‘Dark fiber meest veilige keuze’

Organisaties worden verplicht privacygevoelige data optimaal te beschermen

In zes stappen naar een veilige infrastructuur

De Europese Commissie werkt aan nieuwe data-beschermingsregels en in Nederland is onlangs de Wet bescherming persoonsgegevens uitgebreid met de Meldplicht Datalekken. De nieuwe regels hebben verregaande consequenties voor organisaties. Zij worden verplicht om hun privacygevoelige data optimaal te beschermen. Falen zij daarin, dan kunnen ze forse boetes tegemoet zien. Hoe zorgt u ervoor dat uw data zo veilig mogelijk zijn?

Stap 1: Keuze voor de fysieke infrastructuur

Met het oog op veiligheid is een managed dark fiber verbinding de beste keuze. Een volledig eigen buis is dan de meest veilige optie, maar dat is voor slechts zeer weinig organisaties haalbaar én betaalbaar. Een belangrijke voorwaarde is dan wel dat kennis en expertise aanwezig zijn in de organisatie voor de belichting van de vezel. Is die kennis niet voorhanden, dan is een belichte glasvezel een goede keuze. Een telecomleverancier levert in dat geval naast een onbelichte vezel ook de belichtingsapparatuur, maar in beide gevallen (dark fiber en belichte vezel) zorgt de netwerkleverancier voor het beheer en het onderhoud. In zo’n geval maakt het niet uit of er wordt gekozen voor DWDM of Ethernet (zie kader).

Die keuze hangt namelijk weer samen met de benodigde bandbreedte. Heeft een organisatie een hoge bandbreedte nodig, vaak in combinatie met een storage-oplossing, dan wordt gekozen voor DWDM. Is er een transportverbinding nodig om gebruikers met het datacenter te verbinden, dan gebeurt dat veelal op basis van Ethernet. 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 een organisatie het beste kan maken, is dus afhankelijk van de toepassing van de verbinding.

Stap 2: Encryptie op de fysieke infrastructuur

Om te kunnen voldoen aan de nieuwe Nederlandse en komende Europese wetgeving op het gebied van databescherming is encryptie onontbeerlijk. Encryptie versleutelt data, zodat als het onverhoopt verloren of gestolen wordt, kwaadwillenden er niets aan hebben, omdat ze de data niet kunnen ontcijferen. Encryptie kan op verschillende lagen in het OSI-model plaatsvinden. De meest logische plaats voor een organisatie om te versleutelen, is afhankelijk van de toepassing van de verbinding. Op de onderste lagen van het OSI-model, de fysieke laag, wordt encryptie hardwarematig toegevoegd door encryptors in de belichtingsapparatuur. Op de hogere lagen van het model zijn de versleutelingsmogelijkheden softwarematig. Een data-encryptor versleutelt data op een dusdanige manier dat het bijna onmogelijk is om ontvreemde data te ontcijferen. Een goede encryptiesleutel die regelmatig wisselt en verschillende bit-lengtes heeft (hoe langer de lengte des te lastiger te kraken), is cruciaal. Daarnaast moet encryptie voldoen aan de meest gangbare standaarden, zoals AES (Advanced Encryption Standard) en het Amerikaanse FIPS (Federal Information Processing Standard).

Een nadeel van encryptie hoger in de OSI-lagen is dat er steeds meer latency wordt toegevoegd wat een nadelige invloed kan hebben op de snelheid van de verbinding. Een voordeel van encryptie op laag 3 (Ethernet) is dat het mogelijk is om een selectie te maken tussen data die wel of niet versleuteld moeten worden. Op de onderste laag wordt hardwarematig namelijk alle verkeer versleuteld. De meest logische plek voor encryptie hangt dus af van de toepassing. Als het gaat om bijvoorbeeld een ziekenhuis waarbij hoge eisen worden gesteld aan de maximale latency, zal encryptie op het fysiek niveau de voorkeur hebben. Ook als er veel privacygevoelige en geheime informatie over de verbinding wordt verstuurd, is versleuteling op een laag niveau te prefereren.

Stap 3: Keuzes voor en in het datacenter

Een veilige infrastructuur zorgt voor een secure transport van data tussen het datacenter en de organisatie. Dat betekent dat de keuze voor een datacenter nauw samenhangt met de veiligheid van de data. De prestaties van een veilige infrastructuur worden anders volledig teniet gedaan als er te weinig beveiligingsmaatregelen zijn getroffen.

Fysieke beveiliging van het pand is belangrijk, zodat er 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. De keuze voor een solide datacenter kun je eenvoudig maken aan de hand van een aantal stappen (zie kader).

Stap 4: Monitoring van het netwerk

Door middel van monitoring kunnen verstoringen in het netwerk worden gedetecteerd. In het geval van een dark fiber verbinding is de klant degene die de actieve apparatuur in het netwerk monitort. Sommige telecomproviders installeren een RFTS (Remote Fiber Test System) om storingen te kunnen detecteren in de glasvezelkabels, met bijkomend voordeel dat ongewenst aftappen kan worden gedetecteerd. Als er een belichte vezel wordt afgenomen, wordt de monitoring zowel door de klant als door de telecomleverancier gedaan.

‘Versleutel alles dat buiten het domein van de organisatie komt’

Dark fiber, DWDM en Ethernet

Een dark fiber is een onbelichte glasvezel. Dat betekent dat de klant die een dark fiber afneemt, zelf belichtingsapparatuur (Ethernet switch / router of x WDM apparatuur) moet plaatsen op de locaties waar de glasvezel binnenkomt (in het datacenter en op de verschillende locaties van de organisatie).

DWDM staat voor Dense Wavelenght Division Multiplexing en is een privékanaal in een glasvezel. De afgenomen glasvezel wordt dan belicht door apparatuur van de leverancier. Glasvezels transporteren data door middel van lichtpulsen. Deze lichtpulsen hebben een bepaalde golflengte. DWDM is een technologie die data van verschillende bronnen tegelijk door een glasvezel kan sturen, waarbij ieder signaal dat tegelijk met andere wordt verstuurd zijn eigen lichtgolflengte krijgt. Daardoor kunnen aparte kanalen worden gecreëerd.

Ethernet is een netwerk waarbij het kantoornetwerk of het netwerk waar de gebruikers op werken 1:1 wordt verlengd naar een andere locatie of datacenter. Ethernet is een netwerk waarbij diverse virtuele netwerken kunnen worden gedefinieerd, voor het transporteren van data, internet en IP telefonie.

Zo kies je het juiste datacenter

1. Breng de behoefte in kaart
   a. Welke diensten wil je afnemen?
   b. Welke beschikbaarheid is nodig?
   c. Welke behoeftes zijn er in de toekomst?
2. Bepaal de selectiecriteria
3. Stel een longlist samen
4. Stel een shortlist samen
5. Bezoek de datacenters
   a. Hoe is de expertise van het datacenterpersoneel?
   b. Hoe is de beveiliging?
   c. Wat zijn de uitbreidingsmogelijkheden?
6. Vraag offertes op
7. Maak de keuze en start de migratie

[bron: Whitepaper Eurofiber, In zeven stappen naar de juiste keuze voor een datacenter]

> ‘Juiste keuzes voor infrastructuur, encryptie en beleid voorkomt schade door datalekken’

De leverancier heeft zicht op zijn eigen netwerk en de klant heeft overzicht over het gehele stuk, inclusief zijn eigen netwerk en de apparatuur die zich daarin bevindt. Als zich verstoringen voordoen, kan eenvoudig worden nagegaan of het een storing betreft naar aanleiding van (geplande) werkzaamheden of dat er iets anders aan de hand is. Veelal zal een telecomleverancier door middel van een goede registratie vooraf aangeven wanneer en waar werkzaamheden plaatsvinden en welke klanten daar mogelijk iets van kunnen merken. Bij alle netwerkapparatuur worden monitoringtools geleverd waarin onder meer latency, retransmissies en bit errors worden gemeten. Het is aan te bevelen dat klanten actief hun netwerkcomponenten en -poorten beheren waardoor zij bij latency-veranderingen en onderbrekingen van het signaal direct alarmbellen zien afgaan; dat zijn indicaties dat er mogelijk ongewenste apparatuur in het netwerk is geplaatst.

Stap 5: Data-encryptie

De vernieuwde Wet bescherming persoonsgegevens bepaalt dat organisaties verplicht zijn hun data optimaal te beschermen. Bedrijven moeten kunnen aantonen dat hun data op het moment van verlies of diefstal was beschermd. Dat kan met behulp van encryptietools. Waar bij versleuteling op fysiek niveau (OSI-model) alleen data worden beschermd die over de verbinding worden gestuurd, worden data bij data-encryptie ook versleuteld op de interne (en externe) opslagsystemen van de organisatie. Mocht een laptop, smartphone of draagbaar opslagmedium verloren of gestolen worden, is de informatie op de harde schijf nog steeds veilig wanneer het versleuteld is. Om volledig zeker te zijn van optimale bescherming van de data, is het raadzaam om zoveel mogelijk te versleutelen. Zeker als de data buiten het eigen domein van de organisatie opgeslagen worden, zoals bij een hosting- of storageprovider of in een extern datacenter. De data passeren daarbij verschillende externe leveranciers, daardoor is zekerheid alleen geborgd bij volledige encryptie. Immers, op de domeinen van leveranciers heeft een organisatie geen invloed.

Stap 6: Niet-technische randvoorwaarden

In de praktijk blijkt de mens nog altijd de zwakste schakel als het gaat om de beveiliging van privacygevoelige informatie. Naast alle technische mogelijkheden is het belangrijk om een helder beleid (governance) te formuleren voor het omgaan met gevoelige data. Zo is het van belang om goed in te richten welke medewerker welke data mag en kan inzien en gebruiken (Identity & Access Management). Inlogcodes en accounts van vertrekkende medewerkers moeten direct worden geblokkeerd en er zou een jaarlijkse controle op ‘spookaccounts’ moeten plaatsvinden. Verdergaande maatregelen kunnen het screenen van medewerkers zijn, controles op het verplaatsen van bepaalde hoeveelheden data en het verbieden van het gebruiken van externe opslagbronnen. Awareness is een continu proces in een organisatie waarbij medewerkers er steeds opnieuw bewust van worden gemaakt hoe ze veilig kunnen omgaan met gevoelige en geheime data.

Vertrouw niemand

Hoe goed een organisatie zijn beveiliging ook inricht, de praktijk leert dat cybercriminelen altijd een stap verder zijn. Vertrouw niemand anders dan jezelf 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 de systemen binnen te komen. Met de juiste keuzes voor infrastructuur, encryptie en beleid kun je een hack wellicht niet voorkomen, maar wel zorgen voor de juiste maatregelen als die situatie zich voordoet.

Rudi de Visser is Sr. Business Consultant bij Eurofiber

Verschillende encryptiestandaarden

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.

Cloudian begeleidt bedrijven naar slimme object storage

Cloudian, leverancier van object storage-oplossingen, lanceerde recentelijk haar nieuwe ‘forever live’-product en een update van haar Hyperstore-software en daagt daarmee de gevestigde merken uit.

Ook andere partijen zoals EMC, NetApp en HP hebben immers omgevingen in de markt die praktisch oneindig geschaald kunnen worden. Toch is er volgens Jacco van Achterberg, EMEA-verantwoordelijke bij Cloudian een belangrijk verschil. “In ons geval kun je grote en kleine nodes mixen, dat kan bij veel van de grotere leveranciers niet. Het is het verschil tussen ‘scale up en scale out’.”

De productaankondiging valt samen met de aankondiging van Hyperstore 5.2, een sleutelelement in het aanbod van Cloudian. Van Achterberg: “We hebben een slag gemaakt in de nieuwe software op het gebied van dynamische herkenning, de toevoeging van een nieuwe node wordt automatisch herkend en desgewenst wordt de workload direct herverdeeld. Daarbij maakt het niet uit of de storage-omgeving over verschillende datacenters gedistribueerd is.”

Cloudian gebruikt de REST S3-API voor de communicatie van haar systemen. Daarnaast ‘leende’ de storage-leverancier de hierarchische infrastructuur nodes, racks, datacenters, regio’s van Amazon. “Dankzij S3 kunnen we een peer to peer-concept toepassen, zodat de nodes rechtstreeks met elkaar kunnen communiceren.” Omdat Cloudian met deze RESTful API werkt, kunnen gebruikers hun data naar een publieke cloud brengen en deze weer terugzetten op een lokale omgeving. Dat is momenteel nog alleen Amazon, maar in de planning zitten ook andere leveranciers van public clouds. Om bedrijven die pas aan het begin van hun ‘cloud’-leven staan een soepele transitie te bieden, biedt de opslagfabrikant in de nieuwe versie van haar software ook file access. “Zo bieden we een migratiepad voor organisaties die naar objectstorage willen, maar het historisch niet kunnen.”

HyperStore 5.2 biedt daarnaast policies voor opslag op basis van selfservice. Gebruikers kunnen policies voor hun gegevens definiëren op bucket-niveau. De functionaliteit van HyperStore voor het beheer van policies op gebruikersniveau stelt medewerkers in staat om beleidsregels te specificeren voor hun gegevens en zorgt daarmee voor een aanzienlijke vermindering van de operationele kosten. “Voorheen was het zo dat alle data als ‘even belangrijk’ werd aangemerkt, nu kunnen we bijvoorbeeld voor back-ups aangeven dat bepaalde informatie maar op twee locaties wordt opgeslagen en andere op acht locaties”, aldus Van Achterberg.