

Hoe kies ik een datacenter?

De Datacenter Checklist



De keuze voor een datacenter hangt natuurlijk af van veel dingen. Om het iets makkelijker te maken, geven we de dingen die je moet overwegen.

Locatie

Bij het kiezen van een datacenter is het belangrijk een datacenter te kiezen die past bij het bedrijf. Wanneer het bedrijf lokaal opereert en over eigen engineers beschikt, is het verstandig om te kiezen voor een datacenter die fysiek dichtbij is. Indien het bedrijf internationaal opereert of tijdkritische diensten heeft draaien, is latency belangrijk en de afstand tot belangrijke internetknooppunten. Dan is fysieke nabijheid tot Amsterdam AMS-IX, of een ander internetknooppunt, belangrijk bij de locatiekeuze. Wereldwijde of lokale spreiding kan belangrijk zijn indien je graag alles bij één datacenter onderbrengt, in tegenstelling tot de keuze van spreiding in leveranciers.

Het maakt echter ook uit waar de operator van het datacenter vandaan komt, en met welke andere datacenters deze in contact staat. Wil je je gegevens in de cloud hebben, maar vanwege de wetgeving absoluut binnen de landsgrenzen, bijvoorbeeld? Dan moet je de zekerheid hebben dat de gekozen cloud ook echt fysiek in Nederland is ondergebracht.

Eisen beschikbaarheid

De beschikbaarheidseisen zijn daarnaast belangrijk. Een 100-procentgarantie is niet te geven, maar het risico kan met de juiste techniek wel worden geminimaliseerd. Vaak is er een relatie tussen techniek, prijs en trackrecord.

Wat zijn de kosten van downtime? Hoe is downtime verzekerd/boetes/SLA's? Mag gepland onderhoud downtime veroorzaken? Hoe redundant is het datacenter? Hoe redundant is de powerinfrastructuur? Heb je de mogelijkheid tot twinning bijvoorbeeld? Belangrijke vragen bij de keuze. Op dit punt is volledige transparantie cruciaal, ook waar het in het verleden gemaakte fouten betreft.

Eisen veiligheid

Welke voorwaarden worden gesteld aan de veiligheid? Zijn er eisen vanuit de verzekeraar of klanten? Wordt er 24x7 on-site security geëist of is monitoring voldoende omdat er geen

bedreigingsrisico van personeel bestaat? Dit zijn eisen die vanuit het bedrijf moeten komen. Maar je moet ook denken aan fysieke veiligheid. Een datacenter boven NAP zal in geval van een overstroming minder snel in de problemen komen dan een faciliteit in een polder. Dat hoeft overigens niet te betekenen dat het daadwerkelijke risico echt veel hoger ligt, maar het is een overweging.

Eisen brandveiligheid

Ook voor brandveiligheid worden vaak de eisen van de verzekeraar gehanteerd. Belangrijk blijft een tijdige detectie van brand en automatische blussing in kritische bedrijfsruimtes. Certificering van het systeem kan een kortingen opleveren gezien de impact wordt gelimiteerd als het risico van brand zich voordoet. Vroegtijdige rookmeldsystemen (apsiratie detectie systemen) zijn veel voorkomende systemen in datacenters die ervoor zorgen dat brand en rook tijdig worden ontdekt en gecontroleerd kan worden indien noodzakelijk. Denk echter ook aan de constructie van het pand. Een rack opgesteld in een grote hal kan wellicht eerder worden blootgesteld aan gevolgen die zich bij andere zaalgebruikers voordoen. Een risico hoeft zich dus niet altijd in de eigen hardware/racks voor te doen om tot een nadelige uitval te leiden. Behalve de inrichting van het datacenter is ook de vuurlast van een gebouw van belang. Hoe brandbaarder de materialen, des te groter het risico. Rook trekt zich niet zoveel aan van een hek, hoe effectief deze ook is tegen ongewenst bezoek.

Eisen dienstverlening

Biedt de dienstverlener/het datacenter aanvullende diensten die het bedrijf kan ondersteunen (technische ondersteuning, rack en stack, etc.) en is het datacenter

niet concurrerend met het eigen bedrijf (SaaS/PaaS-dienstverlening)? Een ander belangrijk aspect van dienstverlening is de integratie met huidige leveranciers (fiber-leverancierconnectie met datacenter, connectie met cloud-aanbieders bijvoorbeeld Microsoft Azure, Amazon). Overigens heeft Nederland een uitstekend fibernetwerk, en de komst van virtuele netwerken als DCSpine hebben de flexibiliteit verhoogd.

Flexibiliteit van het datacenter en meerkosten

Het kiezen voor een strak gestandaardeerde, veelal internationale, datacenterketen kan in eerste instantie interessant en makkelijk lijken. Maar niet alle grote ketens zullen even flexibel omgaan met mogelijke extra wensen, of zullen mogelijk extra services in rekening willen brengen buiten je huidige contract. Vaak wordt ook een minimaal aantal racks vereist. Zorg daarom dat je ook goed nadenkt over welke diensten jij verwacht van je datacenter. Nu en in de toekomst.

Bezoek het datacenter altijd

Een bezoek aan het gebouw laat beveiligingslagen zien en striktheid van de beveiliging. Een kritisch bezoek geeft een goede indruk. Tijdens een bezoek moet het gevoel van het datacenter goed zijn en moet worden gekeken (voor zover mogelijk) indien belofde/benodigde aspecten daadwerkelijk aanwezig zijn. Luister ook goed naar ervaringen van andere klanten over flexibiliteit, technische advisering en service van het datacenter.

Externe certificering

Dienstverleners kunnen externe certificeringen verkregen hebben. Deze kunnen van belang zijn voor de eindklanten van het bedrijf en deze laten zien dat het datacenter voldoet aan bewezen standaarden.

Belangrijke certificering vanuit de ISO/NEN:

- Interne informatieveiligheid -> ISO 27001 / NEN 7510
- Kwaliteitsbeheer -> ISO 9001
- Milieumanagement -> ISO 14001

Marktspecifieke certificeringen zijn echter ook van groot belang. De betaal-branche werkt voor transacties bijvoorbeeld met PCI-DSS. De datacentermarkt hecht veel waarde aan de TIER-klassificaties van het Uptime Institute, en aan TIA 942, voor redundantie en uptimegarantie.

Derdenverklaringen

Derdenverklaring/certificering komt van een externe auditor die de inrichting beoordeelt, en de werking van processen en procedures tijdens het afgelopen jaar toetst. Dit wordt verwerkt in een SOC1-, SOC2- of SOC 3-rapport. Een datacenter kan goede procedures hebben en mooie techniek, als blijkt dat deze niet hebben gewerkt over een periode geeft dit geen vertrouwen en blijkt dus dat het datacenter zijn processen niet goed op orde heeft. Voor het toetsen van werking over een periode zijn rapporten als SOC1/ SOC2 belangrijk als ondersteunend bewijs bovenop referenties.