CHEOPS REPORT

Bent u **‘always on’?**

De klok rond **beschikbaar**

Iedereen verwacht dat u ‘always on’ bent: uw klanten, leveranciers, medewerkers en niet in het minst uzelf. De belangrijkste processen in uw onderneming zijn afhankelijk van IT-systemen en die mogen niet uitvallen. Tenminste als uw reputatie en klantenbestand u lief zijn. Werken doen we al lang niet meer van negen tot vijf, dus moet u ervoor zorgen dat uw bedrijfssystemen de klok rond beschikbaar zijn.

Deze gids biedt u een leidraad om te voorkomen dat u op een dag ‘always off’ bent. We brengen in kaart welke risico’s u loopt en waarom, en schotelen u een reeks concrete maatregelen voor om de continuïteit van uw bedrijfssystemen en -werking te verbeteren en vrijwaren.

Uitval is geen optie

DE INZET IS HOOG

Weet u welke risico's u loopt wanneer uw bedrijfssystemen het laten afweten? Voor een middelgroot bedrijf kost elk uur uitval al snel duizenden tot tienduizenden euro's. Denk maar aan productieverlies, potentieel vertrek van klanten, extra kosten en communicatie, of zelfs schadevergoedingen. De meeste bedrijven hebben het kostenrisico nog nooit berekend.

Naast de financiële impact en een mogelijk verlies van waardevolle gegevens, berokkent een onderbreking van de productiviteit ook schade aan uw reputatie en concurrentiepositie. Het kan de beurswaarde van grote organisaties doen kelderen en zware juridische gevolgen met zich meebrengen. En wat als blijkt dat u als bedrijf niet meer kunt voortwerken omdat u belangrijke gegevens niet meer kunt recupereren? Logisch dat niemand nog het belang van bedrijfscontinuïteit onderschat.

IT ALS CENTRALE SPIL

Uw bedrijfsprocessen kunnen niet meer zonder technologie en die wordt bovendien steeds complexer ingezet. Er gaan elke dag meer gegevens automatisch rond in uw onderneming en daarbuiten. Medewerkers en klanten willen van overal toegang tot informatie wanneer het hen past.

Een goed ingerichte en beveiligde IT-infrastructuur is meer dan ooit een voorwaarde om als een betrouwbare zakenpartner te worden beschouwd. Strengere regelgeving rond privacy en de vertrouwelijkheid van gegevens maakt het er niet eenvoudiger op.

DE RISICO'S BEPERKEN

Bedrijfscontinuïteit is veel meer dan een snelle doorstart na een noodsituatie. Uw IT-afdeling is er dan ook niet als enige verantwoordelijk voor. Daarom raden we u een geïntegreerde aanpak aan. Hoewel 100 procent ononderbroken werken vandaag een utopie lijkt, kunt u met een doelgerichte aanpak de grootste risico's drastisch beperken. In dit document leggen we uit hoe.

De impact van downtime en gegevensverlies is veel groter dan u denkt.

Wat beïnvloedt ‘always on’?

De kans dat het een IT-probleem is dat uw activiteiten onderbreekt, was nooit groter dan vandaag. Het aantal toepassingen en gegevens groeit pijlsnel en er gebeurt steeds meer online en in real time. Als u ‘always on’ wilt zijn, houdt uw strategie het best rekening met een aantal belangrijke tendensen op het vlak van IT:

1. ALLE IT-TOEPASSINGEN ZIJN MET ELKAAR VERBONDEN

Aanvankelijk hielden organisaties hun bedrijfsprocessen en de daarbij horende IT-applicaties vaak van elkaar gescheiden. Tegenwoordig integreren bedrijven zo veel mogelijk applicaties en afdelingen om de efficiëntie te verhogen. Wanneer een applicatie in één afdeling uitvalt, kan dat een grote impact hebben op essentiële processen in een andere. Bovendien wordt het onderhoud van sommige toepassingen uitbesteed, terwijl het voor andere intern gebeurt. De technologische opzet die al deze bedrijfsprocessen ondersteunt, wordt daardoor een moeilijk te ontwarren knoop.

2. UW BEDRIJFSGEGEVENS ZIJN OVERAL

Door de opkomst van cloudcomputing, sociale netwerken, bring your own device (medewerkers die een eigen laptop, tablet of smartphone ook voor het werk gebruiken) en het internet of things (alle mogelijke apparaten, melders en sensoren die gegevens doorsturen naar uw IT-applicaties) zijn alles en iedereen met elkaar verbonden. We werken mobiel en vinden het maar normaal om altijd en overal online te zijn. Professioneel en privé lopen door elkaar, vaak op dezelfde toestellen. Bedrijfsgegevens en toestellen voor professioneel gebruik blijven niet langer binnen de fysieke grenzen van uw bedrijfsnetwerk en zijn moeilijk te beveiligen.

Professioneel en privé
lopen door elkaar.
Uw gegevens zijn overal.

3. TE WEINIG BESEF VAN DE RISICO’S

Een gedegen aanpak om uw IT beschikbaar te houden, begint al bij een degelijk besef van de mogelijke risico’s. Daar loopt het vaak al fout. Te veel bedrijven wachten bijvoorbeeld om over te stappen naar nieuwere – en beter beveiligde – versies van applicaties en besturingssystemen, zelfs wanneer de fabrikant de oudere versies technisch niet meer ondersteunt. Evengoed zorgt het gebrek aan besef

ervoor dat er te weinig wordt geïnvesteerd in het gespecialiseerde beheer dat IT en IT-beveiliging vereisen. Op die manier ontstaan kwetsbaarheden die gemakkelijk vermeden hadden kunnen worden.

4. DE REGELGEVING WORDT STRENGER

De toenemende risico's doen overheden maatregelen nemen om de privacy van burgers beter te beschermen. In de Europese Unie is een belangrijke mijlpaal daarin de komst van de General Data Protection Regulation (of GDPR). Die nieuwe regelgeving dwingt bedrijven vanaf 2018 een nieuw en strenger kader af voor het beheer en bescherming van persoonlijke gegevens in de EU. Ze omvat zaken als toegang tot en overdraagbaarheid van persoonlijke data, het recht om 'vergeten' te worden of op de hoogte te worden gebracht als je individuele gegevens mogelijk gelekt zijn. Ze voorziet ook ernstige boetes voor overtreders.

5. DE FYSIEKE RISICO'S NEMEN TOE

Tot slot kunnen ook economische en politieke factoren – zoals het afschakelplan bij elektriciteitsschaarste – tot downtime leiden. We krijgen vaker te maken met uitzonderlijke weersomstandigheden zoals koude- en hittegolven, stormen en overstromingen. Dat brengt meer risico op onderbrekingen met zich mee.

Denk strategisch na over IT en bedrijfscontinuïteit

Het mag duidelijk zijn dat bedrijfscontinuïteit, IT en de beveiliging ervan vandaag op een **strategische manier** moeten worden benaderd. **Risico's maximaal inperken** is één belangrijke reden. Een andere, even belangrijke reden, is dat uw technologische keuzes en strategie u vandaag een heus **concurrentieel voordeel** kunnen opleveren. Als u expertise of mankracht mist om er werk van te maken, schakelt u het best een gespecialiseerde partner in. Een die loskomt van de bits en bytes, en samen met u de brug maakt tussen IT en uw business.

De wetgeving wordt veel strenger. In Europa is de komst van GDPR een mijlpaal.

Wat zijn de **echte risico's?**

We hadden het al over tendensen. Maar weet u wat de grootste bedreigingen zijn voor de continuïteit van uw IT-systemen? Denkt u in de eerste plaats aan brand of een natuurramp? Uit onderzoek blijkt dat onderbrekingen en uitval door dat soort problemen pas op de laatste plaats komen in de top vijf van de meest voorkomende risico's.

Factoren van allerlei aard kunnen uw bedrijfscontinuïteit ondermijnen. Hieronder staan ze in de volgorde waarin ze het meest voorkomen. Afhankelijk van de bron spelen de eerste drie al eens haasje-over:

1. DE IT-SYSTEMEN ZELF

Op nummer één staat nog altijd en overduidelijk het falen van IT-systemen door het slecht functioneren van hardware, software of inconsistente gegevens. Dat is heel vaak het gevolg van slecht beheer. Uw IT-infrastructuur en systemen permanent en doorgedreven managen, is dus de absolute basisvereiste om 'always on' te zijn. Waak er nauwgezet over dat een crash van een server of een onmisbaar softwareprogramma uw bedrijfsactiviteiten niet stillegt.

2. ONGEWENSTE INDRINGERS

Sterk opkomend in het lijstje met bedreigingen: malware (niet in het minst ransomware of 'gijzelsoftware') en andere activiteiten van cybercriminelen, zoals diefstal van gegevens en uw identiteit. Een goede afweer tegen dergelijke indringers blijft een absolute prioriteit, want er duiken steeds meer soorten bedreigingen op (zie kaderstuk hieronder). Ongewenst bezoek breekt overigens niet altijd online binnen: traditionele inbraak en diefstal van apparatuur komt dagelijks voor.

Criminelen slaan online en offline toe.

3. ELEKTRICITEIT

Had u verwacht dat stroompannes bij de grootste oorzaken horen van een onderbreking in de bedrijfscontinuïteit? Veel bedrijven vergeten om op dat vlak voorzieningen in te bouwen en die regelmatig te testen. Moderne datacenters voorzien ontdubbelde stroomvoorziening via krachtige noodinstallaties en bieden een veilig alternatief voor uw lokale infrastructuur.

4. U EN UW COLLEGA'S

Wat u al wist: uw medewerkers kunnen onbewust heel wat schade veroorzaken, bijvoorbeeld door onvoorzichtig om te gaan met wachtwoorden. Verlies van toestellen, meestal door onoplettendheid, rekenen we daar ook bij. Minder vaak – maar niet zelden – komt bewuste sabotage of diefstal voor, bijvoorbeeld door mensen die vertrekken, ontevreden zijn met hun job of gewoon van kwade wil zijn.

Menselijke fouten op de IT-afdeling hebben doorgaans grotere gevolgen dan een misstap van een gewone computergebruiker. Verkeerde installaties of configuraties uitvoeren kan altijd gebeuren, maar u moet voorbereid zijn op de mogelijke gevolgen ervan.

5. OVERMACHT

Overmacht of een calamiteit komt als oorzaak van een onderbreking niet zo vaak voor. Maar een brand, overstroming of storm kan wel erg zware gevolgen hebben. Zelfs stakingen of uitzonderlijke verkeersproblemen kunnen de toegang tot uw IT-systemen belemmeren.

Hou de keten intact

Een professioneel IT-beveiligingsbeleid **houdt niet op bij het uitsluiten van één welbepaald risico** of zogenoemde single point of failure (een schakel die de hele keten doet begeven wanneer zij breekt). In een digitale wereld waarin data koning zijn, draait het erom **alle schakels van de IT-infrastructuur permanent intact te houden**.

Uw medewerkers vormen – vaak door onoplettendheid – een belangrijk risico.

Iedereen is een **doelwit**

Vandaag is cybercriminaliteit een van de belangrijkste risico's voor de continuïteit van zowel grote als kleine ondernemingen geworden. We lichten de belangrijkste dreigingen en termen kort toe:

ransomware: software met als enige doel om uw bedrijfsdata te gijzelen door die eenzijdig te versleutelen en de sleutel – private key – te koop aan te bieden aan de rechtmatige eigenaar van de data.

phishing attack: cyberaanval, vaak via e-mail, met als doel om persoonlijke gegevens van computergebruikers te verzamelen. Cybercriminelen doen zich daarbij voor als een vertrouwde bron, zoals een bank.

ddos-aanval (distributed denial of service): een aanval op een IT-infrastructuur met als enige doel om die te overbelasten, zodat de geleverde diensten niet meer beschikbaar zijn (bijvoorbeeld een onlinesysteem voor de ticketverkoop van evenementen dat plots uitvalt).

social engineering: een techniek waarbij wordt geprobeerd om persoonlijke gegevens van computergebruikers te verzamelen, door middel van sociaal contact en vals vertrouwen, of door zich voor te doen als een vertrouwd persoon.

zero-hour attack: een aanval die gebruikmaakt van recente malware of virussen waarvoor antivirussoftwarebedrijven nog geen bescherming hebben uitgebracht. Meestal worden kleine aanpassingen aan bestaande malware uitgevoerd, om zo scans te omzeilen.

advanced persistent threat: een doelgerichte, langdurige aanval, meestal door een groepering van cybercriminelen, met als enige doel om zo veel mogelijk data te bereiken en zo veel mogelijk schade aan te richten binnen één organisatie of omgeving.

Cyberdreigingen als ransomware gijzelen uw bedrijf. Iedereen is vandaag een doelwit.

Essentiële maatregelen

Uw beleid moet voor elk van de opgesomde risico's een antwoord hebben. Maar hoe kunt u zich in de praktijk het beste wapenen? De noden zijn anders voor elk bedrijf. De aard en risico's van de bedrijfsactiviteiten, de bedrijfskritieke applicaties, maar ook de processen en het belang van de gegevens spelen daarbij een rol.

Er zijn twee gemene delers die voor álle bedrijven gelden. De eerste is dat ze problemen moeten voorkomen door hun netwerk, gegevens en applicaties te beschermen. De tweede is dat ze ook maatregelen moeten nemen om bij incidenten de zaak snel onder controle te krijgen, de schade te beperken en systemen snel en volledig up and running te krijgen.

PROBLEMEN VOORKOMEN

Het cliché 'voorkomen is beter dan genezen' geldt zeker voor IT-problemen die uw bedrijfscontinuïteit kunnen onderbreken. Deze vier vuistregels slaat u het best niet in de wind:

1. **Laat uw IT proactief door experts beheren**
   U mag nog zoveel technologie in huis halen, als u die niet professioneel beheert, is dat een slag in het water. Zorg dus in de eerste plaats voor de nodige expertise. Beveiliging is en blijft werk voor specialisten. Een netwerk opzetten, configureren en beheren, vereist niet alleen technische kennis, maar ook permanentie én tijd.

   Als dat al niet het geval was, stap dan zo snel mogelijk en definitief af van een IT-beheermodel van break-fix of brandjes blussen. Voorkom IT-problemen door proactief te monitoren en onderhoudstaken te automatiseren. Zo bent u niet altijd op achtervolgen aangewezen. Durf, indien nodig, ook te erkennen dat u binnen het bedrijf niet over alle expertise en tools beschikt om uw IT professioneel te beveiligen en beheren. De belangen zijn veel te groot.

Laat uw IT proactief door experts beheren.

2. **Scherm uw netwerk af**
   Zet een veilig netwerk op. Dat lijkt de logica zelve, maar de realiteit leert ons anders. Kies voor een gelaagde structuur met segmenten en controleer het gegevensverkeer tussen elk segment. Uw gevoelige gegevens mogen niet rechtstreeks in verbinding staan met het internet.

- Een firewall is de standaardbewaker van uw netwerk. Ideaal hebt u meerdere firewalls, opnieuw in een

gelaagde structuur. Die inspecteren alle inkomende en uitgaande gegevens om verkeer en handelingen te blokkeren die niet zijn toegestaan. Moderne firewalls combineren verschillende functies in één apparaat, zoals een antiviruscontrole en een verkeersinspectie op basis van gebruikersidentiteit en specifieke applicaties.

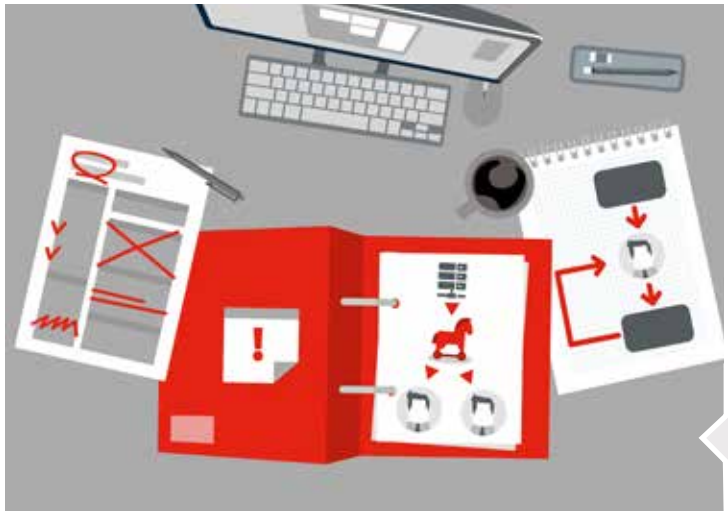
- Steeds vaker gebruiken cybercriminelen de achterdeur van een draadloos netwerk om binnen te raken. Maak er daarom een topprioriteit van om uw draadloze netwerken, toegangspunten en andere draadloze systemen gepast te configureren en te beveiligen.

- Geef malware geen kans om in uw netwerk schade te berokkenen. Maak gebruik van antivirussoftware, antispyware, centraal beheerde persoonlijke firewalls en intrusiepreventie op uw systemen en de apparaten van eindgebruikers. Nog belangrijker: hou die bescherming automatisch en up-to-date, en voer een strikt beleid.

- Hanteer processen, software en encryptie om gevoelige data in het oog te houden en te vermijden dat die ongewenst wegsijpelen of in verkeerde handen terechtkomen. Dat geldt niet het minst voor gegevens op mobiele apparaten.

- Controleer en beheer tot slot de digitale én fysieke toegang tot uw netwerk. Ga na welke gebruikers toegang hebben of proberen te krijgen. Gebruik centrale gebruikers-authenticatie en stel een actief wachtwoordenbeleid in. Extra maatregelen door middel van certificaten, tokens of biometrische scans bieden bijkomende zekerheid.

- Het spreekt voor zich dat ook de toegang tot bedrijfsgebouwen, -afdelingen of fysieke ruimtes (bijvoorbeeld uw datacenter of serverruimte) strikt moet worden geregeld en bewaakt.



Voer doorgedreven procedures in en pas ze nauwlettend toe.

3. Beveilig uw applicaties

Bepaal welke software uw medewerkers mogen gebruiken op uw netwerk. Alle andere software die zijn weg vindt naar uw netwerk moet worden gecontroleerd om te vermijden dat ongewenste applicaties zomaar kunnen worden uitgevoerd.

Om misbruik voor te zijn dient u alert te blijven en uw systemen consequent up-to-date te houden. Voer daarom regelmatig audits en analyses uit die kwetsbaarheden blootleggen. Door onmiddellijk en liefst automatisch bij te werken met beschikbare patches en updates voorkomt u lekken door applicaties en software – ook zelfgeschreven programma's. Verzamel permanent informatie over nieuwe bedreigingen, zodat u er zich op kunt voorbereiden.

Hou, tot slot, de gebruikersrechten onder controle. Beperk en controleer de toegang van gebruikers die aanpassingen mogen uitvoeren aan systemen.

4. Stel procedures in en pas ze toe

Uw eindgebruikers realiseren zich doorgaans onvoldoende hoe belangrijk hun rol is in de beveiligingsketen. Geef hen daarom richtlijnen over verantwoord gebruik van e-mail, software, internet en persoonlijke versus bedrijfsgegevens. Controleer dat ze die ook toepassen. Eenmalig training of documentatie geven, volstaat niet. Om hen regelmatig te herinneren aan de risico's kunt u steekproeven en praktische tests gebruiken.

U vertrouwt het best niet op de standaardinstellingen van uw IT-componenten. Hanteer een uniform configuratieproces, toegespitst op uw organisatie. Netwerkonderdelen zoals firewalls, routers en switches moet u veilig en uniform instellen, en op maat van uw behoeften. Dat geldt uiteraard ook voor uw mobiele toestellen, laptops, servers en pc's.

Test regelmatig de weerstand van uw IT-beveiliging. Simuleer een cyberaanval op uw organisatie, een panne of hardware-defect, een inbraak of diefstal. Breng in kaart hoe efficiënt uw bestaande processen en richtlijnen zijn. Om de kwetsbaarheden van uw IT op te lijsten, is een beveiligingsaudit alvast een goede start.

PROBLEMEN SNEL OPLOSSEN

Bent u ondanks alle voorbereiding toch het slachtoffer van een IT-incident of uitval? Dan moet u onmiddellijk actie ondernemen om snel uw activiteiten te herstellen. U bepaalt vooraf in een plan wie wat moet doen, wanneer en op welke manier. Dat gaat van het incident analyseren en verhelpen, tot gebruikers, bevoegde instanties en uw juridische dienst informeren. Beheer van de respons op incidenten is een onderdeel van uw plan voor bedrijfscontinuïteit. Hier zijn enkele belangrijke onderdelen van uw aanpak:

1. **Uw gegevens altijd in veiligheid**
   U hebt in de eerste plaats een back-up en restore plan nodig om uw bedrijfsgegevens te allen tijde veilig te stellen. Daarin houdt u rekening met de beste locatie voor uw back-ups, beheer en monitoring ervan en de benodigde technologie. Zo'n plan is altijd afgestemd op de noden van uw business en bevat alle procedures en verantwoordelijkheden.

   Back-ups in de cloud kunnen een rendabele oplossing bieden, omdat u alleen betaalt voor de opslagruimte die u daadwerkelijk gebruikt bij uw cloudleverancier. Investeren in apparatuur en onderhoud hoeft dan niet meer.

   Uw back-up moet rigoureus worden beheerd. U kunt het risico niet lopen dat back-ups niet volledig zijn of mislukken. Het beheer ervan moet dus automatisch verlopen en regelmatig moet de back-up worden gecontroleerd aan de hand van zogenoemde restore tests. Vergeet best voor altijd de tape die in de kast op kantoor wordt bewaard.

2. **Onmiddellijk weer van start**
   Als uw organisatie na een IT-uitval snel opnieuw aan de slag moet, voert u het best een plan voor noodherstel *(disaster recovery of DR)* in. Uw gegevens veiligstellen is één ding. Maar als uw systemen platliggen, kunt u ze niet gebruiken. Net zoals bij een back-up en restore plan, staan in uw DR-plan twee zaken centraal. Enerzijds de tijd binnen dewelke uw data en systemen opnieuw beschikbaar moeten zijn na een uitval *(het recovery time objective of RTO)*. Anderzijds de hoeveelheid gegevens die maximaal verloren mogen gaan *(het recovery point objective of RPO)*.

   Is uitval, zelfs voor korte tijd, een absoluut doem-scenario? Dan is een volledig dubbel uitgevoerde

Maak gebruik van de cloud om uw data veilig te stellen en uw systemen snel te herstellen.

IT-omgeving aan de orde. Het probleem is dat niet elk bedrijf zich een uitwijkmogelijkheid op een tweede, zogenoemde redundante locatie kan veroorloven.

Disaster Recovery as a Service (DRaaS) biedt daarbij een kostenefficiënte oplossing, die verder gaat dan een back-up in de cloud. Niet alleen uw gegevens, maar uw hele IT-omgeving, inclusief fysieke of virtuele servers, staat via de cloud ter beschikking voor een snelle doorstart wanneer dat nodig is. Bovendien legt u in het contract met uw dienstenleverancier vast binnen welke termijn u uw bedrijfsactiviteiten weer moet kunnen opstarten na een IT-incident.

3. **Reageer beheerst en kordaat**

   Operationeel moet u adequaat en beheerst op incidenten reageren volgens uw plan. Uw eerste prioriteit is zo snel mogelijk de situatie onder controle brengen. Door het netwerkverkeer en de logs goed te controleren, te analyseren en verbanden te leggen, kunt u bijvoorbeeld verdachte of criminele activiteiten toch in kaart brengen en erop reageren. Incidenten documenteren kan ook doorslaggevende bewijzen bieden bij eventuele juridische stappen.

   Uw juridische afdeling gaat uiteraard geen IT-problemen oplossen, maar kan een belangrijke rol spelen bij de afhandeling ervan, bijvoorbeeld om compensaties te verkrijgen, te beslissen om een aangifte te doen of om uw contracten bij te werken. Had u zomaar een half uur zonder elektriciteit mogen zitten? Moet u na een effectieve aanval naar de politie?

‘Always on’ start met een professionele aanpak

Downtime kan ook voor uw organisatie zwaar doorwegen. U kunt de gevolgen vooraf inschatten met de rekenformule ‘risico maal impact’: hoe groot is uw beveiligingsrisico en hoe groot is de impact van een incident? De vraag blijft: hoeveel risico bent u bereid te lopen?

Als u als bedrijf ambieert ‘always on’ te zijn, is een professionele en proactieve aanpak aan de orde. Dat betekent **niet alleen de juiste technologie toepassen, maar vooral ook die technologie permanent en proactief laten beheren door experts.**

Almaar meer organisaties werken daarom met internettoepassingen en slaan hun gegevens en systemen buiten de bedrijfsmuren op, omdat ze beseffen dat **cloudcomputing** hun IT-beveiliging net kan versterken. Betrouwbare lokale cloudpartners bieden waterdichte contracten en investeren voortdurend in de nieuwste beveiligingstechnologie. Investeringen die bedrijven zelf niet of moeilijk aankunnen.

Uw IT beschikbaar houden en beveiligen is en blijft een complexe materie, waarin u snel het overzicht kunt verliezen. Het antwoord op een aantal basisvragen vindt u in deze gids. Als volgende stap kunt u een risicoanalyse of IT-audit laten uitvoeren. De resultaten daarvan bieden u een concrete basis om uw bestaande beleid te optimaliseren of indien nodig grondig te hervormen.

Checklist: heb ik alles onder controle?

Hebt u recentelijk uw IT-beveiligingsbeleid nog voor de spiegel gehouden? Op basis van de checklist hieronder kunt u zich een idee vormen van de stand van zaken en de nood aan verbetering.

- Hoe actueel is uw plan voor de bescherming van uw bedrijfsgegevens?
- Welke garanties hebt u om na een uitval van uw IT snel opnieuw bedrijfsklaar te zijn? En in hoeveel tijd?
- Wanneer hebt u dat scenario voor het laatst getest?
- Bent u zeker van de kwaliteit en de consistentie van de back-ups die u maakt?
- Hebt u de zwakke schakels in uw IT-beveiliging in kaart gebracht?
- Beheert u uw IT-beveiliging permanent en hebt u daarvoor de juiste mensen en middelen?
- Houdt uw beveiligingsbeleid rekening met mobiele toestellen (ook de privétoestellen van medewerkers en bezoekers) en draadloze netwerken?
- Hebt u een plan voor het geval u het slachtoffer wordt van cybercriminaliteit? En in het geval van stroompanne?
- Wanneer hebt u voor het laatst aan iedereen een training gegeven over IT-beveiliging?
- Hoeveel personen kennen uw volledige IT-infrastructuur en kunnen die beheren?
- Voldoet uw beveiliging aan uw behoeften, de regelgeving en kunt u dat aantonen met een audit van een onafhankelijke partij?

HEBT U VRAGEN OVER HOE U UW BEDRIJFSCONTINUÏTEIT KUNT VERHOGEN?

Neem dan contact met ons op via **cheops@cheops.be** om te bespreken welke aanpak het best bij uw organisatie past. Wij helpen u om IT als een strategisch middel in te zetten en meetbaar te doen bijdragen aan uw bedrijfsdoelstellingen. Met een aanbod van *managed* en *cloud services*, een ervaren team van IT-experts en unieke tools zorgen we voor meer bedrijfscontinuïteit, rendabiliteit en productiviteit van onze klanten.

cheops

Prins Boudewijnlaan 49
B-2650 Edegem
België

T +32 3 880 23 00
E cheops@cheops.be
www.cheops.be