De succesformule voor een veilige ICT-infrastructuur

Alles wat een ICT-manager zou moeten weten

eurofiber

De succesformule voor een veilige ICT-infrastructuur

Tegenwoordig verbinden we meer en meer apparaten met elkaar via het internet. Zowel in ons privéleven als in het bedrijfsleven creëren we netwerken die, zonder menselijke tussenkomst, met elkaar communiceren. Denk bijvoorbeeld aan de opkomst van zelfrijdende auto's en koelkasten die automatisch de boodschappen voor u bestellen doordat ze met het internet verbonden zijn.

Ook in het bedrijfsleven wordt het internet voor meer en meer toepassingen gebruikt. Medewerkers werken steeds vaker thuis of onderweg. En via innovatieve applicaties hebben we steeds makkelijker toegang tot alle bedrijfsinformatie via onze smartphones en tablets.

Deze ontwikkelingen voltrekken zich in hoog tempo. Om niet achter te blijven, moeten organisaties hier nu op een goede manier op inspelen. Allereerst om te profiteren van alle voordelen en nieuwe mogelijkheden van het internet en innovatieve applicaties. Maar ook om de nieuw ontstane risico's, die bij deze ontwikkelingen komen kijken, tegen te gaan. Cybercriminelen krijgen steeds meer mogelijkheden om binnen te dringen op een bedrijfsnetwerk. Er zijn immers steeds meer apparaten verbonden met internet en dus kunnen er op steeds meer plekken zwakheden ontstaan in de beveiliging. Deze zwakke plekken moet u zoveel mogelijk verkleinen, of nog beter, voorkomen. Hoe richt u uw ICT-infrastructuur nu op een juiste manier in, zodat uw organisatie zo veilig mogelijk is en zo goed mogelijk beschermd tegen cyberaanvallen?

In dit e-book geven we u de succesformule waarmee u uw infrastructuur veiliger maakt. We gaan in op waarom een nieuwe, passende infrastructuur nodig is, hoe u uw netwerk en data maximaal beveiligt, hoe u uw databeheer veiliger kan maken, de noodzaak van monitoring en de overige niet-technische randvoorwaarden waar u aan moet denken.

Veel leesplezier!

Eurofiber Nederland

Inhoud

De keuze voor de fysieke infrastructuur

In dit e-book gaan we in op de succesformule voor een veilige ICT-infrastructuur. Maar dan moeten we eerst weten waarom een ICT-infrastructuur zo belangrijk is voor uw organisatie.
En welke infrastructuren zijn er eigenlijk? U leest het in dit hoofdstuk.

Een gedegen digitale netwerkinfrastructuur is het fundament van ieder bedrijf. Zeker nu data en toepassingen zich in toenemende mate buiten het bedrijfspand bevinden is connectiviteit van onschatbare waarde. Is een verbinding niet beschikbaar, dan kan dat al gauw een schadepost voor de onderneming betekenen of imagoschade opleveren.

Waar het netwerk voor gebruikt wordt, bepaalt voor een groot deel de keuze in infrastructuur. Heeft u een organisatie waar veel met privacygevoelige gegevens en bedrijfskritische systemen wordt gewerkt? Dan zijn een hoge beschikbaarheid en betrouwbaarheid van cruciaal belang. Twin-datacenters die data synchroon repliceren vragen een andere infrastructuur dan wanneer u alleen behoefte heeft aan internettoegang en IP-telefonie.

Verschillende fysieke infrastructuren uitgelegd

Er bestaat niet één ICT-infrastructuur, de mogelijkheden zijn enorm. Hieronder lichten we een aantal opties toe, zodat u een idee krijgt welke verbinding voor u geschikt zou kunnen zijn.

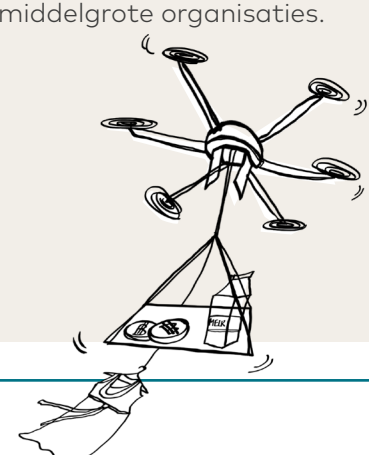
- **Dark fiber** betekent onbelichte glasvezel. Met dark fiber zullen organisaties zelf belichtingsapparatuur plaatsen op hun verbinding. Dit type verbinding wordt vaak gebruikt om enorme hoeveelheden data, tot 100 Gb/s of meer, te transporteren waarbij organisaties zelf bepalen wat de bandbreedte wordt.

- **WDM** staat voor Wavelenght Division Multiplexing. WDM kan worden gebruikt voor alle datacommunicatieprotocollen, zoals Ethernet, Fiber Channel, SDH en niet-gecomprimeerde video. Elke dienst gaat over een eigen lichtpad, wat WDM zeer veilig maakt. De combinatie van WDM-technologie en glasvezel maakt snelheden tot 1,6 Tb/s mogelijk waarmee organisaties voldoende datatransportcapaciteit hebben voor de meest veeleisende toepassingen.

- **Ethernet** technologie wordt al jaren gebruikt om kantoren, medewerkers en datacenters veilig met elkaar te verbinden. Op basis van het ethernet protocol kan een virtueel privénetwerk worden ingericht voor het veilig transporteren van ICT-diensten zoals internet, telefonie en video. In combinatie met glasvezel kunnen er snelheden tot 5 Gb/s worden gerealiseerd.

- **Coax**, ook wel kabel genoemd, wordt vooral gebruikt voor internet, televisie en radio en telefonie in de consumentenmarkt. Het aantal kabelaanbieders per regio is meestal maar één, waardoor organisaties beperkte keuze hebben.

- **DSL** staat voor Digital Subscriber Line. DSL heeft in tegenstelling tot glasvezel niet standaard symmetrische bandbreedtes en kan maximaal snelheden tot 50 Mb/s (VDSL) realiseren. DSL wordt veelal gebruikt door kleine en middelgrote organisaties.



De juiste keuze voor uw organisatie

Met het oog op veiligheid is een Managed Dark Fiber verbinding de beste keuze. Een volledig eigen buis is natuurlijk de meest veilige optie. Een belangrijke voorwaarde is dan wel dat de kennis en expertise in de organisatie aanwezig zijn voor de belichting van de vezel. Is die kennis niet voorhanden, dan is WDM een goede keuze. Een telecomleverancier levert in dat geval naast een onbelichte vezel ook de belichtingsapparatuur, maar in beide gevallen zorgt de netwerkleverancier voor het beheer en het onderhoud.

Twijfelt u tussen WDM en Ethernet? Kijk dan naar de benodigde bandbreedte. Heeft u een hoge bandbreedte nodig, kies dan voor WDM. Heeft u uw ICT-omgeving gecentraliseerd en is er dus een verbinding nodig om gebruikers met de ICT-omgeving te verbinden, dan is een ethernetverbinding noodzakelijk.

Tot slot

Belangrijk is dat privacygevoelige data bij voorkeur niet via het publieke internet worden getransporteerd. Dit omdat het publieke internet hackers vele mogelijkheden biedt om data te onderscheppen. Welke keuze uw organisatie het beste kan maken, is dus afhankelijk van de toepassing van de verbinding.

Maximale beveiliging van netwerk en data

Heeft u uw nieuwe, passende infrastructuur in gebruik, dan is het zaak om te kijken hoe u de veiligheid kan verbeteren. Voor een veilige infrastructuur is encryptie noodzakelijk. Maar niet alleen voor uw infrastructuur heeft u encryptie nodig, ook voor de veiligheid van uw data. In dit hoofdstuk leggen we uit hoe u zowel uw netwerk als uw data goed versleuteld.

Wat is encryptie?

Encryptie versleutelt data, zodat, als het onverhoopt verloren of gestolen wordt, kwaadwillenden er niets aan hebben. Ze kunnen de data immers niet ontcijferen. Encryptie is niet alleen nodig voor het beschermen van uw data, het is ook wettelijk verplicht. De vernieuwde Wet Bescherming Persoonsgegevens bepaalt dat organisaties verplicht zijn hun data optimaal te beschermen. U moet kunnen aantonen dat uw data op het moment van verlies of diefstal was beschermd. Dit kan met behulp van encryptietools.

Encryptie op het netwerk

Encryptie op het netwerk betekent dat alle data die over het netwerk wordt getransporteerd eerst versleuteld wordt. Als een kwaadwillende een zwakke plek in de verbinding ontdekt of ergens de kabel opgraaft, heeft hij niks aan de data zonder de sleutel.

Data-encryptie

Data-encryptie betekent dat de data versleuteld wordt opgeslagen op een harddisk. Mocht een kwaadwillende er met de harddisk vandoor gaan, dan kan hij er niets mee zonder de encryptiesleutel.

Encryptie op het netwerk

Bij encryptie op het netwerk wordt allereerst een encryptiesleutel bedacht, oftewel een codewoord. Een goede encryptiesleutel die regelmatig wisselt en verschillende bICT-lengtes heeft, is cruciaal. Hoe langer de bICT-lengte, des te lastiger te kraken.

Het codewoord wordt toegevoegd aan een algoritme, zoals AES (Advanced Encryption Standard) en het Amerikaanse FIPS (Federal Information Processing Standard). Het algoritme zorgt ervoor dat de data op een bepaalde manier door elkaar gehusseld wordt. Dit wordt zo gedaan dat het bijna onmogelijk is om ontvreemde data te ontcijferen.

Vervolgens wordt de encryptiesleutel uitgewisseld met de apparatuur op de verbinding. Ook wordt er een tijdslimiet bepaald waarop de sleutel veranderd moet worden. Meestal is dit om de minuut. Dus: mocht een

kwaadwillende de sleutel achterhalen, dan is deze na een minuut alweer anders en wordt de data alweer op een andere manier door elkaar gehusseld.

Verschillende encryptiestandaarden voor het netwerk

Advanced Encryption Standard (AES) is de opvolger van de computerversleutelingstechniek **Data Encryption Standard** (DES). Eind jaren negentig bleek DES niet meer te voldoen en werd er een wereldwijde wedstrijd uitgeschreven voor een nieuwe standaard. Het Rijndael-algoritme won, vanwege de combinatie van veiligheid, prestatie, efficiëntie, eenvoudig en flexibiliteit.

RSA (naar de bedenkers Rivest, Shamir en Adleman) is een asymmetrisch encryptiealgoritme dat in 1977 werd ontworpen. De veiligheid van RSA is gebaseerd op het probleem van de ontbinding in factoren (bij heel grote getallen). Het gevaar voor RSA is dat nieuwe ontwikkelingen op dit gebied het algoritme onbruikbaar zouden kunnen maken. De **Federal Information Processing Standard** (FIPS) is een Amerikaanse standaard voor encryptie. Het zijn normen voor de wijze waarop bepaalde informatie in informatiesystemen moet worden vastgelegd. Ze zijn bedoeld voor gebruik door overheidsinstanties en contractpartners van de overheid.

Hardwarematige encryptie versus softwarematige encryptie

Encryptie op het netwerk kan op verschillende manieren. Wat de beste optie is voor uw organisatie, is afhankelijk van de toepassing van de verbinding. Zo kan encryptie hardwarematig worden toegevoegd door encryptors in de belichtingsapparatuur. Hardwarematige encryptie zorgt ervoor dat álle data die over de verbinding plaatsvindt, wordt versleuteld. Wordt er dus veel privacygevoelige en geheime informatie over de verbinding wordt verstuurd, dan is versleuteling op een hardwarematig niveau aan te raden.

Bij hardwarematige encryptie heb je specifieke hardware nodig die de encryptiesleutel verzorgd. Deze vorm van encryptie is zeer veilig. Als een hacker in deze hardware probeert te komen om te kijken hoe de encryptie precies zit, en hij draait er een schroefje uit, dan wordt de sleutel meteen gewist.

Er zijn ook softwarematige versleutelings-mogelijkheden. Een voordeel hiervan is dat het mogelijk is om een selectie te maken tussen data die wel of niet versleuteld wordt. Een nadeel van softwarematige encryptie is dat er

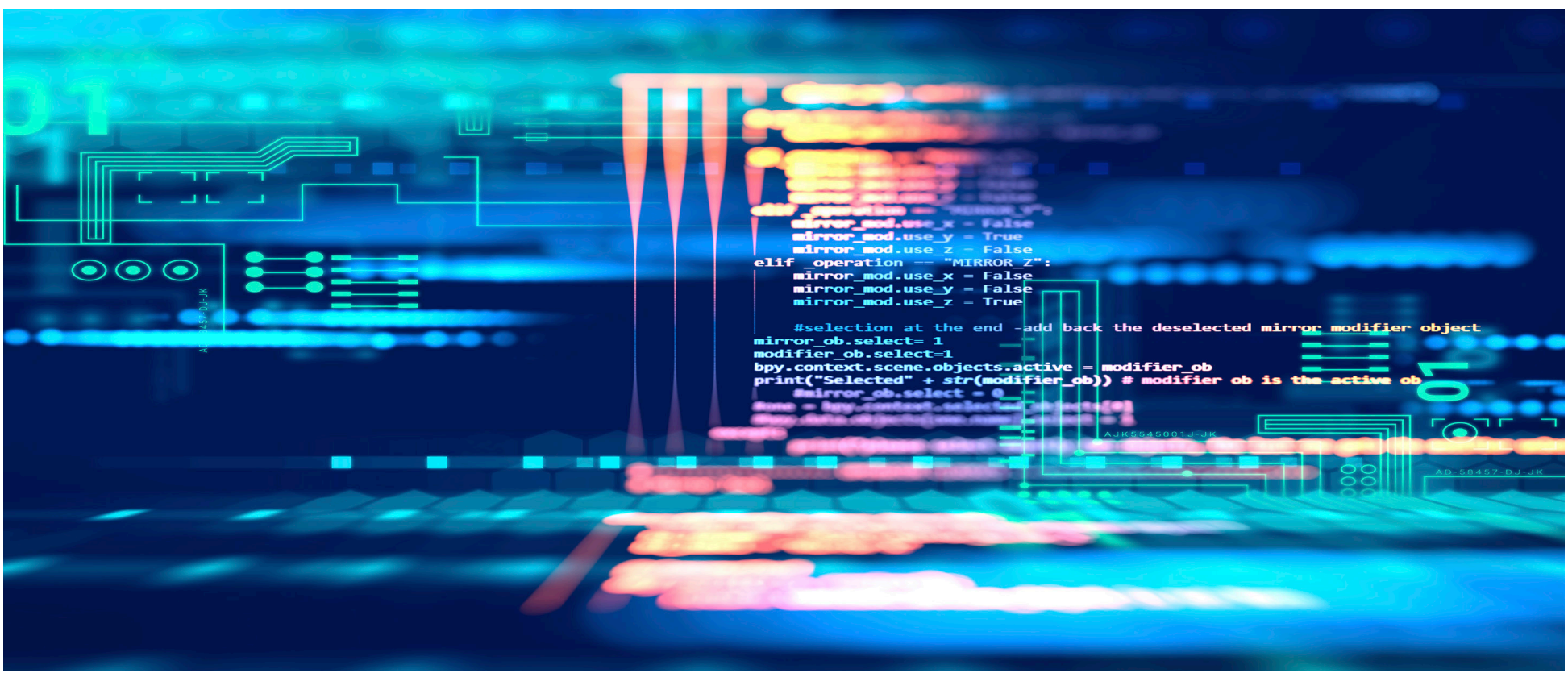
steeds meer latency wordt toegevoegd wat een nadelige invloed kan hebben op de snelheid van de verbinding.

Data-encryptie

Bij versleuteling op netwerk-niveau wordt alleen data beschermd die over de verbinding worden gestuurd. Maar data kan ook versleuteld worden op de interne (en externe) opslagsystemen van de organisatie.

Over het algemeen zit er een aparte chip in de server waarop de encryptiesleutel wordt opgeslagen. Zo is de sleutel altijd gescheiden van de harddisk. Alleen als een kwaadwillende én de harddisk heeft, én bij de chip op de server kan, zou hij de sleutel kunnen ontcijferen. Dus, mocht een laptop, smartphone of draagbaar opslagmedium verloren of gestolen worden, dan is de informatie op de harde schijf nog steeds veilig.

Om zeker te zijn van optimale bescherming van uw data, is het raadzaam om zoveel mogelijk te versleutelen. Zeker als de data buiten het eigen domein van de organisatie opgeslagen wordt, zoals bij een hosting- of storageprovider of in een extern datacenter. De data passeren daarbij verschillende externe leveranciers.



Uw ICT-omgeving in eigen beheer of in een datacenter?

Tegenwoordig hebben we te maken met enorm grote hoeveelheden data. Vaak is uw bedrijfsinformatie vertrouwelijk en daarom lijkt het voor de hand liggend om deze zelf te beheren. Toch is een extern datacenter vaak een stuk veiliger. Waarom? In dit hoofdstuk gaan we hier dieper op in.

De voordelen van een datacenter

Natuurlijk bent u ervan overtuigd dat u uw data goed beschermt. Een extern datacenter is echter volledig ingericht op het beheer van ICT-omgevingen en omdat de volledige focus hierop ligt, is het inschakelen van een extern datacenter vaak een stuk veiliger.

Voordelen op een rij:

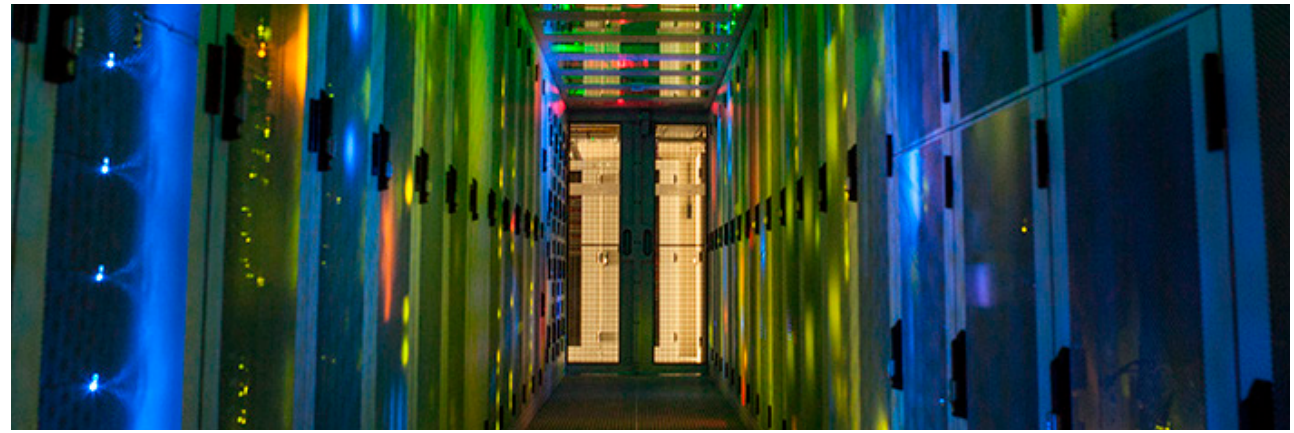
- Volledige focus op het beheer van uw ICT-omgeving door gespecialiseerde professionals.
- Goede beveiligingsmaatregelen. Denk aan een groot gesloten hek om het pand en beveiligingscamera's. En, niemand kan zomaar binnenlopen. Er komen alleen mensen bij uw ICT-omgeving als er onderhoud nodig is. Bij inhouse databeheer kunnen medewerkers vaak zo binnenlopen en bij bedrijfsgevoelige data in de buurt komen.
- De koelingstechniek en het energieverbruik is zeer efficiënt. Er wordt veel capaciteitsvoordeel behaald doordat er meerdere ICT-omgevingen worden beheerd.

Hoe maakt u de juiste keuze voor uw datacenter?

Datacenters kennen grote onderlinge verschillen. Waar moet u nu op letten om de juiste keuze te kunnen maken. De belangrijkste onderscheidende factor is veiligheid. Een datacenter moet hoge veiligheidsstandaarden hebben. U steekt immers zelf ook veel tijd en geld in uw ICT-infrastructuur voor een veilig transport van data tussen het datacenter en de organisatie. Deze veiligheid wordt volledig teniet gedaan als er door het datacenter te weinig beveiligingsmaatregelen zijn getroffen.

Zo is de fysieke beveiliging van het pand zeer belangrijk. Er moeten geen ongewilde gasten bij de systemen kunnen komen. De security-standaarden ISO 27001 en NEN 7510 zijn aanwijzingen voor het gewenste beveiligingsbeleid. Ook zijn er in een datacenter verschillende mogelijkheden om kwetsbare data extra te beschermen, zoals het bouwen van een 'cage' of een suite om de apparatuur heen.

Checklist – Kies het juiste datacenter in 6 stappen



De keuze voor een datacenter kunt u eenvoudig maken aan de hand van onderstaande checklist.

1. Breng uw huidige en toekomstige behoeftes in kaart

De beste keuze voor een datacenter maakt u als de huidige en toekomstige behoeftes voor de ICT-omgeving bekend zijn.

Breng in kaart hoe de ICT-omgeving van uw organisatie er vandaag de dag uitziet aan de hand van de volgende vragen:

- Wat verbruikt de ICT-omgeving aan energie (werkelijk)?
- Hoeveel ruimte neemt de ICT-omgeving in beslag?
- Heeft alle apparatuur een redundante voeding?
- Welke verbindingen naar de buitenwereld zijn er?
- Gebruikt de organisatie derde partijen voor onderhoud aan de ICT-omgeving?
- Is er behoefte aan een primaire en secundaire locatie?
- Wat mag de maximale latency tussen de locaties zijn?

Breng daarnaast in kaart hoe uw toekomstige ICT-omgeving eruit zal komen te zien. Hierbij kunt u de volgende vragen als leidraad nemen:

- Worden ICT-systemen in de toekomst geconsolideerd of gevirtualiseerd?
- Hoe ziet het groeiscenario er qua rackruimte uit?
- Wat is het verwachte energieverbruik per rack?
- Gaat de organisatie uitbesteden en zo ja, naar welke partij?
- Hoe ziet de connectiviteitsbehoefte er in de toekomst uit (bandbreedte)?
- Is er behoefte aan internettoegang en op welke manier (access, peering of transit)?
- Is er behoefte aan connectiviteit met publieke cloud providers?

2. Bepaal welke diensten en beschikbaarheid u nodig heeft

Stel vast welke diensten uw organisatie wil afnemen in een datacenter. Is dat een footprint, een rack, een suite, een cage of wellicht een eigen zaal?

Welke datacenter-dienst past bij uw organisatie?

F **Footprint**: vloeroppervlakte per m^2 met energie en koeling, waar klanten eigen dataracks kunnen plaatsen.

R **Rack**: een 19″-rack met eigen energievoorziening en koeling.

S **Suite**: aaneengesloten aantal racks, afgesloten door een toegangsdeur waartoe louter de betreffende klant toegang heeft.

C **Cage**: een suite, met daaromheen een hekwerk, zodat er een extra beveiligingslaag om de ICT-apparatuur ontstaat.

Werkt u in een ziekenhuis, dan zal de uptime van uw systemen hoogstwaarschijnlijk minimaal 'vier negens' (99,99%) moeten zijn. Is een storing niet direct levensbedreigend of heeft u redundante locaties, dan kunt u overwegen om een iets lagere beschikbaarheid te kiezen. Hieraan hangt uiteraard een lager prijskaartje.

3. Bepaal de selectiecriteria

Welke zaken vindt uw organisatie belangrijk in een datacenter en zijn onmisbaar voor het goed functioneren van de ICT-omgeving? Deze criteria kunt u onderverdelen naar 'must haves' voor cruciale ICT- en datacenterprocessen, 'should haves' voor het optimaal gebruiksgemak in het datacenter en 'nice to haves' als mooie bijkomstigheid.

4. Stel een long- en shortlist samen

Aan de hand van de selectiecriteria kunt u nu een longlist samenstellen met datacenters die in aanmerking komen als dienstverlener voor uw organisatie. Kijk hierbij in eerste instantie naar de technische eisen en 'must haves'.

Aan de hand van de 'should haves' en 'nice to haves' kunt u de lijst inkorten tot u een stuk of drie datacenters overhoudt die aan zoveel mogelijk criteria voldoen. Met deze datacenters maakt u een afspraak om de locatie te bezoeken.

5. Bezoek de datacenters

Als u naar de datacenters op uw shortlist gaat, houdt u niet alleen uw oren, maar vooral ook uw ogen goed open. Welke algehele indruk krijgt u van de locatie, van het pand en van de mensen die u er ziet?

6. Vraag offertes op

De kans is groot dat de datacenters op uw shortlist vrijwel allemaal aan uw gestelde criteria voldoen. Als dan ook uw indruk tijdens de bezoeken niet doorslaggevend is, kunt u kijken naar de tarieven. Vraag van alle datacenters die nog op de shortlist staan een offerte op en maak vervolgens uw keuze gebaseerd op tarief.

Is het datacenter veilig genoeg?

Tijdens uw bezoek kunt u direct testen hoe het met de beveiliging is gesteld. Mag u zo doorlopen, omdat men weet dat u een afspraak heeft, of moet u toch uw legitimatie laten zien en wordt u aan een security check onderworpen? Let erop hoe makkelijk of moeilijk u toegang tot de diverse ruimtes krijgt. Kunt u overal zomaar komen of zijn er additionele beveiligingsmaatregelen genomen? Hoeveel barrières zijn er voordat u in de serverruimte staat? Is het hek hoog genoeg of kan iemand daar zonder al te veel moeite overheen komen? Hangen er overal camera's? En wordt er ook naar die beelden gekeken?

Waar u verder nog aan moet denken

Met een passende infrastructuur, encryptie van uw data en professioneel databeheer bent u al op de goede weg naar een veilige infrastructuur. Natuurlijk zijn er nog veel meer elementen die de veiligheid van uw infrastructuur beïnvloeden. In dit hoofdstuk lichten we twee belangrijke elementen toe.

1. Monitoring van het netwerk

Ondanks alle beveiligingsmaatregelen, moet u uw netwerk altijd blijven monitoren. Ten eerste om storingen op tijd te traceren en ten tweede om in de gaten te houden dat er geen ongewenste activiteiten plaatsvinden van bijvoorbeeld cybercriminelen.

Wat is monitoring?

Monitoring betekent dat u al uw verbindingen en actieve apparatuur met monitoringssoftware in de gaten houdt. Als er niks vreemds aan de hand is, dan ziet u niks. Maar, op het moment dat bijvoorbeeld een ethernetswitch problemen heeft of er gaat apparatuur kapot, dan krijgt u hier een melding van. Zo kunt u direct actie ondernemen.

Monitoring van uw netwerk vindt vaak plaats aan twee kanten. Indien u een beheerde verbinding afneemt, wordt de monitoring zowel door de organisatie zelf als door de telecomleverancier gedaan. De leverancier heeft zicht op zijn eigen netwerk en de organisatie heeft zicht op de gehele ICT-infrastructuur, inclusief haar eigen netwerk en de apparatuur die zich daarop bevindt.

Monitoring aan de kant van de leverancier

Bij een beheerde glasvezelverbinding wordt vaak een RFTS (Remote Fiber Test System) geïnstalleerd door de provider. Deze software detecteert storingen in de glasvezelkabels en heeft als bijkomend voordeel dat ongewenst aftappen wordt opgemerkt.

Een voorbeeld. Het komt nog wel eens voor, zeker in kleinere organisaties, dat de

schoonmaakster om vijf uur binnenkomt en de stekker uit het stopcontact trekt om de stofzuiger te kunnen gebruiken. De leverancier krijgt hier meteen melding van en kan dan onderzoeken wat er aan de hand is. Is er een stroomstoring? Zijn er werkzaamheden?

Is er een stekker losgetrokken? Of is er een hacker actief? Vervolgens kan gericht actie ondernomen worden. In het geval van de schoonmaakster is dit natuurlijk niet nodig, maar mocht er iets kapot zijn, dan kan er direct een monteur naartoe worden gestuurd.

Monitoring door uw organisatie zelf

Natuurlijk moet uw eigen ICT-afdeling het netwerk en de actieve apparatuur ook in de gaten houden. Bij netwerkapparatuur worden vaak monitoringtools geleverd waarmee u onder meer latency, retransmissies en bit errors kan meten. Het is aan te bevelen dat u uw netwerkcomponenten en –poorten actief beheert, waardoor 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.

2. Niet-technische randvoorwaarden: de mens is de zwakste schakel

Naast alle technische mogelijkheden is het belangrijk een helder beleid te formuleren voor het omgaan met gevoelige data. In de praktijk blijkt de mens nog altijd de zwakste schakel als het gaat om de veiligheid van uw bedrijfsgevoelige informatie.

De mens is vaak de zwakste schakel als het gaat om veiligheid.
Om de risico's van het lekken van uw gevoelige bedrijfsinformatie te verkleinen is het van belang om:

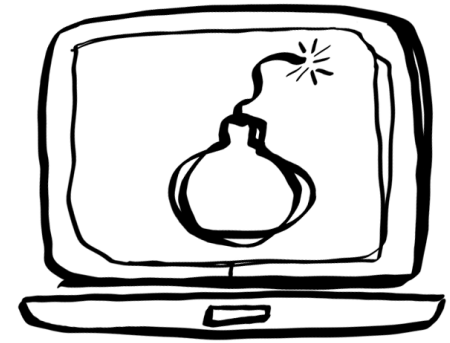
- goed in te richten welke medewerker welke data mag en kan inzien en gebruiken
- awareness te creëren onder uw medewerkers, zodat ze zich bewust worden van de risico's

Het belang van Identity & Access Management

Identity & Access Management houdt in dat u de toegang tot uw bedrijfsinformatie op een gestructureerde manier beheert en dat u de gebruikers van uw data kunt identificeren en controleren.

Een aantal voorbeelden van wat er zowel wordt opgenomen in een Identity & Access Management beleid:

- Inlogcodes en accounts van vertrekkende medewerkers moeten direct worden geblokkeerd
- Een jaarlijkse controle op 'spookaccounts'
- Verplichte screening van medewerkers
- Controles op het verplaatsen van bepaalde hoeveelheden data
- Het verbieden van het gebruiken van externe opslagbronnen
- Zorg voor een bezoekersnetwerk en weet wie er op dit netwerk zitten

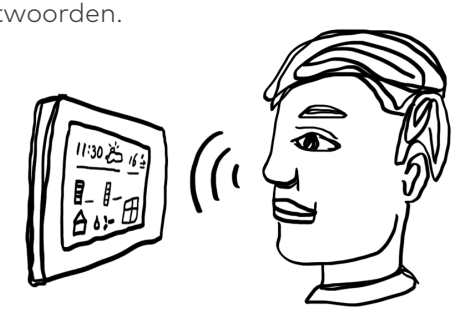


Awareness creëren

Awareness is een continu proces in een organisatie waarmee u uw medewerkers er steeds opnieuw bewust van maakt hoe ze veilig kunnen omgaan met gevoelige data. Ze moeten zich bewust worden van de risico's van onzorgvuldig gebruik van data en ze moeten inzien dat cybercriminelen vandaag de dag steeds meer manieren hebben om bij bedrijfsinformatie te komen. We verbinden immers steeds meer apparaten met het internet.

Om dit voor elkaar te krijgen, kunt u bijvoorbeeld regelmatig een awareness-sessie geven. Een paar voorbeelden van wat u in deze sessies kunt vertellen:

- Laat zien hoe cybercriminelen te werk gaan; leg bijvoorbeeld uit hoe een phishing mail werkt.
- Leg uit wat er kan gebeuren als er wordt ingelogd op onbeveiligde WiFi-verbindingen.
- Maak ze er bewust van dat wachtwoorden opschrijven zeer gevaarlijk is en geef ze tips voor het gebruiken én onthouden van sterke wachtwoorden.



Tot slot

Hoe goed een organisatie zijn beveiliging ook inricht, de praktijk leert dat cybercriminelen altijd een stap verder zijn. Vertrouw niemand anders dan uzelf als het op security aankomt en versleutel zoveel mogelijk op het eigen netwerk van de organisatie.

Met het stijgende aantal cyberaanvallen is het geen kwestie of, maar wanneer hackers proberen uw systemen binnen te komen. Met de juiste keuzes voor infrastructuur, encryptie en data-beleid kunt u een aanval wellicht niet voorkomen, maar zo heeft u wel de juiste maatregelen als die situatie zich voordoet en kunt u hier adequaat op inspelen. Zo houdt u het risico op verlies van uw bedrijfsgevoelige informatie zo klein mogelijk.

Benieuwd naar wat wij voor uw organisatie kunnen betekenen?

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'.

Kijk op www.eurofiber.nl

Eurofiber. Lifeline for the digital society

Safariweg 25-31, 3605 MA Maarssen
Postbus 7072, 3502 KB Utrecht
+31(0)30 242 8700, info@eurofiber.nl
www.eurofiber.nl

eurofiber