De CIO & IT Manager-gids voor private & hybride cloud

Zes inzichten voor een toekomstbestendige IT-strategie

YOU FOCUS, WE MANAGE.

EPACT

Inleiding

De cloudmarkt is de voorbije jaren ingrijpend veranderd.

Licentiemodellen werden herzien, compliance-vereisten aangescherpt, en de verwachting dat alles naar public cloud zou migreren, is voor veel organisaties niet uitgekomen of heeft geleid tot kosten en afhankelijkheden die achteraf moeilijk te rechtvaardigen waren.

CIO's en IT-managers die vandaag hun cloudstrategie (her)bekijken, doen dat in een complexere context dan vijf jaar geleden. De keuze is niet langer "cloud of geen cloud", maar welk model past bij welke workload, welke partner biedt de juiste combinatie van controle en ontzorging, en hoe bouw je een omgeving die zowel technisch als juridisch houdbaar is.

Dit ebook gaat over die afwegingen. Niet als introductie voor beginners, maar als referentie voor wie de basiskennis al heeft en op zoek is naar scherpere inzichten: over private en hybride cloud, beveiliging en compliance, migratie en beheer. Elk hoofdstuk staat op zichzelf. Samen vormen ze **een kader om de juiste vragen te stellen én de antwoorden beter te beoordelen.**

HOOFDSTUK 1

Waarom private cloud nog steeds relevant is voor moderne IT-organisaties

Er is de voorbije jaren een hardnekkig verhaal verteld in de IT-sector: public cloud is de toekomst, en wie nog nadenkt over private infrastructuur, kijkt achteruit. Dat beeld klopt niet, en het kost organisaties die er kritiekloos in meegaan geld en controle.

Private cloud is niet nostalgisch. Het is een bewuste strategische keuze met duidelijke voordelen, maar tegelijk ook met reële kosten en verantwoordelijkheden die je niet mag onderschatten.

Het verschil dat er echt toe doet

Public cloud en private cloud zijn geen varianten van hetzelfde product.
Ze vertrekken vanuit fundamenteel andere uitgangspunten.

Bij public cloud betaal je voor gedeeld gebruik: de provider beheert alles en je schaalt moeiteloos op. Dat is niet alleen een verkooppraatje. De flexibiliteit is reëel, de time-to-market is snel en je hoeft geen infrastructuurexpertise in huis te houden.

Maar die structuur brengt ook beperkingen met zich mee. De belangrijkste pijnpunten: je data verlaat je eigen omgeving, je hebt geen controle over de onderliggende hardware en de kostenstructuur wordt al snel complex en moeilijk voorspelbaar naarmate je omgeving groeit.

Private cloud draait op infrastructuur die exclusief voor jouw organisatie is ingericht, ofwel in je eigen datacenter, ofwel bij een partner zoals Epact. Je behoudt volledige controle over netwerk, opslag, hypervisorlaag en datalocatie. Beveiliging en compliance zijn niet afhankelijk van de regels van een grote externe provider, maar van keuzes die jij zelf maakt.

Maar eerlijk is eerlijk: private cloud vraagt een hogere initiële investering in hardware, vereist interne of externe infrastructuurexpertise, en biedt minder elasticiteit bij onverwachte piekbelasting.

Wanneer public cloud tekortschiet

Bij Epact geloven we dat private cloud voor veel middelgrote tot grote KMO's de beste basis vormt, maar niet voor allemaal. Hieronder helpen we je inschatten wanneer dat het geval is, en wanneer niet. De drie momenten waarop public cloud zijn beloftes niet waarmaakt, zijn telkens dezelfde.

1

Kostenbeheer

Public cloud is goedkoop om mee te beginnen en duur om bij te blijven. Licentiekosten voor specifieke services, de prijs van managed databases, netwerktransfers, support-contracten, egress-kosten (cloudproviders rekenen vaak kosten voor data die uit hun cloud wordt gehaald, terwijl inkomende data (ingress) vaak gratis is): de kosten stapelen zich op.

Organisaties die hun public cloudkosten nauwkeurig analyseren, komen er zelfs regelmatig achter dat ze voor een voorspelbare workload significant meer betalen dan nodig. Dat gezegd zijnde: voor onregelmatige of onvoorspelbare workloads kan public cloud wél goedkoper zijn dan een eigen infrastructuur.

2

Vendor lock-in

Hoe dieper je integreert in het ecosysteem van één provider, hoe groter je afhankelijkheid wordt. Migreren naar een andere omgeving, of zelfs een deel van je workloads terugbrengen, wordt een architecturale en budgettaire uitdaging. Die afhankelijkheid heeft ook een strategische prijs: als de provider zijn prijsbeleid of productaanbod wijzigt, heb je weinig onderhandelingsmarge.

Volledigheidshalve: ook private cloud kan tot lock-in leiden als je diep integreert met de tooling of hypervisor van één leverancier. De vraag is dus niet of je afhankelijkheid vermijdt, maar van wie en in welke mate.

3

Datasoevereiniteit en compliance

Voor organisaties in gereguleerde sectoren, zoals de zorgsector, de overheid, de financiële sector of de sector van de juridische dienstverlening, is de locatie van data geen detail. GDPR en sectorspecifieke regelgeving zoals NIS2 stellen concrete eisen aan waar data wordt opgeslagen en verwerkt, wie er toegang toe heeft en welke garanties er gelden.

Bij public cloud is dat vertrouwen afhankelijk van contractuele clausules. Bij private cloud is het een architecturele zekerheid. Dat onderscheid is op zijn sterkst in sectoren met hoge regulatoire druk. Voor bedrijven zonder strikte compliance-vereisten weegt dit argument minder zwaar.

Business impact: drie concrete voordelen

1 Voorspelbare TCO

Bij private cloud weet je op voorhand wat je infrastructuur kost. Geen verrassingen op de factuur, geen onverwachte meerkosten bij een piek in gebruik.

Die voorspelbaarheid is bijzonder waardevol voor meerjarenplanning, op voorwaarde dat je workloads stabiel en voorspelbaar zijn. Is dat niet het geval, dan is de redenering omgekeerd: je betaalt dan voor capaciteit die je niet altijd gebruikt.

2 Lage latency

Workloads die snelle responstijden vereisen, presteren beter op infrastructuur die geografisch dicht bij de gebruikers staat.

Dat geldt voor ERP-systemen, databases en elke applicatie waarbij milliseconden merkbaar zijn. Voor workloads waarbij latency minder kritisch is (batch-verwerking, archivering, testomgevingen) is dit voordeel minder doorslaggevend.

3 Maximale controle

Van de configuratie van de hypervisor tot firewall-regels en back-upbeleid: in een private cloudomgeving ben jij (en/of je IT-partner) de enige beslisser. Dat maakt audits eenvoudiger, incidentrespons sneller en architecturale keuzes autonomer.

Die controle is ook een verantwoordelijkheid: je draagt zelf de last van updates, patches, monitoring en capaciteitsplanning of je delegeert die aan een partner die dat in een managed services model voor jou opneemt.

De hypervisorlaag: een strategische keuze die te lang wordt uitgesteld

Wie nadenkt over private cloud, focust doorgaans op architectuur, datalocatie en beheermodel. Maar er is een keuze die daar structureel onder zit en die veel organisaties te laat stellen: welk platform drijft je virtualisatielaag?

Jarenlang was dat antwoord vanzelfsprekend: VMware. Maar door de overname van VMware door Broadcom en de ingrijpende wijzigingen in het licentiemodel, zijn de kosten voor veel organisaties in korte tijd sterk gestegen.

Voor CIO's en IT-managers is dit dan ook geen louter technische vraag meer. Het raakt rechtstreeks aan de TCO-berekening die private cloud aantrekkelijk maakt. Open source alternatieven zoals Proxmox bieden een volwaardig alternatief.

Als je daarover meer wil weten, is ons Ebook waarin we een vergelijking maken tussen VMware en Proxmox interessant leesvoer.

Bekijk ons Ebook

CONCLUSIE

Private cloud is geen tegenhanger van innovatie. Het is de infrastructuurlaag die je als organisatie in staat stelt om innovatie te sturen op je eigen voorwaarden, mits je de schaal, de stabiliteit en de compliance-noden hebt om dat te rechtvaardigen.

Voor CIO's en IT-managers die nadenken over hun cloudportfolio, is de vraag niet "public of private cloud?", maar "welke workloads passen waar?" Een weloverwogen private cloudomgeving als kern van je strategie, aangevuld met public cloudcapaciteit waar dat zinvol is, geeft je het beste van beide werelden. Niet als compromis. Wel als bewuste architectuurkeuze.

HOOFDSTUK 2

Hybride cloud: brug tussen legacy & future-proof IT

De realiteit van de meeste IT-omgevingen is er geen van een schone lei. Er zijn legacy-systemen die kritische processen ondersteunen en niet zomaar kunnen worden vervangen. Er zijn applicaties die gebouwd zijn voor een on-premise infrastructuur. Er zijn compliance-vereisten die bepalen waar bepaalde data mag bewaard worden. En tegelijk is er de verwachting van de business om flexibel, snel en schaalbaar te kunnen opereren.

Hybride cloud is dan ook een bewuste – en vaak noodzakelijke - architectuurkeuze die continuïteit, flexibiliteit en controle combineert in één coherent model.

Wat hybride cloud concreet betekent

Een hybride cloudomgeving combineert je on-premise infrastructuur en, waar zinvol, public cloud resources in één geïntegreerd geheel. De sleutel zit niet in de technologie zelf, maar in de integratie: workloads, data en identiteitsbeheer moeten idealiter naadloos kunnen bewegen tussen omgevingen, op basis van wat functioneel en/of strategisch het meest logisch is.

Dat betekent in de praktijk dat je je bedrijfskritische data en applicaties kan behouden op een private, gecontroleerde omgeving, terwijl je tegelijk kan schalen naar publieke cloudcapaciteit voor piekmomenten of experimentele workloads. Een best of both worlds als het ware.

Het beste van twee werelden, zonder de valkuilen

De kracht van hybride cloud zit in de vrijheid die het geeft. Geen gedwongen keuze tussen de flexibiliteit van de public cloud en de controle van private infrastructuur. Geen afhankelijkheid van één provider voor alle workloads. Geen plotse migraties die operationele risico's introduceren.

Voor CIO's en IT managers is hybride cloud het model dat het dichtst aansluit bij de realiteit van hun organisatie: geleidelijke evolutie in plaats van disruptieve overstap, met een architectuur die meeschaalt naarmate de noden evolueren. Dat is niet de makkelijkste weg, maar wel de meest verantwoorde.

Wat hybride cloud oplevert voor je organisatie

De businesswaarde van hybride cloud is het meest tastbaar op drie vlakken.

1

Kostendiscipline zonder capaciteitsangst

Je betaalt permanent voor wat je structureel nodig hebt, en schakelt tijdelijk op naar public cloudcapaciteit wanneer dat zinvol is.

Dat voorkomt twee klassieke valkuilen tegelijk: de overcapaciteit die on-premise omgevingen traditioneel kenmerkt, én de ongecontroleerde clouduitgaven die ontstaan als public cloud de enige optie is.

Het resultaat is een kostenstructuur die je kan plannen en verdedigen, ook tegenover een CFO die wil weten waar het IT-budget naartoe gaat.

2

Operationele weerbaarheid

Een hybride architectuur is van nature redundanter dan een enkele omgeving. Kritische processen kunnen worden gevirtualiseerd over meerdere locaties.

Als een on-premise component uitvalt, neemt de cloudlaag het over. Als een cloudservice tijdelijk onbeschikbaar is, draaien kernprocessen door op de private infrastructuur.

3

Snelheid waar het telt

Teams die nieuwe applicaties willen uitproberen, tijdelijk extra rekenkracht nodig hebben voor een project, of snel willen schalen voor een campagne of lancering: ze hoeven niet meer te wachten op infrastructuur.

De public cloudlaag vergroot je zakelijke slagkracht zonder de stabiliteit van de kernsystemen te raken.

Typische use cases

Burst workloads

Sommige applicaties kennen voorspelbare pieken: de maandafsluiting in een ERP-systeem, seizoensgebonden verwerking van orders, jaarlijkse rapportagecycli.

In plaats van permanent overcapaciteit te voorzien voor die pieken, kan je kiezen voor extra rekenkracht uit de public cloud.

Business continuity en disaster recovery

Een hybride architectuur laat toe om back-ups en failover-capaciteit te verdelen over meerdere locaties en omgevingen.

Als een on-premise systeem uitvalt, kunnen kritische processen worden overgenomen door een cloudlaag, met minimale impact op de werking van je organisatie.

Datalokalisatie

Niet alle data mag of kan op dezelfde plek staan.

Gevoelige klantgegevens, medische dossiers of financiële records kunnen worden bewaard in een gecontroleerde private omgeving, terwijl minder gevoelige data of analytische workloads elders worden verwerkt.

Gefaseerde migratie

Hybride cloud is ook de meest realistische manier om een migratietraject te plannen.

Applicaties kunnen stapsgewijs worden overgezet, met de mogelijkheid om terug te vallen op de bestaande omgeving als een workload nog niet klaar is voor de cloud.

Beveiliging en compliance: een aparte discipline

Een hybride omgeving vergroot het risico op aanvallen niet per definitie, maar het vereist wel een doordachte aanpak. Identiteits- en toegangsbeheer, encryptie, netwerksegmentatie en monitoring moeten de gehele omgeving bestrijken, niet alleen de on-premise laag.

Omdat beveiliging in een hybride context een eigen strategische diepgang verdient, behandelen we dit uitgebreid in het volgende hoofdstuk.

Andere uitdagingen die je niet mag onderschatten

Hybride cloud is een krachtig model, maar geen eenvoudig model. Als je er met de juiste verwachtingen aan begint, vermijd je de meest voorkomende struikelblokken.

1

Complexiteit van beheer

Twee omgevingen beheren is niet twee keer zo complex als één, het is exponentieel complexer. Netwerkconfiguraties, beveiligingsbeleid, monitoring en updates moeten consistent worden doorgevoerd over private én publieke laag. Zonder een duidelijke governance-structuur en tooling die dat overzicht biedt, ontstaat er al snel een operationeel grijze zone waar niemand het volledige plaatje ziet.

2

Integratiekwaliteit bepaalt alles

Een hybride omgeving staat of valt met de kwaliteit van de connectiviteit tussen de private en publieke laag. Trage of onbetrouwbare verbindingen maken de belofte van naadloze workload-mobiliteit hol. Dat vraagt aandacht voor netwerkarchitectuur, API-ontwerp en latency-monitoring, zeker als applicaties in real-time data uitwisselen over omgevingsgrenzen heen.

3

Gebrek aan interne expertise

Hybride cloud vereist expertise die niet altijd in huis is: kennis van zowel on-premise infrastructuur als cloudplatformen, gecombineerd met inzicht in beveiliging, compliance en architectuurontwerp. Die combinatie is schaars. Organisaties die dit onderschatten, merken het pas als een incident de zwakste schakel blootlegt. Een ervaren partner die het beheer (deels) overneemt, is voor veel organisaties geen luxe maar een noodzaak.

4

Kosten lopen uit de hand zonder governance

De flexibiliteit van de public cloudlaag is waardevol, maar ook verleidelijk. Teams die zelfstandig cloudresources kunnen opstarten, doen dat niet altijd met oog voor de factuur. Zonder centrale kostencontrole en duidelijke spelregels over wie wat mag inzetten, verandert de voorspelbare TCO van hybride cloud snel in een onaangename verrassing.

CONCLUSIE

Hybride cloud lost een probleem op dat organisaties al jaren kennen maar zelden hardop benoemen: de kloof tussen de infrastructuur die ze hebben en de wendbaarheid die ze nodig hebben. Het model biedt een realistisch pad van waar je nu staat naar waar je naartoe wilt, zonder alles overboord te gooien en zonder je vast te rijden in de beperkingen van één model.

Maar hybride cloud is geen productaankoop. Het is een architectuurkeuze die vraagt om een heldere strategie, een competent team of partner, en een governance-model dat meeschaalt met de omgeving. Als je dat goed aanpakt, win je op alle fronten: kostenbeheersing, operationele veerkracht en de vrijheid om te schalen wanneer de business daarom vraagt.

De vraag is niet of hybride cloud past bij jouw organisatie. De vraag is of jouw organisatie klaar is om er het maximale uit te halen.

HOOFDSTUK 3

Beveiliging in hybride en private cloud: IAM, netwerk en compliance

Een hybride cloudomgeving brengt meer aanvalsoppervlak met zich mee dan een enkelvoudige infrastructuur. Niet omdat de technologie inherent onveiliger is, maar omdat de complexiteit toeneemt. Er zijn meer omgevingen, meer koppelingen, meer lagen waar iets fout kan gaan. Beveiliging in een hybride context is daarom geen feature die je achteraf inschakelt. Het is een architectuurprincipe dat je van bij het begin meeneemt.

We bekijken drie domeinen die in hybride omgevingen structureel aandacht verdienen: identiteits- en toegangsbeheer, netwerkarchitectuur, en compliance en datasoevereiniteit.

Identiteitsbeheer: de stille complexiteit van hybride cloud

Van alle uitdagingen in een hybride cloudomgeving is identiteitsbeheer de minst zichtbare maar een van de meest kritische. De vraag is simpel te stellen: hoe zorg je dat de juiste gebruikers, met de juiste rechten, toegang hebben tot de juiste systemen, ongeacht of die systemen op je private infrastructuur draaien, in een publieke cloud zitten, of ergens tussenin?

In de praktijk betekent dit dat je directory-diensten — Active Directory, Entra ID, of een combinatie — consistent moeten werken over alle omgevingen heen. Single Sign-On (SSO) en Multi-Factor Authenticatie (MFA) zijn geen opties maar minimumeisen. Role-Based Access Control (RBAC) moet over de grenzen van de omgevingen heen worden beheerd, niet omgeving per omgeving.

Waar dit fout loopt (en het loopt regelmatig fout) is bij de uitzonderingen. De applicatie die geen SSO ondersteunt en dus een lokale account vereist. De legacy-dienst die nog draait op NTLM-authenticatie. De externe partner die tijdelijk toegang nodig heeft en daarvoor een account krijgt die nadien nooit wordt opgeruimd.

Een hybride omgeving dwingt je om identiteitsbeheer als architectureel principe te behandelen, niet als operationele taak. Dat begint bij een identiteitsaudit vóór de migratie en wordt verankerd in een governance-model dat bijhoudt wie toegang heeft, waarom, en tot wanneer.

Netwerkarchitectuur: de verbinding bepaalt de waarde

Een hybride omgeving is zo goed als de verbinding die de onderdelen samenhoudt. Traditionele netwerkarchitecturen zijn gebouwd voor een wereld waarbij alles binnen het bedrijfsnetwerk zit. In een hybride context waarbij gebruikers overal werken, applicaties in meerdere omgevingen draaien en data tussen private en publieke laag beweegt, volstaat dat model niet meer.

Moderne alternatieven zoals SASE (Secure Access Service Edge) integreren netwerkconnectiviteit en beveiliging in één platform. In plaats van al het verkeer terug te sturen naar een centraal punt voor inspectie wordt beveiliging toegepast op het punt waar de gebruiker of het systeem zich bevindt. Het resultaat is betere performantie, minder complexiteit en een consistenter beveiligingsniveau over alle omgevingen heen.

Als CIO of IT-manager die een hybride architectuur bouwt of moderniseert, is de keuze van het onderliggende netwerkmodel een strategische beslissing die je best vroeg in het traject neemt, niet pas als de prestatie- of beveiligingsproblemen zich melden.

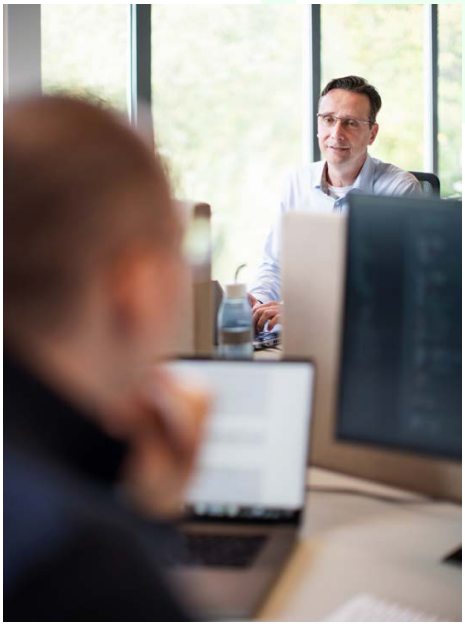
Drie minimumvereisten voor de netwerklaag in een hybride omgeving

Encryptie van data in transit
Alle communicatie tussen private en publieke laag moet versleuteld zijn, ook op interne verbindingen die “veilig genoeg” lijken.

Netwerksegmentatie
Verschillende omgevingen, applicaties en gebruikersgroepen horen in afzonderlijke netwerksegmenten met expliciete toegangsregels. Dat beperkt de impact van een beveiligingsincident tot het getroffen segment.

End-to-end monitoring
Netwerkmonitoring die stopt aan de grens van de on-premise omgeving, creëert blinde vlekken. Monitoring moet de gehele hybride omgeving bestrijken, met centrale correlatie van events over alle segmenten heen.

Compliance en datasoevereiniteit: structurele garanties versus contractuele beloftes



Voor compliance — of het nu gaat om GDPR, NIS2 of sectorspecifieke regelgeving — is het cruciaal dat de hybride architectuur traceerbaar en auditeerbaar is. Welke data zit waar? Wie had er toegang? Hoe wordt de dataflow gemonitord?

NIS2 voegt voor organisaties in essentiële sectoren een bijkomende laag toe: de richtlijn stelt concrete eisen aan de beveiliging van de volledige supply chain, inclusief cloud service providers. Als CIO ben je dus niet alleen verantwoordelijk voor je eigen omgeving, maar ook voor de keuzes van de partners die deel uitmaken van je IT-keten.

Datasoevereiniteit verdient bijzondere aandacht. Bij een Belgische of Europese cloud hosting partner is de controle over de datalocatie structureel gewaarborgd: architectureel, niet enkel contractueel. Dat onderscheid is relevant geworden in het licht van het Schrems II-arrest en de aanhoudende spanning rond de extraterritoriale werking van Amerikaanse wetgeving zoals de CLOUD Act.

Clouddiensten van Amerikaanse providers die fysiek in Europa draaien, bieden geen absolute bescherming tegen toegang door Amerikaanse autoriteiten. Voor organisaties met gevoelige data of strikte compliance-vereisten is dat geen theoretisch risico maar een reëel juridisch vraagstuk dat je expliciet moet bekijken bij de keuze van een cloud partner.

CONCLUSIE

Beveiliging in een hybride cloudomgeving is geen technisch eindpunt maar een doorlopend proces. De organisaties die het goed doen, behandelen IAM, netwerkarchitectuur en compliance niet als drie afzonderlijke projecten, maar als drie dimensies van één coherente beveiligingsstrategie, die bovendien meeschaalt naarmate de omgeving evolueert.

De partner die je kiest voor het beheer van je hybride of private cloudomgeving, is ook je partner in die beveiligingsstrategie. De kwaliteit van die samenwerking (de transparantie, de certificeringen, de lokale aanwezigheid) bepaalt mee hoe stevig dat fundament is.

HOOFDSTUK 4

Managed private & hybride cloud: wat je als CIO of IT-manager moet weten

Er is een paradox in de manier waarop veel organisaties omgaan met hun cloudinfrastructuur.

Ze investeren in een private of hybride omgeving om meer controle te krijgen, maar besteden vervolgens een disproportioneel deel van hun IT-capaciteit aan het dagelijkse beheer van die omgeving. Updates uitrollen, alerts opvolgen, performance monitoren, incidenten afhandelen, back-ups valideren: het zijn taken die essentieel zijn, maar die weinig strategische waarde toevoegen.

Managed cloud lost die paradox op. Niet door de controle weg te nemen, maar door het beheer van de infrastructuurlaag te delegeren aan een partner met de juiste expertise, zodat je interne team zich kan richten op wat er werkelijk toe doet.

Het échte verschil: capaciteit versus diepgang

De keuze tussen managed en self-managed cloud is voor de meeste middelgrote IT-organisaties geen principiële vraag, maar een capaciteitsvraag. Niet of het intern kan, maar of het intern vol te houden is.

Infrastructuurbeheer vereist actuele kennis over een brede waaier van domeinen: hypervisors, storage, netwerken, beveiliging, monitoring, compliance. Die breedte combineren met voldoende diepgang om incidenten snel en correct op te lossen (en dat ook ‘s nachts en in het weekend) is voor een IT-team van beperkte omvang structureel onhaalbaar. Niet omdat de mensen niet bekwaam zijn, maar omdat de verantwoordelijkheid te breed is.

Een bijkomende dimensie die vaak over het hoofd wordt gezien: de leercurve bij platformtransities. Organisaties die migreren van VMware naar een alternatieve hypervisorlaag — een traject dat steeds meer CIO's bewust overwegen vanwege de sterk gestegen licentiekosten — onderschatten hoeveel interne kennis daarvoor nodig is. Een managed partner die die transitie al meerdere keren heeft begeleid en de nieuwe omgeving dagelijks beheert, verkort die curve aanzienlijk en verlaagt het operationele risico in de kwetsbare periode net na de migratie.

De meest tastbare impact van managed cloud op een IT-team is niet de tijdsbesparing op papier, maar de mentale rust die het geeft. Wanneer monitoring, back-upvalidatie en incidentrespons zijn overgedragen aan een partner, verandert de dagelijkse werking van het team fundamenteel. Projecten die jarenlang op de backlog bleven staan komen opnieuw in het vizier. De energie die naar reactief beheer ging, kan worden ingezet voor migraties, modernisering of de uitrol van nieuwe diensten.

KPI's die ertoe doen

Een goed managed cloud-contract is geen vage afspraak over "goede service". Het is een set van meetbare engagementen die worden opgevolgd en gerapporteerd.

Uptime en beschikbaarheid

Een SLA van 99,9% klinkt hoog, maar betekent in de praktijk minder dan negen uur downtime per jaar. Weet wat er in jouw SLA staat, en weet ook wat erbuiten valt: gepland onderhoud, force majeure, incidenten veroorzaakt door de klant zelf. Die nuances bepalen de werkelijke waarde van de garantie.

Performantie

Worden de afgesproken performantieparameters gehaald? Worden afwijkingen proactief gesignaleerd en gecorrigeerd, of pas reactief na een klacht? Een goede managed services partner rapporteert structureel, niet alleen als er iets misgaat.

Beveiliging:

Hoe snel worden patches uitgerold? Hoe wordt er gereageerd op security-alerts? Worden penetratietests en vulnerability scans ingepland? De volwassenheid van je managed services partner op vlak van security bepaalt mee de volwassenheid van je eigen omgeving.

Drie absolute aandachtspunten voor CIO's en IT-managers

1 De kloof tussen SLA en werkelijke responsiviteit

Evalueer een managed services partner niet alleen op de papieren beloftes van de SLA, maar ook op de praktijk. Stel concrete vragen: hoe snel wordt een incident écht opgepakt? Is er lokale aanwezigheid of werkt alles remote? Zijn escalatieprocedures duidelijk en gedocumenteerd? Wat zeggen bestaande klanten? Lokale ondersteuning — iemand die je kan opbellen en die desnoods ter plaatse komt — is een onderscheidende factor die in de meeste SLA's niet zichtbaar is, maar in crisissituaties wel degelijk het verschil maakt.

2 Exit-strategie en portabiliteit

Een vraag die zelden wordt gesteld bij de keuze van een managed partner: wat als we ooit willen wisselen? Vendor lock-in is niet alleen een risico bij public cloud. Ook managed private cloud kan tot afhankelijkheid leiden als de beheerde omgeving steunt op propriëtaire tooling of gesloten platformen. Een omgeving gebouwd op open standaarden geeft je structureel meer portabiliteit dan een omgeving die vastgeknoopt is aan de toolset van één leverancier. Maak van portabiliteit een expliciete eis bij het selecteren van een platform en partner, niet een bedenking achteraf.

3 Transparantie over de onderliggende infrastructuur

Managed cloud betekent niet dat je als CIO niets hoeft te weten over de laag die voor je wordt beheerd. Het betekent dat je er niet dagelijks mee bezig hoeft te zijn. Dat is een belangrijk onderscheid. Vraag bij elke managed services partner naar inzicht in de onderliggende infrastructuur: waar staat jouw data fysiek? Op gedeelde of exclusieve hardware? In welk datacenter? Welke redundantie is ingebouwd? En hoe verhoudt zich dat tot jouw compliance-vereisten? Een partner die die transparantie biedt, en liefst ook de bijhorende certificeringen zoals ISO 2700, geeft je de basis om die vragen ook richting je eigen management en auditors te beantwoorden.

CONCLUSIE

De ROI van managed cloud is reëel, maar vraagt een eerlijke berekening. Aan de kostenzijde staat de factuur van de partner. Aan de opbrengstzijde staan de interne uren die vrijkomen, de hogere uptime die operationele continuïteit garandeert, de snellere incidentrespons die schade beperkt, en het risico dat niet gerealiseerd wordt omdat monitoring en patching structureel worden uitgevoerd.

Voor de meeste organisaties is de financiële businesscase positief. Maar de waarde van gemoedsrust en operationele focus is minstens even reëel, ook als die niet in een spreadsheet past.

HOOFDSTUK 5

Cloudmigratie: succesfactoren & valkuilen bij private & hybride trajecten

Een cloudmigratieproject slaagt of faalt grotendeels vóór de eerste server wordt overgezet. De technische uitvoering is relatief behapbaar. Wat migraties complex maakt, zijn de afhankelijkheden die niemand volledig had gedocumenteerd, de applicaties die anders reageren dan verwacht in een nieuwe omgeving, en de afstemming tussen IT en de rest van de organisatie die onvoldoende was voorbereid.

Een gestructureerde aanpak is geen garantie voor een perfecte migratie, maar het is het meest betrouwbare middel om de risico's te beheersen.

1 inventaris en voorbereiding

De eerste en meest onderschatte stap van elk migratietraject is een grondige inventaris van de bestaande omgeving. Dat klinkt vanzelfsprekend, maar de praktijk leert dat de meeste IT-omgevingen minder goed gedocumenteerd zijn dan aangenomen.

Welke servers draaien welke workloads? Welke applicaties communiceren met welke andere systemen? Welke afhankelijkheden zijn er met externe diensten, on-premise hardware of specifieke netwerkconfiguraties? Zijn er applicaties met hardcoded IP-adressen of servernamen die bij een migratie direct zullen breken?

Een aandachtspunt dat in de inventarisfase vaak ontbreekt: softwarelicenties en hypervisor-afhankelijkheden. Sommige software, in het bijzonder Microsoft-producten zoals Windows Server en SQL Server, kent licentievoorwaarden die afhankelijk zijn van het onderliggende virtualisatieplatform. Een migratie van VMware naar een alternatieve hypervisor kan daardoor licentietechnisch gevolgen hebben die pas zichtbaar worden als de factuur binnenkomt of de software-audit plaatsvindt. Breng dit in kaart vóórdat de architectuurkeuzes worden gemaakt, niet erna.

Een goede inventaris brengt ook in kaart hoe kritiek elke workload is. Welke systemen zijn bedrijfskritisch en mogen geen downtime hebben? Welke kunnen tijdelijk offline worden gezet? Die classificatie bepaalt de volgorde en de aanpak van de migratie.

2

architectuur-keuzes en plannings-afstemming

Op basis van de inventaris wordt de doelarchitectuur bepaald. Welke workloads gaan naar de private cloud? Welke worden in een hybride model opgezet? Zijn er systemen die eerder in aanmerking komen voor rationalisatie of vervanging dan voor migratie?

De planningsafstemming overstijgt de IT-afdeling. Business stakeholders moeten weten wanneer bepaalde systemen tijdelijk minder beschikbaar zijn. Externe leveranciers of partners die afhankelijk zijn van bepaalde systemen moeten worden geïnformeerd. Migratievensters moeten worden afgestemd op de bedrijfscyclus: een migratie plannen tijdens de drukste maand van het jaar is een risico dat eenvoudig te vermijden is.

3

integratie met bestaande systemen

Migratie naar private of hybride cloud betekent zelden een volledige breuk met de bestaande omgeving. Er zijn legacy-systemen die blijven draaien, on-premise hardware die niet wordt vervangen, en externe koppelingen die moeten blijven werken.

De integratie van de nieuwe cloudomgeving met wat overblijft, vereist aandacht voor netwerkconfiguratie, authenticatie en toegangsbeheer, en de consistentie van monitoring en logging over de volledige omgeving. Een hybride omgeving die niet coherent wordt gemonitord, creëert blinde vlekken die pas zichtbaar worden bij een incident.

4

testen, downtime-management en rollback

Geen migratie mag in productie worden gezet zonder grondig te zijn getest. Performance-tests valideren of de nieuwe omgeving de verwachte belasting aankan. Functionele tests bevestigen dat applicaties zich gedragen zoals verwacht. En voor kritische systemen moet er een gedocumenteerd rollback-scenario zijn: een plan om terug te keren naar de oorspronkelijke omgeving als de migratie onverwachte problemen veroorzaakt.

Downtime management is een aparte discipline. Voor systemen die niet offline mogen, bestaan technieken zoals live migratie of parallelle werking van oud en nieuw systeem gedurende een overgangsperiode. De keuze voor de aanpak hangt af van hoe kritiek een systeem is en de technische mogelijkheden van de betrokken applicaties.

5

documentatie, kennisover-dracht en training

Een migratie is pas volledig afgerond wanneer het interne team de nieuwe omgeving begrijpt en zelfstandig kan beheren, tenminste op het niveau dat afgesproken is. Documentatie van de architectuur, de configuratiekeuzes en de beheerprocessen is geen luxe, maar een vereiste voor operationele continuïteit.

Training en kennisoverdracht verdienen expliciete tijd in de projectplanning. Niet een cursus van een halve dag, maar een gestructureerd traject waarbij het interne team actief betrokken is bij de configuratie en inrichting, vragen kan stellen, en vertrouwdheid opbouwt met de nieuwe omgeving vóór die in productie gaat.

De rode draad: communicatie en verwachtingen afstemmen

De valkuilen in cloudmigraties zijn zelden puur technisch. Ze zijn het gevolg van onduidelijke verwachtingen, onvoldoende communicatie tussen IT en business, en een planning die te optimistisch was over de complexiteit van de afhankelijkheden. Een partner die niet alleen de technische uitvoering op zich neemt, maar ook helpt bij de voorbereiding, de afstemming en de kennisoverdracht, maakt het verschil tussen een migratie die onopgemerkt verloopt en één die lang wordt herinnerd.

CONCLUSIE

Een cloudmigratie is geen project, het is een verandertraject. De technologie is beheersbaar. De complexiteit zit in de afhankelijkheden, de communicatie en de verwachtingen die je vooraf al dan niet hebt afgestemd.

Als CIO's of IT-managers volg je dit traject beter niet alleen. Kies een partner die de technische uitvoering beheerst, maar ook begrijpt hoe een organisatie werkt: hoe je draagvlak creëert, hoe je stakeholders informeert, en hoe je een migratievenster kiest dat de business zo weinig mogelijk raakt.

De beste migraties zijn de migraties die niemand opvallen. Niet omdat er niets is veranderd, maar omdat alles zo goed was voorbereid dat de overgang vanzelfsprekend aanvoelde. Dat is het doel. En het is haalbaar, met de juiste aanpak.

HOOFDSTUK 6

Business continuity & compliance in cloud hosting: wat je als CIO of IT-manager moet weten

Cloud hosting is niet alleen een technologische keuze. Het is een risicobeslissing. Welke risico's accepteer je? Welke draag je over aan een partner? En welke zijn zo kritisch dat ze structureel moeten worden beperkt, ongeacht de kostprijs?

De vragen die ertoe doen zijn niet hoeveel IOPS de storage haalt, maar wat er gebeurt als een datacenter uitvalt, wie er aansprakelijk is bij een datalek, en hoe snel kritische processen kunnen worden hersteld na een incident. CIO's en IT-managers die cloud hosting vanuit die risicolens beoordelen, stellen zichzelf en hun partners structureel betere vragen en krijgen ook betere antwoorden.

Redundantie en failover: architect voor het slechte scenario

Hoge beschikbaarheid begint bij de architectuur, niet bij de SLA. Redundantie op elk niveau (stroomvoorziening, netwerkconnectiviteit, storage, rekencapaciteit) zorgt ervoor dat het uitvallen van één component niet leidt tot een totale uitval van de omgeving.

Voor kritische workloads gaat dat verder dan interne redundantie. Failover naar een tweede locatie of omgeving, geautomatiseerd of handmatig te activeren, zorgt voor continuïteit ook bij een ernstig incident op de primaire locatie. RTO en RPO zijn de parameters die hier de toon zetten. Maar het is de businesscontext die bepaalt wat aanvaardbaar is, niet de IT-afdeling alleen.

Back-upstrategie: verder dan een dagelijkse kopie

Een back-up die nooit getest is, is geen back-up. In de praktijk blijkt regelmatig dat back-ups wel worden gemaakt, maar dat het herstelproces niet is gevalideerd. Een back-up is pas waardevol als het herstel werkt, snel genoeg is, en het juiste datapunt terugzet. Een robuuste back-upstrategie steunt op drie pijlers: de 3-2-1-regel (drie kopieën, twee media, één offsite), immutabiliteit (back-ups die niet kunnen worden aangepast of verwijderd, ook niet door een aanvaller met toegang tot de productieomgeving), en geregelde restore-tests, gedocumenteerd en opgevolgd.

De immutabiliteit van back-ups is in een context van toenemende ransomware-aanvallen geen nice-to-have maar een harde vereiste. NIS2 maakt de verwachting rond immutabele back-ups ook expliciet voor organisaties in essentiële en kritische sectoren. Maar ook buiten die sectoren is het een architectureel minimum geworden.

GDPR, NIS2 en datasoevereiniteit: verder dan de juridische checkbox

1 GDPR

GDPR is inmiddels al jaren van kracht en toch blijven er organisaties die cloud hosting benaderen zonder na te gaan waar hun data precies terechtkomt, hoe lang die wordt bewaard en wie er toegang toe heeft.

Die nalatigheid is een risico — niet alleen omdat boetes reëel zijn, maar omdat een datalek ook reputatieschade veroorzaakt die moeilijk te herstellen is.

2 NIS2

NIS2 voegt een extra laag toe voor organisaties in essentiële sectoren. De richtlijn stelt concrete eisen aan risicobeheer, incidentrapportering en de beveiliging van de supply chain — inclusief cloud service providers.

Dat laatste punt is cruciaal: als CIO ben je niet alleen verantwoordelijk voor je eigen omgeving, maar ook voor de keuzes van de partners die deel uitmaken van je IT-keten. Je moet kunnen aantonen dat je hosting provider voldoet aan de gestelde eisen — en dat vraagt om meer dan een contractuele clausule.

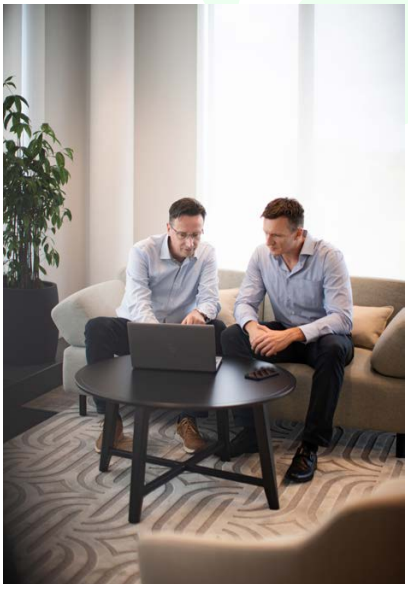
Vraag naar certificeringen (ISO 27001 is een gangbaar referentiepunt), auditrechten, en de concrete procedures bij een beveiligingsincident.

3 Datasoevereiniteit

Datasoevereiniteit is de derde dimensie, en een die aan belang wint. Bij een Belgische of Europese cloud hosting partner is de controle over de datalocatie structureel gewaarborgd: architectureel, niet enkel contractueel.

Dat onderscheid is relevant geworden in het licht van het Schrems II-arrest en de aanhoudende spanning rond de extraterritoriale werking van Amerikaanse wetgeving zoals de CLOUD Act. Amerikaanse clouddiensten die fysiek in Europa draaien, bieden geen absolute bescherming tegen toegang door Amerikaanse autoriteiten.

Voor organisaties met gevoelige data of strikte compliance-vereisten is dat geen theoretisch risico maar een reëel juridisch vraagstuk dat expliciet moet worden geadresseerd in de keuze van een cloud partner.



CONCLUSIE

De meest waardevolle mindshift die je als CIO kan maken rond cloud hosting, is de overgang van een technische naar een risicogebaseerde benadering. De vraag is niet alleen “werkt het?”, maar “wat als het niet werkt?”, “hoe snel zijn we terug operationeel?” en “kunnen we aantonen dat we correct handelden?”

Organisaties die die vragen beantwoord hebben en de antwoorden hebben vertaald in een architectuur, een beheermodel en een set van afspraken met een partner, zijn niet alleen technisch beter beschermd. Ze zijn ook beter voorbereid op de strategische, juridische en reputationele dimensies van een wereld waarin IT-continuïteit steeds vaker een boardroom-onderwerp is.

SLOTBESCHOUWING

Private en hybride cloud zijn relevanter dan ooit

Dit ebook is geen pleidooi voor één specifieke technologie of één bepaald model. Het is een uitnodiging om de juiste vragen te stellen voordat er beslissingen worden genomen.

Welke workloads horen thuis in een private omgeving? Waar heeft hybride cloud meerwaarde? Wat zijn de werkelijke kosten en risico's van uw huidige set-up? En welke partner helpt je niet alleen bij de technische uitvoering, maar ook bij het denken?

Bij Epact begeleiden we organisaties bij alle vragen: van intake en sizing tot implementatie, beheer en compliance.

Met onze eCloud-omgeving, gebouwd op het open source Proxmox-platform, bieden we een volwaardig, schaalbaar en betaalbaar alternatief voor wie zijn cloudstrategie wil bouwen zonder afhankelijk te zijn van één grote vendor. Beheerd vanuit België, door een team dat je kent en dat je kan bellen. Niet als product van de plank. Wel als oplossing op maat, met de langetermijnrelatie die hoort bij infrastructuurkeuzes die er toe doen.

Benieuwd wat dat concreet betekent voor jouw omgeving? Neem contact op! We denken graag mee.

Wil je weten welke of private of hybride cloud past in jouw cloudstrategie?

De vraag is niet langer “public of private cloud?”, maar “welke workloads passen waar?” Een weloverwogen private cloudomgeving als kern van je strategie, aangevuld met public cloudcapaciteit waar dat zinvol is, geeft je het beste van beide werelden. Niet als compromis. Wel als bewuste architectuurkeuze.

Neem contact op met ons

Voor een vrijblijvend assessment of technische deep dive. Zo maak je geen sprong in het diepe, maar een onderbouwde keuze.

Christof Ugau
Managing Partner

christof.ugau@epact.be

Leo Chang
Business Developer

leo.chang@epact.be

EPACT