



Data Centers, Algemeen

Door Eric Lavrijsen

LGSR Experts in Green Data Center Solutions

White Paper 20 January 2009

SAMENVATTING

Toekomstvastheid van Datacenters en Datacenters is steeds meer een vereiste in de snel veranderende ICT technologie. Veel van de in gebruik zijnde ruimtes voldoen vaak ongemerkt niet meer aan de huidige eisen met betrekking tot flexibiliteit en continuïteit.

Om tot een bedrijfszekere en toekomstvast datacenter te komen, dient voldoende aandacht geschonken te worden aan een groot aantal niet-ICT-gerelateerde facetten zoals bouwkundige, veiligheids-, koelings-, preventie- en energievoorzieningen. Pas wanneer al deze elementen in een juist evenwicht zijn gebracht, zal het Datacenter de nodige bedrijfszekerheid en flexibiliteit kunnen bieden om ook op de lange termijn zijn toekomstvastheid te behouden en de gedane investeringen optimaal te laten renderen.

In deze white paper wordt aandacht besteed aan de volgende zaken:

- Betrouwbaarheid van het Datacenter en de risico's waarmee men rekening dient te houden.
- Aantal belangrijke aandachtsgebieden waar aandacht aan besteed dient te worden om tot een toekomstvast oplossing te komen.
- Het "Room in Room"-concept waarbij gebruikt gemaakt wordt van standaard datacenters die kant-en-klaar op locatie worden aangeleverd.
- De LCC Green Server Room benadering om tot een toekomstvast datacenter te komen.

Inhoudsopgave

SAMENVATTING	2
1 Beschikbaarheid	4
1.1 Uptime & downtime.....	4
1.2 Calamiteiten	4
1.3 Risico's	5
1.4 Beschikbaarheid	5
1.5 Klasse indelingen	6
1.6 Design & Engineering	6
2 Aandachtsgebieden	7
2.1 Klimaatbeheersing	7
2.1.1 Temperatuur en luchtvochtigheid	8
2.1.2 Distributie van koele lucht	8
2.1.3 High-Density koeltechniek.....	9
2.2 Power Management.....	9
2.2.1 Trend: het vermogen neemt toe.....	9
2.2.2 Stroomstoringen	9
2.2.3 UPS power supply	10
2.2.4 NSA noodstroomvoorziening	10
2.3 Brandbeveiliging	10
2.3.1 Branddetectie	11
2.3.2 Brandblussing	11
2.4 Overige controlesystemen.....	11
2.4.1 Toegangscontrole	12
2.4.2 Camerabewaking	12
2.4.3 Multifunctionele toepassingen	12
2.5 Verhoogde computervloeren	13
2.5.1 Functies van computervloeren	13
2.5.2 Ontwerp en installatie	13
2.5.3 Vloerbelasting	14
2.6 Gestructureerde bekabeling	14
2.6.1 Behoeftebepaling	14
2.6.2 Toekomstvastheid.....	14
2.6.3 Redundantie	15
2.6.4 Garanties.....	15
2.6.5 Efficient beheer van de bekabelinginfrastructuur	15
3 De LGSR aanpak.....	16
3.1 Voordelen van de oplossing 'datacenters'.....	17
4 Samenwerken met LGSR.....	17
5 Complementaire diensten.....	17

1 Beschikbaarheid

In de huidige 24/7-cultuur is beschikbaarheid de sleutel. De continuïteit van de onderneming is mede afhankelijk van de beschikbaarheid van faciliteiten, medewerkers en informatie. Vanwege de steeds sneller evoluerende technologie en de groeiende informatiebehoefte is er een groeiende vraag naar verhoogde IT-prestaties en een hogere beschikbaarheid en continuïteit van de ICT Infrastructuur en datacenters. Managers zien zich geconfronteerd met een nieuwe reeks hindernissen, ten einde een ICT-omgeving te creëren met voldoende flexibiliteit en betrouwbaarheid om het primaire bedrijfsprocessen te kunnen waarborgen.

Momenteel richten veel ondernemingen zich op het upgraden of vervangen van de infrastructuur en het datacenter. Daar zijn een aantal redenen voor: een groeiende vraag naar verhoogde IT-prestaties, een noodzakelijke hogere beschikbaarheid en consolidatie van datacentra.

Een goed en doordacht ingerichte datacenter is flexibel en biedt ruimte voor verdere groei. De ruimte waar de ICT apparatuur staat opgesteld, heeft geheel eigen specificaties en verdient daarom speciale aandacht bij het ontwerp en beheer van de voorzieningen. Uit kostenoverwegingen lijkt het misschien aantrekkelijk om integratie met de bestaande gebouwinfrastructuur te zoeken, maar deze benadering zal zaken als betrouwbaarheid, beschikbaarheid, continuïteit en veiligheid negatief beïnvloeden.



Het is vrijwel onmogelijk om een standaardoplossing te bepalen, omdat vele factoren het ontwerp beïnvloeden. Een overzicht van de risico's geeft aan dat er sprake is van een absolute noodzaak speciale maatregelen te treffen om het Datacenter te optimaliseren om het primaire bedrijfsproces te kunnen waarborgen.

1.1 Uptime & downtime

Downtime komt de laatste jaren steeds vaker voor. Voor 35% van alle bedrijven ligt de maximale toelaatbare downtime van het netwerk onder de 3 uur. In het jaar 2002 had 74 procent van de Nederlandse ondernemingen ermee te maken. Bij 22% van alle bedrijven veroorzaakt 1 minuut downtime al torenhoge kosten. Het grootste deel van deze uitvallen duurde echter korter dan 4 uur, desondanks gingen getroffen bedrijven hierdoor failliet. Een onderzoek van Daimler- Chrysler naar faillissementen door falende ICT laat zien dat bijna een kwart van de bedrijven na één tot drie dagen ICT-uitval failliet ging en 44 procent na drie tot zeven dagen. Een uptime garantie van 99,99 procent leidt tot een downtime die kan oplopen tot 53 minuten per jaar en een uptime garantie van 99,9999 procent beperkt de downtime tot 32 seconden per jaar. De investeringen die hiervoor gedaan moeten worden zijn vaak hoog, maar wegen niet op tegen het risico dat men loopt.

1.2 Calamiteiten

Downtime is een uiterst kostbare gebeurtenis, dus het vermijden ervan krijgt steeds meer prioriteit. Elke organisatie kan echter getroffen worden door externe calamiteiten.

Deze calamiteiten kunnen komen in de vorm van brand, stroomstoringen, computervirussen, etc. Een calamiteit verstoort het bedrijfsproces ernstig en de meeste organisaties hebben dan ook een diversiteit aan rampenplannen klaarliggen. Echter deze rampenplannen richten zich nauwelijks op de facilitaire ICT-infrastructuur.

Consequenties van een computeruitval zijn:

- Gegevensverlies
- Productieverlies
- Financiële verliezen
- Verlies van "omzet"

Bij het bepalen van de optimale beschikbaarheid van uw datacenter dient er altijd een balans gevonden tussen kosten van een storing en de investeringskosten in de preventieve maatregelen.

1.3 Risico's

Tegenwoordig kan geen enkel bedrijf meer zonder een goed beveiligd datacenter. In het datacenter wordt alle belangrijke bedrijfsinformatie opgeslagen. Hierdoor wordt deze ook wel het hart van het bedrijf genoemd. Deze ruimte dient natuurlijk goed beveiligd te zijn.

Het belangrijkste risico is het gehele of gedeeltelijke uitvallen ten gevolge van:

- Brand buiten het Datacenter(70% van de branden ontstaan elders in of buiten het gebouw)
- Brand binnen het datacenter
- Bijkomende schade naast de directe brandschade
 - o Waterschade t.g.v. de blusacties
 - o Schade t.g.v. de corrosieve gassen die vrijkomen bij een brand
 - o Vocht migratie door de muren. Beton bestaat voor 10-15 procent uit vocht en dat komt er bij een brand aan de 'koude' kant uit. Bij een gemiddeld Datacenter kan dit oplopen van 220 tot 870 liter water met als gevolg kortsluiting. Dit geldt ook voor betonnen muren met brandwerendheid van RF60 (minimaal 60 minuten brandveilig)
- Elektrische problemen, zoals stroomuitval, overspanning en bliksem. Het Nederlandse stroomnet heeft een leveringsgarantie van 99,9 %, oftewel bedrijven hebben daardoor een uptime garantie van 99,9%. Vaak is dit niet toereikend omdat dit een downtime van ongeveer 9 uur per jaar betekent.

Deze oorzaken zijn bij elkaar goed voor 68,1 procent van alle schades. Vandalisme en diefstal spelen ook een rol maar een veel kleinere.

1.4 Beschikbaarheid

Daarnaast wordt de omvang van het uitvalrisico ook nog bepaald door:

- De plaats van de ruimte binnen het pand. Zonder voorafgaande zorgvuldige analyse ontstaan grotere risico's, omdat deze ruimtes vaak eenvoudig toegankelijk zijn.
- Onbeheerste aanwas apparatuur. Vaak komt het Datacenter door het groeiproces binnen organisaties steeds voller te staan met apparatuur. De gevolgen hiervan zijn:
 - o Een steeds slechter functionerende koeling.
 - o Toename van kabeldoorvoeren die niet altijd meer even goed brand- en gasdicht zijn afgewerkt.

- o Niet meer optimaal functionerende traditionele branddetectie, zodat (smeul)branden in het datacenter niet meer op tijd worden opgemerkt.
- Doordat er vaak ook waterleidingen door de ruimte lopen is er onvoldoende bescherming tegen (blus)water.

1.5 Klasse indelingen

Regelmatig ontstaat verwarring over hoe de betrouwbaarheid van een datacenter uitgedrukt moet worden. De meest gangbare manier is het bepalen van de beschikbaarheid van het datacenter. De beschikbaarheid is een percentage van de "uptime" en wordt berekend door het maken van een computersimulatie, waarbij onder meer de faalkans van de kritische componenten als parameter wordt ingevoerd.

Het is niet altijd direct nodig om uw gebouwinfrastructuur door een computersimulatie te laten doorrekenen. Over het algemeen kan men terugvallen op gangbare industriestandaarden en de daarin omschreven klasse-indelingen (Tier).

	Tier I	Tier II	Tier III	Tier IV
Building Type	Tenant	Tenant	Stand-alone	Stand-alone
Staffing shifts Staff/shift	None None	1 Shift 1/Shift	1+Shifts 1-2/Shift	"24 by Forever" 2+/Shift
Useable for Critical Load	100% N	100% N	90% N	90% N
Initial Build-out kW per Cabinet (typical)	<1kW	1-2 kW	1-2 kW	1-3 kW
Ultimate kW per Cabinet (typical)	<1 kW	1-2 kW	>3 kW ^{*,‡}	>4 kW ^{*,†}
Support Space to Raised- Floor Ratio	20%	30%	80-90+%	100+%
Raised-Floor Height (typical)	12 inches	18 inches	30-36 inches	30-42 inches
Floor Loading lbs/ft (typical)	85	100	150	150+
Utility Voltage (typical)	208, 480	208, 480	12-15 kV	12-15 kV
Single Points-of-Failure	Many + Human Error	Many + Human Error	Some + Human Error	Fire, EPO + Some Human Error
Representative Planned Maintenance Shut Downs	2 Annual Events at 12 Hours Each	3 Events Over 2 Years at 12 Hours Each	None Required	None Required
Representative Site Failures	6 Failures Over 5 Years	1 Failure Every Year	1 Failure Every 2.5 Years	1 Failure Every 5 Years
Annual Site-Caused, End-User Downtime (based on field data)	28.8 hours	22.0 hours	1.6 hours	0.8 hours
Resulting End-User Availability Based on Site- Caused Downtime	99.67%	99.75%	99.98%	99.99%
Typical Months to Plan and Construct	3	3-6	15-20	15-30
First Deployed	1965	1970	1985	1995

1.6 Design & Engineering

Beschikbaarheid van de ICT speelt nog altijd een doorslaggevende rol bij het waarborgen van de bedrijfscontinuïteit. Bij het ontwerpen van een ICT omgeving en ICT netwerk dient de nodige aandacht dan ook geschonken te worden aan het ontwerp en de inrichting van het datacenter. Deze ruimte is en blijft het zenuwcentrum van het netwerk en daarom dient bij het ontwerp gelet te worden op zaken zoals conditionering, brandbeveiliging, toegangscontrole, noodstroomvoorzieningen. De constructie van een datacenter moet direct goed gebeuren. Ook relatief kleine aanpassingen van een slecht uitgevoerde bouwkundige constructie leiden later tot grote problemen.

LCC Green Server Room heeft brede ervaring met het ontwerpen van datacenters en maakt in onderling overleg het beste ontwerp voor elke specifieke situatie. Het bouwkundig ontwerp begint met het gezamenlijk bepalen van een plattegrond. Hierbij wordt gelet op een efficiënte plaatsing van server cabinets, airconditioning, UPS en andere componenten. Ook een efficiënte plaatsing van kabelgoten wordt hierin meegenomen. Het bouwkundig ontwerp van een professionele datacenter dient aan een aantal richtlijnen te voldoen.

- Vaak worden in het Datacentersystemen geplaatst die speciale eisen stellen aan de bouwkundige voorzieningen, zoals isolatie ten behoeve van de airconditioning, voorzieningen voor de blusinstallatie.
- De wanden en deuren dienen minimaal 60 minuten brandwerend te zijn.
- Sparingen dienen luchtdicht en brandwerend te worden afgesloten. Er zijn systemen beschikbaar die het mogelijk maken later eenvoudig kabels door te voeren.
- Door overdruk in de ruimte worden verontreinigingen buiten de ruimte gehouden.
- Er zijn wettelijke en mogelijk ook Arbo regelingen waaraan de ruimte dient te voldoen, zoals vluchtwegen, verlichting, daglicht toetreding.
- De fysieke beveiliging van de ruimte kan vaak door eenvoudige maatregelen worden verbeterd.



2 Aandachtsgebieden

Om tot een bedrijfszekere en toekomstvaste datacenter te komen, dient integraal voldoende aandacht geschonken te worden aan een groot aantal niet ICT-gerelateerde facetten, zoals bouwkundige, veiligheids-, koelings-, preventie- en powervoorzieningen.

2.1 Klimaatbeheersing

De beschikbaarheid van iedere datacenter valt of staat met de klimaatbeheersing. De ICT apparatuur stelt voorwaarden aan de klimaatbeheersing om optimaal te kunnen functioneren. Europese richtlijnen geven aan dat er een maximale toegestane temperatuur en luchtvochtigheid bestaat voor het behoud van functionaliteit. Deze richtlijnen spelen ook een rol in verzekeringstechnische zaken met betrekking tot de in gebruik zijnde datadragers.

De klimaatbeheersing van het gebouw ook gebruiken voor het conditioneren van een datacenter is niet verstandig. De tegengestelde belangen tussen kantooromgevingen en

datacenter zijn lastig te combineren en leiden daardoor bijna automatisch tot gescheiden systemen.

2.1.1 Temperatuur en luchtvochtigheid

Het beheersen van de temperatuur en relatieve vochtigheid (RLV) is van essentieel belang voor een optimaal functioneren van ICT apparatuur. De ideale temperatuur in het Datacentervarieert van 18° C tot 25° C, de RLV mag variëren van 40% tot 60%. Te hoge temperaturen in een datacenter kunnen leiden tot verlies van data en of ongecontroleerde shutdown van het gehele systeem.

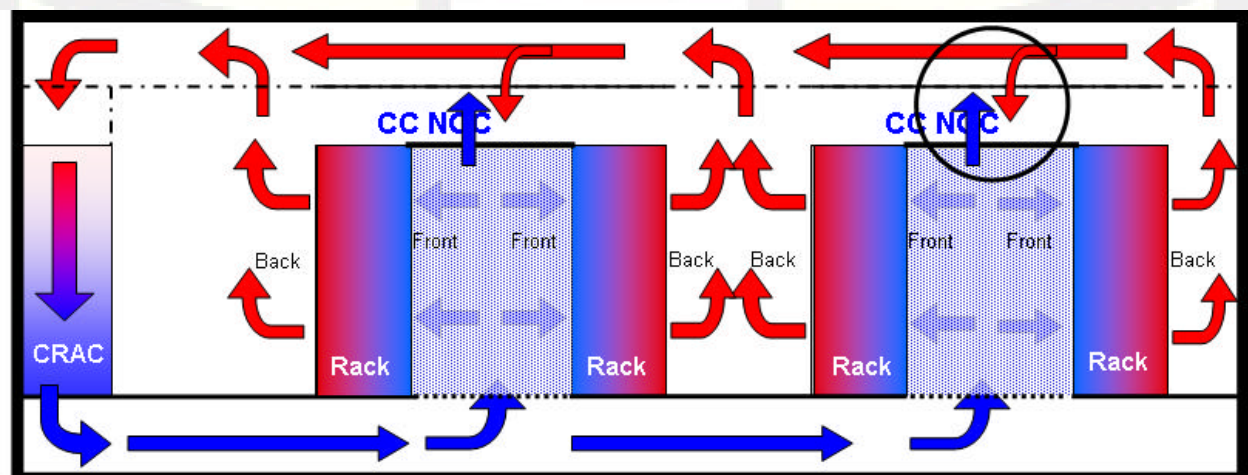
Lage relatieve vochtigheid kan leiden tot statische elektriciteit, resulterend in dataverlies en schade aan elektrische componenten. Hoge relatieve vochtigheid kan problemen veroorzaken door condensatie en corrosie van hardware en tapes.

2.1.2 Distributie van koele lucht

De beste distributie van de koele lucht vindt plaats door een systeem van downflow airconditioning units die de koele lucht onder de verhoogde vloer inblaast. Vervolgens zijn er twee systemen om de koele lucht naar de ICT apparatuur te voeren: ruimtekoeling of upflow cabinets.

Bij het ontwerp van een datacenter dient de airconditioning een integraal onderdeel te vormen van het totale ontwerp. Waarbij rekening gehouden dient te worden met onderstaande zaken:

- Het koelvermogen dient te zijn gerelateerd aan het elektrische vermogen van de apparatuur.
- Het zekerstellen van de beschikbaarheid van de airconditioning op (kosten)efficiënte wijze.
- Het goed op elkaar zijn afgestemd van o.a.
 - o de verhoogde vloer
 - o het type server cabinets
 - o Indeling van de ruimte
- Ook dient aandacht geschonken te worden aan een geoptimaliseerde monitoring en sturing van de airconditioning met luchtbehandelings en blussysteem.



Close Control airconditioning is meestal voordeliger dan comfort airconditioning om de volgende redenen:

- Comfort airconditioning verwijdert vocht uit de ruimte. Vervolgens dient de ruimte vaak weer te worden bevochtigd. Dit kost dubbele energie.
- Close Control airconditioning kan energie efficiënt werken door gebruik te maken van zogenaamde vrije koeling; hogere vloeistoftemperatuur gekoppeld aan groter koelvermogen.
- Lagere onderhoudskosten.

2.1.3 High-Density koeltechniek

De opmars van blade servers binnen het Datacenter heeft grote invloed op koelcapaciteit. Rack-koeling is de oplossing voor het steeds acuter wordende probleem van stijgende servercapaciteiten. De conventionele methoden van ruimte- of kastkoeling via verhoogde vloeren is voor de steeds krachtiger wordende servers niet meer toereikend.

Bij rack-koeling wordt de zijwand van een 19"-kast of een van de zijwanden tussen twee 19"-kasten vervangen door zogenaamde koel Packs. Daarin worden één, twee of drie lucht/lucht-waterwarmtewisselaars ondergebracht. De gekoelde lucht wordt direct voor elke serverrij geblazen en zorgt voor uitgebalanceerde warmtetechnische omstandigheden.

2.2 Power Management

Organisaties zijn steeds meer afhankelijk van de stroomvoorziening ten behoeve van de ICT apparatuur. Deze apparatuur vereist "schone" en continue elektrische voeding. Tegelijkertijd staat de betrouwbaarheid van de stroomvoorziening onder druk door een toenemende vraag en verdergaande privatiseringen.

Hoewel stroomstoringen breed worden uitgemeten in de media komen vaker er meer stroomstoringen voor dan men denkt, omdat de gevolgen niet altijd direct aan een stroomstoring worden toegeschreven.

2.2.1 Het vermogen neemt toe

De stroomconsumptie per rack/footprint in een datacenter is in de loop der tijd alleen maar toegenomen. Dit toegenomen stroomverbruik is een bedrijfseconomisch probleem voor de bestaande datacenters. Hetzelfde probleem geldt voor de koelcapaciteit. De koelcapaciteit voldoet dus ook vaak niet meer door de enorme toegenomen warmte-uitstoot per rack, hetgeen veroorzaakt wordt door het sterk toegenomen stroomgebruik.

Vrijwel alle compterruimtes zijn gebouwd op 16 Ampere stroomverbruik per rack. Deze 16 Ampere beperking is niet alleen een probleem m.b.t. de netstroom voeding, maar nog veel sterker bij de noodstroomvoorzieningen: (UPS, generators en schakelapparatuur).

De koelcapaciteit voor high density apparatuur is dus bij lange na niet toereikend.

2.2.2 Stroomstoringen

Men kan verschillende soorten storingen onderscheiden: overspanningen, te lage spanning, spanningsdalen, spanningspieken, onderbrekingen, transiënten, impulsen, elektrische ruis, harmonische vervuiling. De laatste twee storingen zijn eerder continu

van aard. Elektrische ruis heeft een frequentie van 5kHz en hoger. Deze ruis is gesuperponeerd op de basis sinusgolf en stelt eigenlijk zo geen probleem.

33% van alle computeruitval is het gevolg van netstoringen. 33% van alle bedrijven die een computeruitval ondervinden, hebben meer dan 24 uur nodig om de oorzaak te achterhalen.

Bedrijven ondervinden gemiddeld 10 maal per jaar een computeruitval. De gemiddeld benodigde tijd om weer operationeel te zijn bedraagt 4 uur. De benodigde tijd om een netwerk weer operationeel te krijgen kan tot 48 uur oplopen.

2.2.3 UPS power supply

Er zijn verschillende soorten UPS systemen die voor elke situatie betere of minder goede eigenschappen hebben. Voor alle UPS systemen geldt dat ze voorzien in de basisfunctie: het continu verzorgen van geconditioneerde elektrische voeding voor computerapparatuur.

Bij de keuze voor een UPS systeem dienen een aantal zaken in aanmerking te worden genomen:

- De plaats van de UPS in het elektrische systeem; lokaal, centraal of zone configuratie.
- Afhankelijk van de situatie ter plaatse kan de UPS zodanig geïnstalleerd worden dat de beschikbaarheid geoptimaliseerd wordt.
- De specificaties van de elektrische input en output.
- Het benodigde vermogen, rekening houdend met continu- en piekvermogens, dynamische fluctuaties van het stroomverbruik, de power factor van de UPS, etc.
- Harmonische vervuiling kan leiden tot storingen of overbelasting van het systeem.
- Mogelijkheid tot uitbreiding of verhuizing van het systeem.

2.2.4 NSA noodstroomvoorziening

Een noodstroom aggregaat verhoogt de beschikbaarheid aanzienlijk. Stroomstoringen die langere tijd duren worden door de noodstroom aggregaat opgevangen. Hierbij moet bedacht worden dat de airconditioning uitvalt als deze geen backupvoeding van een NSA heeft. Ervaring leert dat een standaard datacenter die volledig gevuld is met operationele ICT apparatuur, ca. 15 tot 30 minuten zonder airconditioning kan. De temperatuur kan zo hoog oplopen dat er een ernstig risico op computer apparatuur uitval gaat ontstaan.

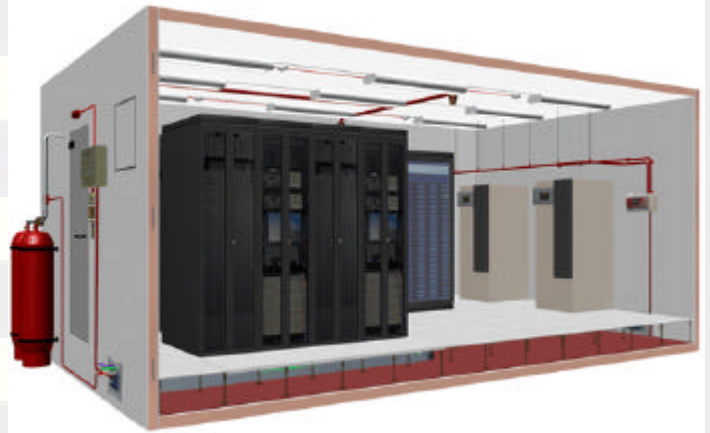
De in eerste instantie niet kritische componenten zoals ventilatoren in de server cabinets, monitoring apparatuur, blussysteem etc., vervullen tijdens dergelijke calamiteiten dus juist een cruciale rol.

2.3 Brandbeveiliging

Met 28% is brand, zowel binnen als buiten het datacenter, een grote bedreiging te noemen (water is eerste met 60%). Brandbeveiliging is daarom dan ook een belangrijk onderdeel van de continuïteits- en calamiteitenplanning. Het hebben en onderhouden van een gecertificeerd brandbeveiligingssysteem is één van de belangrijkste aspecten om de veiligheid van mensen, de beschikbaarheid van het gebouw en het veiligstellen van informatie zeker te stellen.

Organisaties veranderen echter vrijwel continu, zodat ook de continuïteitsmaatregelen aangepast moeten blijven worden, zodat er altijd een balans blijft bestaan tussen van het aanvaardbare risico en veiligheidsniveau. Door het tijdig nemen van de juiste organisatorische, bouwkundige en technische maatregelen zullen de risico's geminimaliseerd worden.

De voor hardware geldende norm EN1047-2 is veel stringenter dan de geldende DIN4102 norm die van toepassing is op de bouwkundige zaken. Dus indien de bouwkundige constructie gebaseerd is op de gangbare DIN4102 norm (bouwbesluit) is het Datacenteronvoldoende beschermd tegen brand.



2.3.1 Branddetectie

Wanneer we een (smeul)brand willen blussen, zullen we deze eerst, het liefst zo snel mogelijk, moeten kunnen detecteren. Omdat de meeste datacenters zijn voorzien van een airconditioner, is er sprake van een verhoogde luchtsnelheid. Dit heeft als nadelig gevolg dat conventionele brandmelders niet of nauwelijks werken. Om toch een smeulbrand snel te kunnen detecteren wordt in datacenters ook wel een rookaanzuigsysteem toegepast (aspiratiedetectie systeem).

2.3.2 Brandblussing

Wanneer het aspiratiedetectiesysteem een smeulbrand detecteert, zal direct de airconditioner uit worden gezet. Dit voorkomt direct het extra aanwakkeren van de smeulbrand en zorgt er voor dat de conventionele melders nu correct kunnen functioneren.

Wanneer nu een tweede meldergroep een brand detecteert (volgens NEN2535) mag er een bluscommando worden afgegeven. Voor de blussing in datacenters zijn er meerdere opties zoals:

1. Argon (ar)
2. Argonite (ar+cO₂)
3. Inergen (ar+cO₂+stikstof)
4. Oxyreduct.

Alle genoemde blusgassen werken volgens het zelfde principe, en zijn niet schadelijk voor het milieu en de apparatuur ondervindt tevens geen schade van deze gassen. Bij oxyreduct wordt het zuurstofgehalte continue op 12-13% gehouden, hierdoor is er in de gesloten ruimte geen ontbranding mogelijk.

2.4 Overige controlesystemen

Ongewenste bezoekers hebt u liever niet binnen in een datacenter en bedrijfsinformatie dient uiteraard geheim te blijven. Om dit te bewerkstelligen dient men maatregelen te nemen die liggen op de volgende vlakken:

- Toegangscontrole
- Camerabewaking

2.4.1 Toegangscontrole

Een toegangscontrole systeem is een voorziening die de fysieke beveiliging sterk verhoogt. Doordat de autorisatie persoonsgebonden is, worden alleen bevoegde personen toegelaten in de ruimte. In het geval van een incident kan achteraf gecontroleerd worden wie op dat moment binnen is geweest; de toegang is per individu te controleren. Een traditioneel systeem met sleutels heeft deze functie niet.

Er zijn diverse toegangscontrole systemen op de markt beschikbaar. De systemen verschillen zowel in functionaliteit als in praktisch gebruiksgemak en onderhoud.

- Een deurdranger voorkomt openstaande deuren.
- Een open/dicht signalering voorkomt dat de deuren open worden vastgezet.
- Een eenvoudig systeem werkt met magneetpassen. Nadeel van dit systeem is dat de passen bij veelvuldig gebruik slijten en storingen gaan vertonen.
- Proximity cards werken met een chip en kennen deze storingen dus niet.
- Een anti pass-back heeft als bijkomend voordeel dat "meelopen" door een persoon zonder toegangkaart wordt voorkomen.
- Biometrische systemen controleren op persoonsgebonden gegevens. Er zijn bijvoorbeeld systemen die een scan van de iris of handpalm als identificatie gebruiken. Deze systemen zijn pas sinds enkele jaren in ontwikkeling en daarom vrij duur maar sluiten wel uit dat toegangspassen eenvoudig aan een ander kunnen worden uitgeleend

Het toevoegen van een biometrische parameter aan een kaartstelsel maakt het vrijwel onmogelijk dat een onbevoegde toegang krijgt tot voor hem niet toegankelijke ruimte. Biometrie biedt een volkomen niet-overdraagbare herkenning van personen, in tegenstelling tot kaarten of badges. Er zijn systemen beschikbaar die volledig zijn gebaseerd op intelligente toegangscontrole, inclusief bezoekersregistratie, aanwezigheidsregistratie en foto-identificatie.

2.4.2 Camerabewaking

Cameratoezicht is een essentieel onderdeel van het veiligheidsplan. De videobewakingsoplossingen (CCTV) zijn vrijwel allemaal gebaseerd op analoge traditionele systemen, waarbij de opslag plaats vindt middels VCR en/of Video Hard Recorder. Nieuwe moderne systemen zijn geheel of gedeeltelijk gebaseerd op IP technologie. Door het effectief en efficiënt inzetten van deze middelen, kunnen de operationele kosten met 45% verlaagd worden. IP Video Surveillance biedt de mogelijkheid pro-actief te beveiligen. Deze nieuwe ontwikkelingen hebben impact op het huidige veiligheidsbeleid. Een IP Video Surveillance heeft meer gebruiksmogelijkheden, welke met analoge systemen niet of alleen tegen zeer hoge kosten te realiseren zijn.

2.4.3 Multifunctionele toepassingen

Intelligente toegangscontrole en multifunctionele toegangskarten worden geïntegreerd in één overzichtelijk totaalsysteem. Hiermee wordt de 'security & safety' van de

bedrijfsvoering gewaarborgd. Door een multifunctionele kaart wordt toegang verschaft, maar deze kan tegelijk ook worden gebruikt om betalingen te verrichten, kopieën te registreren, pc's te beveiligen en werktijden te registreren. Sommige organisaties vragen echter om nog strengere controle en ook dat is mogelijk. LCC Green Server Room baseert haar complete oplossingen op een diepgaand inzicht in het bedrijf van de klant en heeft toonaangevende expertise op alle gebieden van security technologie.

2.5 Verhoogde computervloeren

Een verhoogde vloer, of computer vloer, is bijna een vanzelfsprekend onderdeel van een datacenter. Toch is het nuttig om te begrijpen wat de onderliggende redenen zijn voor de plaatsing van een verhoogde vloer.



2.5.1 Functies van computervloeren

De functies van een verhoogde vloer zijn:

- Distributie van koele lucht naar de server cabinets. Bij verandering van de plaats van de cabinets, of bij hotspots, kan de koeling precies gedistribueerd worden.
- Wegwerken van koelleidingen.
- Wegwerken van kabelgoten voor power en data.
- Wanneer de databekabeling vaak moet worden aangepast kan overwogen worden de databekabeling "overhead" te installeren; dit vereenvoudigt het installeren en controleren van databekabeling.
- Aarding van de vloer ter voorkoming van schade aan printplaten door elektrostatische ontlading

Bij nieuwe gebouwen kan een eventueel doorzakken van de verdiepingsvloer worden gecompenseerd door de hoogte van de verhoogde vloer aan te passen.

2.5.2 Ontwerp en installatie

Bij het ontwerp van een ruimte met een verhoogde vloer dient extra aandacht te worden gegeven aan de volgende aspecten:

- De hoogte van de vloer dient te worden afgestemd met de gewenste airflow onder de vloer.
- Beperking van de luchtstroom door obstakels onder de vloer zoals kabelgoten.
- De plaatsing van een ramp of opstap.

Bij de installatie zijn de volgende zaken belangrijk:

- Plaats de verhoogde vloer niet te vroeg in het project zodat de vloer zo min mogelijk moet worden geopend voor installatie van koelleidingen, blusinstallatie, kabelgoten, etc.
- Verwijder maximaal 2 aansluitende vloertegels per keer om instabiliteit van de vloer te voorkomen.

2.5.3 Vloerbelasting

Racks vol met blade servers en blade storage wegen bijzonder veel. De normale computervloeren zijn berekend op maximaal 500 kilo per rack. Racks gevuld met blade technology wegen echter tot over de 1000 kilo per rack. Dit vraagt om een compleet andere constructie, van zowel het gebouw als de computervloer. In het ontwerp dient men hier rekening mee te houden.

2.6 Gestructureerde bekabeling

Het is sterk aan te bevelen om de databekabeling op een gestructureerde manier aan te leggen. De meest toegepaste structuur is een sterconfiguratie waarbij in elk serverkast een patchpaneel geïnstalleerd wordt. Aan de andere zijde van de (backbone) bekabeling worden alle patchpanelen geconcentreerd in een centraal knooppunt. Een verbinding tussen twee componenten die niet in hetzelfde server kast zitten, wordt in de centrale patchkast gemaakt.

Voordelen van deze configuratie zijn:

- De bekabeling is universeel te gebruiken.
- Volledige transparantie, alle apparatuur kan snel en direct met elkaar verbonden worden.
- Er is reservecapaciteit aanwezig voor uitbreidingen.
- Storingen kunnen snel worden verholpen.
- Een "oude" verbinding wordt snel verwijderd. Er ontstaat geen spaghetti van niet meer in bedrijf zijnde bekabeling tussen individuele kasten.

2.6.1 Behoeftebepaling

De specifieke behoeften van de gebruiker maken dat de keuze voor een type netwerk bekabeling altijd maatwerk is en bepaald wordt door:

- Het soort toepassing is bepalend voor de benodigde bandbreedte.
- Specificaties van de ICT apparatuur, type netwerk kaarten, etc.
- Eis voor wel/niet een gecertificeerd systeem.
- Verwachte uitbreidingen van systemen.

2.6.2 Toekomstvastheid

Onder normale omstandigheden mag een infrastructuur niet de beperkende factor zijn voor systeemupdates gedurende de 20-jarige levensduur. Met goed ontworpen bekabelingssystemen kunnen gegevens 10-15 keer sneller worden verwerkt dan met de meeste LAN's. Hierdoor kunnen nieuwe netwerktechnologieën worden geïntroduceerd zonder dat de bekabeling vervangen moet worden.

De applicaties bepalen de minimumspecificatie van een infrastructuur. Echter, in een aantal situaties waarin een Categorie 5e kabel wordt gezien als een adequate oplossing, kan het toch zinvol zijn een betere bekabeling te installeren, bijvoorbeeld een Categorie 6 of Categorie 6a, om optimaal te kunnen inspelen op toekomstige behoeften.

2.6.3 Redundantie

Wanneer systemen van essentieel belang zijn voor een bedrijf, kunnen redundante backbones en risers nodig zijn om een mesh-netwerk te implementeren, waardoor het vereiste fouttolerantieniveau voor het systeem wordt bereikt. In zulke situaties moeten duplicaten van paden fysiek zover mogelijk uit elkaar liggen.

2.6.4 Garanties



De kwaliteit van de garantie op een infrastructuur is de beste zekerheid dat storingen in het systeem niet zullen leiden tot een onverwachte kostenpost. In de meest optimale situatie heeft de garantie betrekking op de volledige verwachte levensduur van het systeem van 20 jaar en dient niet alleen bekabelingsinfrastructuur en alle componenten te bevatten maar ook de betreffende LAN applicaties. Alleen bekabelingsleveranciers die de LAN applicatie volledig hebben getest en gedocumenteerd, kunnen een dergelijke garantie vol vertrouwen aanbieden. Wanneer het netwerk ontworpen en aangelegd is door een erkend installateur, zullen er met betrekking tot de garantie in de toekomst geen verrassingen zijn. In deze situatie is er geen enkele discussie over de vraag welke specifieke leverancier verantwoordelijk is voor een storing of fout.

2.6.5 Efficiënt beheer van de bekabelinginfrastructuur

Netwerken worden vanwege technologische ontwikkelingen steeds omvangrijker en complexer. De bekabelingsinfrastructuur is, meer dan ooit tevoren, het zenuwstelsel dat alle bedrijfskritieke informatie van een onderneming transporteert.

Door de complexiteit van de netwerken is het van cruciaal belang het beheer van de ICT middelen goed in te richten. Daardoor kan het primaire bedrijfsproces van de onderneming gewaarborgd en gecontinueerd worden.

Een van de belangrijkste peilers voor succesvol beheer is het creëren van een controleerbare en stabiele omgeving. Het menselijke aspect is vaak de zwakste schakel als het om beheer gaat. Beheer- en registratiefouten kunnen soms grote gevolgen hebben.

Het betrouwbaar houden van de administratie en inventarisatie bestaat bij veel ondernemingen uit het voortdurend achter de feiten aan lopen. Verhuizingen, reorganisaties en/of aanschaf van nieuwe apparatuur (switches en PC's), maar ook ongeautoriseerde mutaties van verbindingen, zorgen er voor dat de veel

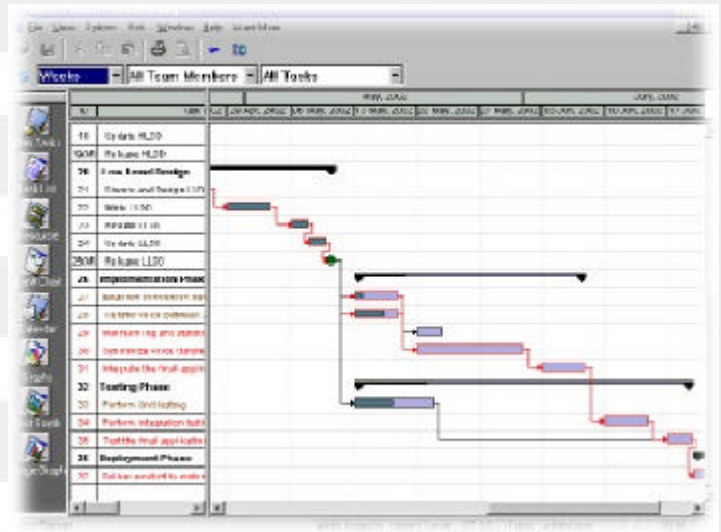
netwerkbeheerders het overzicht kwijt zijn. Deze inefficiëntie, zoals het steeds opnieuw inventariseren van informatie en het handelen op basis van incidenten, betekent een verhoging van de operationele kosten en een verlaging van de productiviteit.

Bij bedrijfskritische processen is het raadzaam om preventief beheer toe te passen, zodat de continuïteit van het bedrijfsproces veilig gesteld wordt.

3 De LGSR aanpak

Bij het ontwerpen van een datacenter hanteert LCC Green Server Room een procesmatige aanpak gericht op een duidelijke praktische invulling met een vastgelegd kwaliteitsniveau op het gebied van bedrijfsvoering en aanwezige vakkennis. Het gehele proces vanaf het uitvoeren van risicoanalyses tot en met het onderhoud verloopt volgens een erkend wettelijk en normatief kader. Belangrijk is dat in het begin inzichtelijk wordt gemaakt wat de werkelijke risico's en knelpunten zijn waarmee rekening gehouden dient te worden. Om te komen tot een goed en gedegen veiligheidsplan hanteert LCC Green Server Room een Plan van Aanpak bestaande uit de volgende stappen:

1. **Risicoanalyse-evaluatie:** Voorafgaand inzicht verkrijgen in mogelijke risico's, knelpunten en onzekerheden.
2. **ICT Ruimte Check:** Door het uitvoeren van een controle wordt een duidelijk beeld verkregen van de aanwezige infrastructuur en omgevingsfactoren. Het uitvoeren van een visuele inspectie en het verrichten van metingen geven een duidelijk beeld van de situatie. In een rapport, waarin uiteraard rekening gehouden wordt met de wensen van de klant, worden adviezen en de huidige status van de ruimte gepresenteerd.
3. **Programma van Eisen:** Definieren en formuleren van eisen en wensen, zodat de geboden oplossing gericht is op maximale beschikbaarheid en betrouwbaarheid van het datacenter. De uitgangspunten worden in overleg met de klant bepaald en getoetst aan de eisen van de wettelijke (bouw-)regelgeving, waaronder het Bouwbesluit, de bouwverordening, de normen en praktijkrichtlijnen geldend voor datacentra en aanvullende wensen ten aanzien van gebruik van het datacenter.
4. **Ontwerp:** Het ontwerp bevat alle samenhangende informatie voor een goede detail- of montageplanning en aansturing van de vereiste voorzieningen.
5. **Implementatie:** Levering van producten, inclusief technische specificaties, documenten, richtlijnen en vereiste productcertificaten, waarna onder leiding van een installatiedeskundige alle technische installaties vakbekwaam aangelegd, geïnstalleerd en opgeleverd worden.
6. **Beheer en onderhoud:** Vastleggen van waarnemingen en bevindingen conform een geïmplementeerde logboekprocedure of werkinstructie op basis van een service level agreement. Toetsen van het alle systemen en voorzieningen aan het vooraf gedefinieerde Programma van Eisen, waarna (indien nodig) zowel preventief als correctief onderhoud plaats vindt.



3.1 Voordelen van de oplossing 'Green Data Center'

- Een betrouwbare en toekomstvaste ICT-omgeving die de continuïteit van bedrijfsprocessen ondersteunt (data-opslag verdubbelt elk anderhalf jaar).
- Het inzetten van LCC Green Server Room als aanspreekpunt voor de totale realisatie resulteert in:
 - o Een eenduidig Programma van Eisen.
 - o Een goede balans tussen ingecalculeerde risico's en investeringen.
 - o Total cost of ownership (TCO) van reeds bestaande complexe technologieën (Oude legacy-omgevingen hebben een upgrade nodig) wegen vaak zwaarder dan eenmalige investeringen in nieuwere technologieën.
 - o Tijdsbesparing doordat de totale implementatie volgens een doordacht plan in één keer wordt gerealiseerd.
 - o Lagere Total Cost of Ownership.
- Een juist ontwerp geeft vermindering van risico's ten gevolge van
 - o controle verlies over systemen en onderbrekingen in het leveren van (computer)services
 - o inbreuk op image en/of reputatie
 - o Het voorkomen van hogere kosten en lagere kwaliteit door in bestaande situaties gebruik te maken van geïntegreerde oplossingen in plaats van reeds aanwezige aparte netwerken voor voice, video en applicaties
 - o Nagegaan zal altijd worden waar de kritische punten liggen. Dit omdat de gevolgschade veel moeilijker in kaart is te brengen dan de directe schade (het vervangen van hardware of het terugzetten van back-ups). Gevolgschade is vaak vele malen groter, dus is van belang deze in kaart te brengen en rekening mee te houden bij het ontwerp.
- Afname van de complexiteit van het netwerk en het beheer ervan.

4 Samenwerken met LGSR

De voordelen van samenwerking met LCC Green Server Room:

- LCC Green Server Room verzorgt, eventueel samen met geselecteerde businesspartners, alle noodzakelijke niet ICT-gerelateerde facetten zoals bouwkundige voorzieningen, energievoorzieningen, klimaatvoorzieningen, beveiligingssystemen en gebouwinrichting (meubilair, verhoogde vloeren, etc.).
- LCC Green Server Room biedt pragmatische oplossingen om optimaal in te spelen op de behoefte. Zij heeft specialisten in huis die de kennis en kunde hebben om kritische punten te bepalen. Hierdoor kan mogelijke gevolgschade beter in kaart worden gebracht en wordt het ontwerp hierop afgestemd.
- Snelle levering van 'ready-for-use' datacentra en server rooms, etc. gebaseerd op voorgedefinieerde oplossingen en bewezen technologieën.
- Hiernaast biedt LCC Green Server Room ook ICT-infrastructurele oplossingen. Een totaal serviceconcept voor complete inrichting van kantoorruimtes, datacenters, switchruimtes, callcenters en dealingrooms.

Door gebruik te maken van de expertise van LCC Green Server Room kunnen klanten zich blijven richten op hun core-business.

5 Complementaire diensten

De dienstverlening van LCC Green Server Room is erop gericht altijd en overal bedrijfskritische informatie voor opdrachtgevers te ontsluiten. Onafhankelijk van de achterliggende systemen. De verschillende componenten van de oplossingen worden aangeboden in een samenhangend palet van vijf services. Opdrachtgevers kunnen zowel een compleet pakket, als specifieke onderdelen van de dienstverlening inzetten.



Data Center Consulting

- Design Green Field DC (data center)
 - Availability
 - Sustainability
 - Capacity
 - Modularity
 - Upgrade ability
- Assessment existing datacenter
 - Status quo
 - Upgrade to high density
 - Upgrade to higher availability level
 - Improvement plan (time, money, impact)

Data Center Construction

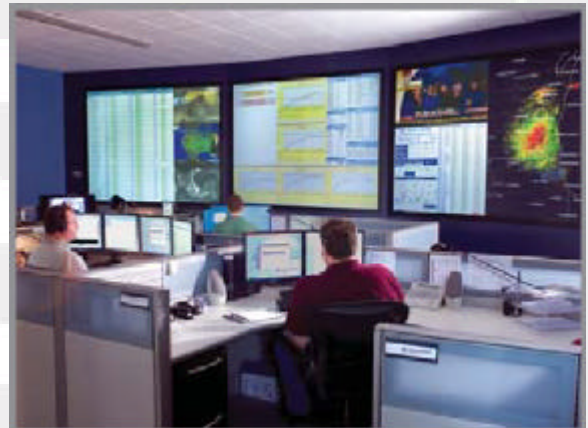
- Design/Build Construction
- Bid & Specification Construction
- Traditional general contracting
- EPMC contracting

Data Center Project Management

- Contractor Management
- Procurement
- Data Center Commissioning
- Data Center Relocation Coordination

Data Center Monitoring & Control

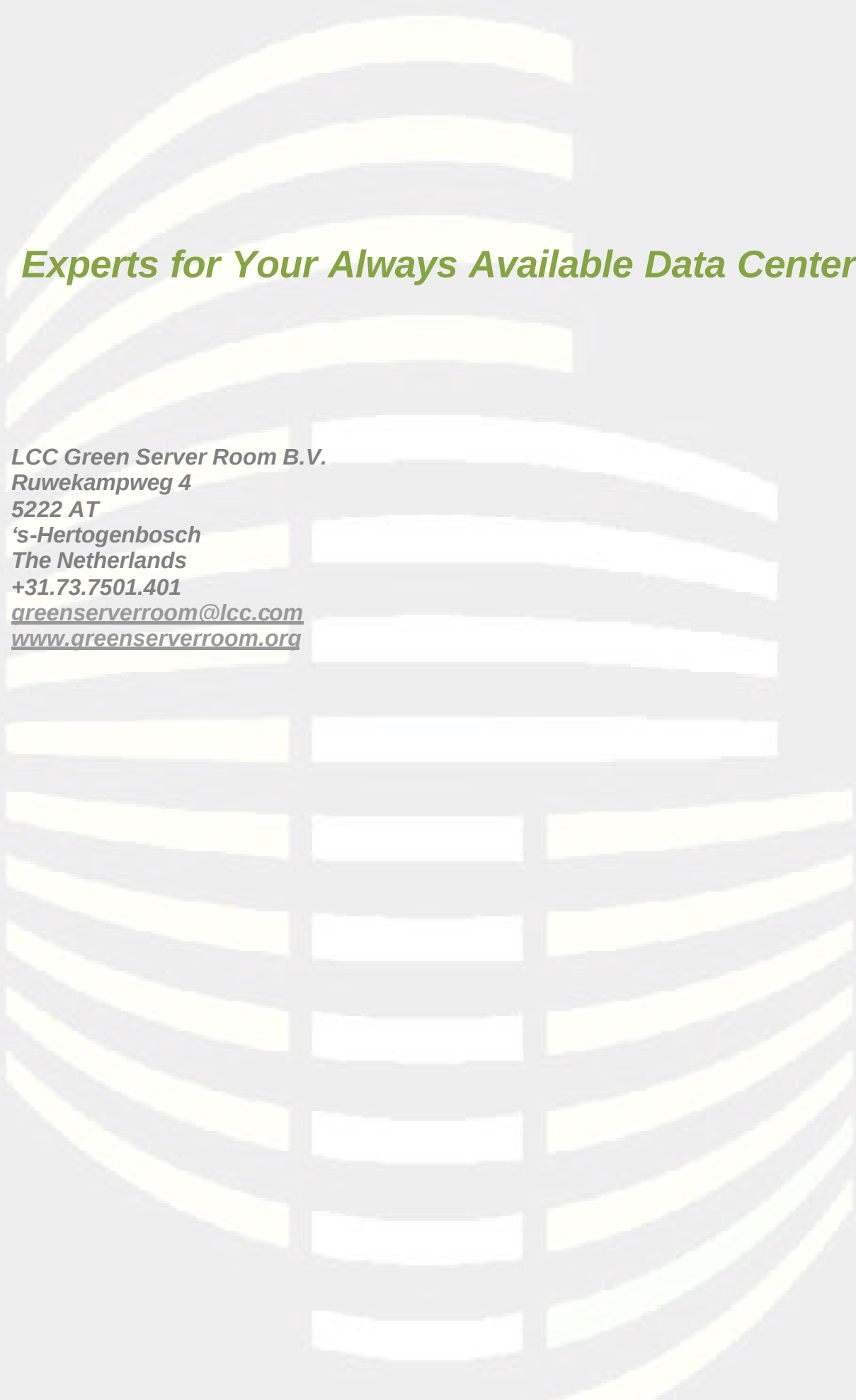
- Supportive Infrastructure Monitoring
 - Power (V/A)
 - Mechanical (T/RH/Air)
 - Security Access & Control
- Network Operations Center (NOC)
- Server (KVM) & Serial Device Access Systems



Data Center Operations & Maintenance

- Facility Electrical Testing Services
- Data Center Site Cleaning
- Support Infrastructure Operations Review

Meer informatie over deze dienstverlening staat op:
www.greenserverroom.org



Experts for Your Always Available Data Center

LCC Green Server Room B.V.
Ruwekampweg 4
5222 AT
's-Hertogenbosch
The Netherlands
+31.73.7501.401
greenserverroom@lcc.com
www.greenserverroom.org