voor interconnectiviteit tussen bijna alle hoogwaardige carrier neutrale datacenters in de Benelux. Eurofiber legt hiermee het fundament onder de digitale samenleving. De Nederlandse overheid heeft Eurofiber dan ook de status toegekend van 'vitale infrastructuur'.

Flexibel en schaalbaar

Ons open netwerk geeft uw organisatie volledige vrijheid en flexibiliteit. U heeft de vrijheid om zelf de diensten, toepassingen en aanbieders te kiezen die u nodig heeft. Tevens biedt Eurofiber managed diensten op basis van het glasvezelnetwerk zoals WDM, Ethernet en Internet.

Veilig ondergronds netwerk

Het netwerk van Eurofiber ligt ondergronds op een diepte van 60 centimeter. Het werk aan ons netwerk gebeurt via gecertificeerde processen, die we continu controleren en jaarlijks toetsen.

We werken met gecertificeerde medewerkers en aannemers. Op het netwerk is een Remote Fiber Test Systeem (RFTS) geïnstalleerd dat continu de beschikbaarheid van de infrastructuur bewaakt. Bij een onverhoopte kabelschade door bijvoorbeeld graafwerkzaamheden kan het RFTS dan exact meten waar de breuk zich bevindt. Om verstoringen voor onze klanten te voorkomen, wordt regelmatig preventief onderhoud verricht om de netwerkkwaliteit te garanderen.

Veel ervaring in de zorg

Hoge beschikbaarheid

De beschikbaarheid van het glasvezelnetwerk van Eurofiber is minimaal 99,9%. Als u kiest voor een volledig gescheiden tweede glasvezelroute (redundantie), bedraagt deze beschikbaarheid minimaal 99,98%. Als u twee gescheiden glasvezelverbindingen heeft, garanderen wij dat wij nooit aan beide verbindingen tegelijkertijd werkzaamheden uitvoeren. Uiteraard informeren wij u als klant, wanneer er werkzaamheden aan het netwerk zijn gepland.

LIFELINE

Netwerk Monitoring Center

U kunt rekenen op de 24/7 ondersteuning van de experts op het Eurofiber Network Monitoring Center. Het Netwerk Monitoring Center is gevestigd in Nederland en wordt bemand door Nederlands en Engels sprekende experts.

Gegarandeerde reparatietijd

Het geografisch vastgelegde Eurofiber glasvezelnetwerk gecombineerd met de actieve bewaking van het Netwerk Monitoring Center zorgt ervoor dat de gegarandeerde reparatietijd op glasvezelverbindingen maximaal 8 uur is. Bij actieve diensten bedraagt deze maximaal 4 uur.

Beschikbaar in 92% van de datacenters van Nederland

Het Eurofiber glasvezelnetwerk is beschikbaar in een groot aantal datacenters in Nederland. Met de additionele Datacenter Services van ons zusterbedrijf Dataplace met moderne Tier3-datacenters in de regio's Amsterdam, Rotterdam, Utrecht, Arnhem en Brabant ondersteunen wij u met hoogwaardige colocatie oplossingen voor veilige huisvesting voor uw bedrijf kritische informatie en systemen.

Garanties

Eurofiber levert connectiviteit op basis van een Service Level Agreement. Hierin is exact vastgelegd welke prestaties, kwaliteitsniveau en garanties u van ons kunt verwachten. Duidelijke afspraken dus, zodat u altijd weet waar u aan toe bent.

Voor meer informatie kunt u contact met ons opnemen:
Safariweg 25-31, 3605 MA Maarssen
+31 (0)30 242 89 93, info@eurofiber.nl
www.eurofiber.nl

Eurofiber. Lifeline for the digital society

eurofiber