

Jaarlijks presenteert Conscia Nederland zijn Technology Outlook, waarin wij de trends benoemen die wij in de markt zien als het gaat om Secure Hybrid IT Infrastructure. Voor de oplettende lezer is ten opzichte van vorig jaar de term 'Hybrid' nu prominent aanwezig. Er is geen omgeving meer die niet – bewust of onbewust – gebruik maakt van één of meerdere clouds als aanvulling op de lokale IT Infrastructuur voor het laten landen van data en applicaties.

Zoals in eerdere Conscia Technology Outlooks aangegeven, is de wereld na de pandemie en de niet voorziene ontwikkelingen op globaal niveau in dit opzicht blijvend veranderd. Het flexibel om kunnen gaan met interne en externe (IT) resources is een principe geworden dat door veel organisaties is omarmd.

Hand in hand hiermee gaat natuurlijk de aandacht voor Cybersecurity. Hebben we de achterstand ingehaald zoals vorige jaren beoogd? Mogelijk is dit een utopie geziende snelheid waarmee ook criminelen ontwikkelen.. De noodzaak om deze bedreigingen serieus te nemen is ondertussen echter wel onderkend. Ook het principe 'Secure by Design' op alle gebieden van de IT -infrastructuur is gemeengoed geworden.

Duurzaamheid

Met de stijgende energiekosten en het bewustzijn dat we het afgelopen jaar hebben gekregen ten aanzien van ons energiegebruik, is duurzaamheid bij veel organisaties nog hoger op de prioriteitenlijst komen te staan. Hebben we alle IT nodig die 's nachts aanstaat of zijn er switches die uit kunnen? Kunnen we servers 's nachts iets anders laten doen dan overdag voor een hogere efficiëntie? Kunnen we ijskoude data offloaden naar offline disks? Zetten we cloud waste services in de Public Cloud in voor minder gebruik?

Er wordt kritisch gekeken naar IT om onze 'carbon footprint' te verkleinen en te besparen op IT kosten. Cruciaal hierbij is de samenwerking met andere afdelingen om de technische mogelijkheden in lijn te brengen met de behoeften vanuit de business.

Een trend die al enige jaren gaande is op het gebied van applicaties en workloads, en die ook bijdraagt aan het efficiënt omgaan met resources, is om zaken 'as-a-Service' af te nemen. Deze trend zet nu ook door in de richting van netwerkinfrastructuren. Niet alleen het buiten de deur zetten van datacenteromgevingen, maar ook het afnemen van de lokale netwerken als dienst in de vorm van een **Network-as-a-Service (NaaS)** of in een pay-per-use model. Ook in 2023 zal er een groei zijn in Network Operation Center (NOC) en Security Operation Center (SOC) dienstverlening.

Secure Connectivity

Bijna alle organisaties willen aansluiten op meerdere clouds volgens dezelfde principes als ze connectie maken met hun lokale datacenters. Wij zien hier een toenemende vraag voor een **centrale hub functie** waar organisaties een connectie naartoe maken. Vanuit deze centrale plek wordt vervolgens de connectie gelegd naar elke gewenste cloud, carrier en locatie; de opstap naar Hybrid Cloud-gebruik en een decentrale architectuur.

Een locatie in een decentrale architectuur is slechts één van de plekken in een groter geheel. Concreet: zorg verlenen, studenten opleiden en distribueren van goederen zijn activiteiten, geen locaties. Een ziekenhuis, universiteit en distributiecentrum verrichten activiteiten en zijn zo onderdeel van een procesketen. Als we dit vertalen naar de benodigde IT architectuur, gaan we dus steeds meer uit van netwerk, security en het verwerken en opslaan van data, ontworpen als **software defined overlay** over diverse locaties en aansluitend bij de activiteit en het proces. Een belangrijk designprincipe is dat

de controle van de decentrale Secure Hybrid IT Infrastructure niet afhankelijk is van één fysieke locatie. De nieuwe standaard is dat **controllers in de cloud** staan.

Cybersecurity

Bij decentralisatie van de enterprise omgeving hoort ook het afhandelen van services en security aan de rand van het netwerk (edge) met verschillende beveiligingsmaatregelen. Een architectuur die hierop inspeelt is **Secure Access Service Edge (SASE)**. Een SASE architectuur is een combinatie van verschillende oplossingen: SD-WAN, Secure Web Gateway, Cloud Access Security Broker, Firewall-as-a-Service en Zero Trust Network Access, gecombineerd met gecentraliseerd management. SASE (of deze architectuur in een andere benaming) zal door veel organisaties opgenomen worden als doel om tegenwicht te kunnen bieden aan cybercriminaliteit.

Bij beveiliging aan de rand van het netwerk hoort uiteraard end-point protectie. Trend hierin is de ontwikkeling en de inzet van **eXtended Detectie & Response** oplossingen (XDR). XDR combineert de trend van een decentrale architectuur en controle vanuit de cloud, een typisch voorbeeld van een oplossing die past in de SASE architectuur.

Hybrid Cloud

IT is gegroeid tot een niet schaalbare dienst. Veel IT afdelingen krijgen de projectkalender en beheersing hiervan niet voor elkaar en zien alleen groei in FTE's als uitweg. Ook de verschillende platforms - fysiek of virtueel en in eigen datacenters of bij (hyperscale) Cloud Providers - dragen hier niet aan bij. Platforms kunnen binnen zichzelf worden geautomatiseerd met hun eigen tools. Echter, de meeste organisaties zijn genoodzaakt om gebruik te maken van meerdere platforms. De huidige trend is dat organisaties inzetten op het gebruik van overkoepelende **Cloud Management Platforms** die zowel fysiek, virtueel als meerdere hyperscalers vanuit een centrale omgeving aansturen. Hiermee ontstaat in abstractie een centrale omgeving die als zodanig gemanaged wordt, met onderliggend verschillende cloud providers en hun eigenschappen.

Mogelijkheden op Hybride IT, consumptie modellen en technologische innovatie, gecombineerd met toenemende dreiging en issues op het gebied van levertijden en geopolitiek, zorgen voor een toenemend vraag naar cloud- en cybersecuritydiensten. De opmars van gebruik van Public Cloud providers in Nederland zorgt ook voor meer vraag naar soevereine cloud services. Dit zijn diensten die worden geleverd door een **Private Cloud op Nederlands grondgebied**, met Nederlands recht door een Nederlands bedrijf. Een ideale plek bijvoorbeeld voor backup- of archiveringsdiensten.

Een ander vooruitzicht is de toename van **marketplaces**. We gaan zien dat grote tech fabrikanten ook met landingszones en marketplaces komen waar klanten IT kunnen 'aanklikken' en aanverwante services uit het ecosysteem van die fabrikant afnemen.

Consultancy

Met deze ontwikkelingen die het voor de IT gebruiker makkelijker maakt, neemt de **complexiteit** van het IT landschap alleen maar toe. Niet in de laatste plaats door de snelle ontwikkeling en verbreding van het vakgebied (denk aan IoT, IT/OT, ML/AI, Cloud, micro-services, edge computing, etc.). Maar ook als het gaat om de verschuiving van verantwoordelijkheden bij Smart Buildings of Hospitals naar de IT afdeling. Gespecialiseerde consultants kunnen helpen deze complexiteit het hoofd te bieden. Ook in 2023 zal de hulpvraag naar IT specialisten voor het ontwikkelen van een gedegen visie, strategie en architectuur toenemen. De tijd van 'Silo-denken' is voorbij, alle aandacht is nu gericht op het realiseren van een goede en veilige samenhang tussen alle componenten van de totale Secure Hybrid IT Infrastructure.