Hoeveel kost downtime jouw organisatie écht?

Een concrete business continuity gids voor CIO’s en IT-managers

YOU FOCUS, WE MANAGE.

EPACT

Inleiding

Bijna elke organisatie heeft vandaag back-ups. Maar hoeveel organisaties durven met zekerheid zeggen dat ze, op het moment dat het telt, ook effectief kunnen herstellen?

Dat verschil, tussen back-ups hebben en kunnen herstellen, is het onderwerp van dit ebook. Het is een verschil dat vaak pas zichtbaar wordt tijdens een incident. En dan is het te laat om het nog te corrigeren.

De cijfers over cyberaanvallen zijn genoegzaam bekend. Ransomware-aanvallen raken elk jaar meer organisaties. Maar het herstel na zo'n aanval duurt volgens recent onderzoek van Veeam gemiddeld enkele weken in plaats van uren. En aanvallers richten zich bewust op back-upomgevingen, omdat ze weten dat dit de laatste verdedigingslinie is.

Toch blijft back-up in veel organisaties een onderwerp dat louter technisch wordt benaderd: een taak op de checklist van de IT-afdeling, in plaats van een strategische pijler van de bedrijfsvoering.

Met dit ebook willen we die discussie openen. We benaderen back-up niet als een IT-onderwerp, maar als een businessvraagstuk. Met **één heel concrete vraag: wat kost stilstand je organisatie werkelijk?**

Waarom falen back-ups net op het moment dat je ze nodig hebt? Hoe vertaal je technische parameters zoals RTO en RPO naar een beslissing die directie en IT samen moeten nemen? En hoe zet je back-up in als aantoonbare compliance-maatregel in een tijdperk van NIS2 en GDPR?

Dit ebook is niet bedoeld om mensen ongerust te maken. Het is een uitnodiging om de juiste vragen te stellen, vóór een incident je dwingt om ze te beantwoorden.

HOOFDSTUK 1

De downtime-rekening: wat een incident jou écht kost

Dit hoofdstuk is eigenlijk een eenvoudig rekenmodel. Een manier om een abstract risico (“onze systemen zouden ooit kunnen uitvallen”) om te zetten in een concreet, becijferd risico dat je aan je management kan tonen om hen te laten beoordelen welke stappen ze willen ondernemen.

De meeste organisaties onderschatten de kost van downtime. Niet omdat ze de cijfers niet kennen, maar omdat ze nog nooit de volledige rekening gemaakt hebben.

“Onze systemen liggen nooit lang plat” is geen risicoanalyse. Het is een aanname die, tot nu toe, is uitgekomen. Wie de downtime-rekening wél maakt, ontdekt meestal drie dingen: de kost is hoger dan verwacht, ze is voor een groot deel voorspelbaar, en ze bestaat uit lagen die zelden allemaal in kaart worden gebracht.

Drie kostenlagen die samen het volledige plaatje vormen

1

Directe kosten

Dit zijn de kosten die het eerst zichtbaar worden en het makkelijkst te becijferen zijn: de tijd van je eigen IT-team, externe consultants of forensische experten die worden ingeschakeld. Denk aan vervanging van gecompromitteerde hardware, overwerk en weekendwerk, eventuele kosten voor gespecialiseerde incident response...

Bij een ransomware-incident komt daar vaak ook de vraag bij of je al dan niet losgeld betaalt. Dat is overigens een beslissing die zelden verstandig is, aangezien betalen geen garantie biedt op herstel en net het businessmodel van aanvallers in stand houdt.

2

Operationele kosten

Dit is de laag die het snelst oploopt en het makkelijkst wordt onderschat: productiviteitsverlies van medewerkers die niet kunnen werken, gemiste orders en facturatie, vertraagde leveringen, SLA-boetes richting je eigen klanten, en de kost van manuele workarounds (met pen en papier werken is zelden efficiënt, en zeker niet schaalbaar). Voor sommige sectoren, zoals productie, logistiek of retail, is dit vaak de grootste kostenpost van allemaal.

3

Indirecte en strategische kosten

Denk aan reputatieschade, verlies van klantvertrouwen, contractuele gevolgen (denk aan boeteclausules of het verlies van een aanbesteding), mogelijke GDPR- of NIS2-sancties bij een datalek, hogere verzekeringspremies nadien, en tijd van management en communicatie die naar crisisbeheer gaat in plaats van naar de business.

Een kanttekening bij internationale benchmarks

Veel gepubliceerde cijfers over de kost van downtime zijn gebaseerd op grote, vaak Amerikaanse ondernemingen en lopen op tot honderdduizenden euro per uur. Die cijfers zijn nuttig als referentiekader, maar weinig bruikbaar als maatstaf voor een Belgische KMO of middelgrote organisatie.

Bereken daarom altijd je eigen cijfer, op basis van je eigen omzet, medewerkersaantal en operationele context, in plaats van een gepubliceerd gemiddelde als waarheid aan te nemen.

Een eenvoudige rekenmethode

Je hoeft geen dure consultant in te huren om een eerste, realistische inschatting te maken. Een basisberekening bestaat uit vier bouwstenen:

1

Verloren omzet per uur

Je jaaromzet gedeeld door het aantal operationele uren per jaar, eventueel gewogen naar het moment van het incident (een uitval tijdens de piekperiode weegt zwaarder dan tijdens een rustige maand).

2

Verloren productiviteit

Het aantal getroffen medewerkers, vermenigvuldigd met hun gemiddelde loonkost per uur en het percentage van hun tijd dat effectief onproductief wordt.

3

Herstelkosten

De geschatte kost van interne en externe uren, hardware en eventuele gespecialiseerde ondersteuning om opnieuw operationeel te geraken.

4

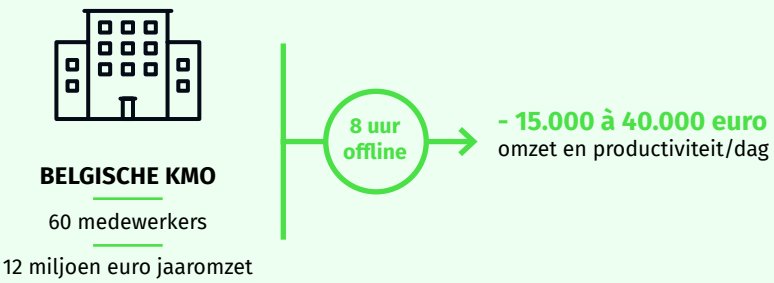
Inschatting van indirecte kosten

Op basis van vergelijkbare incidenten in je sector, of op basis van concrete contractuele risico's die je vandaag al kent (SLA's, boeteclausules, verzekeringsvoorwaarden).

Een vereenvoudigd voorbeeld

Een Belgische KMO met 60 medewerkers en 12 miljoen euro jaaromzet die een volledige werkdag (8 uur) offline ligt, verliest al snel tussen de 15.000 en 40.000 euro aan omzet en productiviteit alleen al voor die dag, exclusief herstelkosten en exclusief eventuele reputatieschade of contractuele gevolgen.

Voor organisaties met kritische, tijdsgevoelige processen (zorg, logistiek, financiële dienstverlening) ligt dat cijfer doorgaans nog hoger.



Waar dit rekenmodel géén rekening mee houdt

Zelfs een zorgvuldige berekening blijft een onderschatting.

Ze vangt zelden de opportuniteitskost van projecten die worden uitgesteld omdat het team met crisisbeheer bezig is, de impact op medewerkersmoraal en verloop, of de langetermijnschade aan een klantrelatie die niet meteen wordt opgezegd, maar wel stilletjes wordt afgebouwd. Die kosten zijn reëel, ook al staan ze niet in ons rekenmodel.

CONCLUSIE

Downtime is een managementonderwerp, geen IT-detail

Zolang de kost van downtime een abstract, ongekwantificeerd risico blijft, blijft het ook makkelijk om te negeren of uit te stellen.

Zodra je het becijfert, verandert het gesprek. Het wordt een investeringsbeslissing die een CFO of zaakvoerder kan afwegen: wat kost een robuuste back-up- en herstelstrategie, tegenover wat een enkel ernstig incident je zou kosten?

Die vergelijking valt in de overgrote meerderheid van de gevallen in het voordeel van de investering uit. De rekening voor downtime is dan ook niet bedoeld om schrik aan te jagen, maar om een besluit te onderbouwen.

HOOFDSTUK 2

Waarom de meeste back-ups falen op het moment dat het telt

“We maken back-ups” is een van de meest misleidende zinnen in IT. Ze klinkt geruststellend, maar zegt niets over de vraag die er werkelijk toe doet: kan je, wanneer het nodig is, ook effectief en tijdig herstellen?

De meeste organisaties die getroffen worden door dataverlies, hadden wel degelijk een back-upoplossing. Het probleem zit zelden bij de afwezigheid van back-ups, maar bij drie klassieke faalscenario’s die zich telkens opnieuw voordoen, in vrijwel elke sector.

Drie scenario’s die telkens terugkomen

1

De back-up bestaat, maar is nooit getest

Een back-upjob die “succesvol” wordt gerapporteerd, betekent niet dat de data ook werkelijk herstelbaar is. Configuratiefouten, incomplete back-upsets, corrupte bestanden of vergeten applicaties (denk aan een database die net buiten het back-upschema valt) blijven vaak onopgemerkt tot het moment van de restore. Een back-up die nooit is getest, is in de praktijk een aanname, geen garantie.

2

De restore duurt veel langer dan verwacht

Zelfs wanneer een back-up technisch in orde is, verloopt het herstel in de praktijk vaak trager dan voorzien. Netwerkbandbreedte, de volgorde waarin systemen moeten worden hersteld (een applicatie die afhankelijk is van een databaseserver die nog niet online is, bijvoorbeeld), en het ontbreken van een gedocumenteerd herstelplan zorgen ervoor dat een geschatte hersteltijd van enkele uren in de praktijk een volle werkdag of langer kan duren.

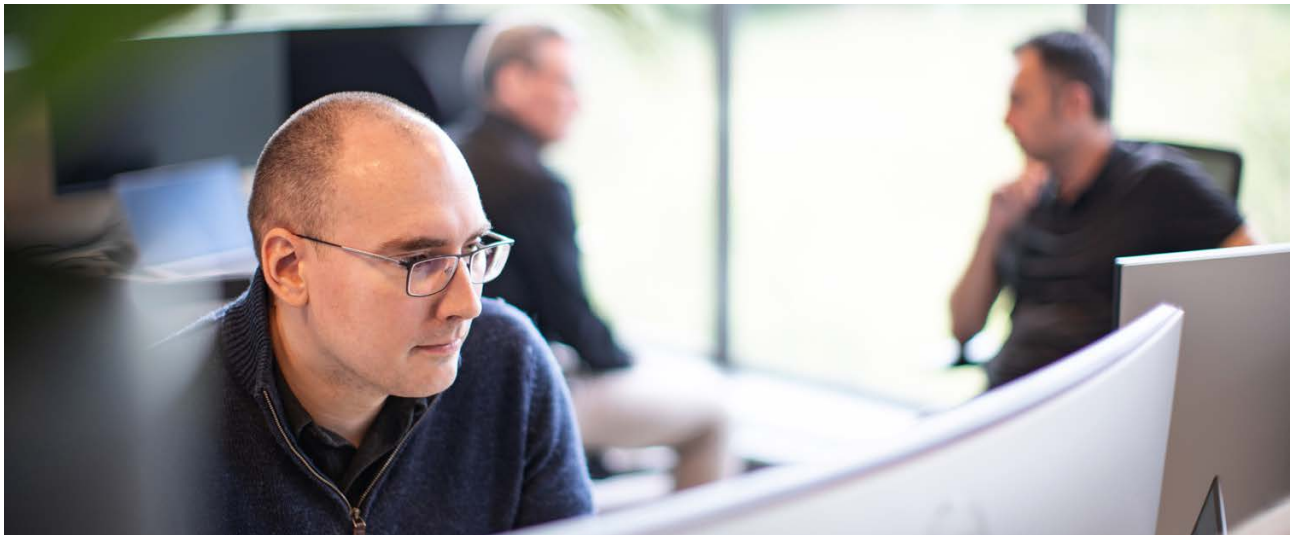
Recent onderzoek van Veeam toont dat de gemiddelde hersteltijd na een ransomware-aanval oploopt tot meer dan drie weken, en dat amper één op tien getroffen organisaties meer dan 90% van hun data effectief kan herstellen.

3

De back-up is zelf geïnfecteerd of versleuteld

Moderne ransomware-aanvallen zijn niet gericht op productiedata alleen. Aanvallers zoeken bewust naar back-upinfrastructuur, om te vermijden dat het slachtoffer kan herstellen zonder losgeld te betalen.

Uit datzelfde Veeam-onderzoek blijkt dat bij 89% van de organisaties die een ransomware-aanval ondergingen, de aanvallers ook actief de back-upomgeving probeerden te compromitteren. Toch gebruikt slechts een minderheid van organisaties immutable (onveranderbare) opslag om dat risico structureel weg te nemen.



De 3-2-1-1-0-regel als praktisch antwoord

Er bestaat geen wondermiddel tegen deze drie scenario's, maar er bestaat wel een beproefde architecturale vuistregel die de risico's structureel beperkt: de 3-2-1-1-0-regel.

3 **3 kopieën van je data**
de productiedata plus minstens twee back-upkopieën.

2 **2 verschillende soorten opslagmedia**
bijvoorbeeld lokale disk-opslag én cloud- of objectopslag, zodat één type storagefout niet al je kopieën tegelijk treft.

1 **1 kopie offsite**
fysiek gescheiden van je productieomgeving, zodat een lokaal incident (brand, diefstal, een volledige site-uitval) niet ook je back-ups vernietigt.

1 **1 kopie offline of immutable**
niet toegankelijk of niet aanpasbaar voor een aanvaller die toegang heeft tot je productieomgeving, zelfs niet met administrator-rechten.

0 **0 fouten**
geregelde, gedocumenteerde en geverifieerde restore-testen. Niet enkel een groen vinkje in een dashboard.

Die laatste twee elementen zijn de voornaamste evolutie ten opzichte van de klassieke 3-2-1-regel, en precies de elementen die in de praktijk het vaakst ontbreken.

Wat betekent dat in de praktijk?

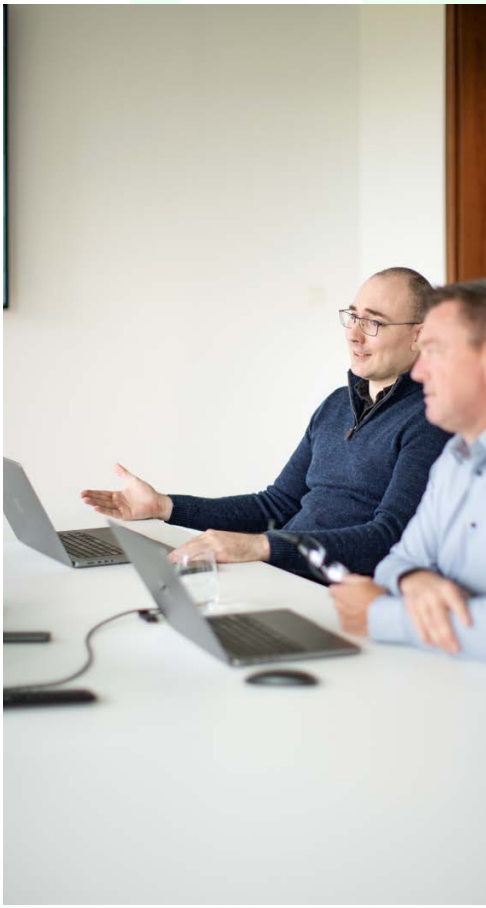
Bij Epact combineren we, afhankelijk van de omgeving, Veeam Backup & Replication of Veeam Data Cloud met immutable objectopslag (onder andere via Wasabi, met Object Lock-functionaliteit) voor de offsite en onveranderbare kopie.

Dat betekent dat een back-up, eenmaal geschreven, gedurende de ingestelde retentieperiode door niemand nog kan worden gewijzigd of verwijderd, ook niet door een aanvaller die volledige toegang heeft verworven tot je productieomgeving of zelfs tot het back-upbeheer zelf.

Testen is geen momentopname, maar een gewoonte

Een restore-test die één keer per jaar gebeurt, tijdens een rustig moment, met een niet-kritieke applicatie, zegt weinig over hoe je omgeving zich gedraagt tijdens een echt incident.

Een volwassen back-upstrategie voorziet in periodieke, gedocumenteerde restore-testen op verschillende soorten workloads (bestandsservers, databases, volledige virtuele machines), met bijhorende meting van de effectieve hersteltijd. Alleen zo weet je of je RTO-doelstelling (zie hoofdstuk 3) ook werkelijk haalbaar is, in plaats van een getal op papier.



CONCLUSIE

Een back-up die nooit getest is, is geen back-up

De drie faalscenario's in dit hoofdstuk hebben één ding gemeen: ze worden pas zichtbaar op het moment dat je ze het minst kan gebruiken.

Een back-upstrategie die structureel steunt op meerdere, gescheiden en onveranderbare kopieën, gecombineerd met geregelde en gedocumenteerde restore-testen, is het verschil tussen een organisatie die een incident overleeft en een organisatie die er weken over doet om weer overeind te komen, als dat al lukt.

HOOFDSTUK 3

Van back-up naar herstelstrategie

Als CIO of IT-manager ken je uiteraard de termen RTO en RPO. Maar heb je die termen ooit vertaald naar een concrete businessbeslissing? Dat is een gemiste kans, want het antwoord op die vraag is zelden een technische kwestie. Het is een beslissing die het management en IT eigenlijk samen moeten nemen.

RTO en RPO kort samengevat

Recovery Time Objective (RTO)

is het antwoord op de vraag:
hoelang mag een systeem offline zijn voordat de impact onaanvaardbaar wordt?

Recovery Point Objective (RPO)

is het antwoord op een andere vraag:
hoeveel data mag je verliezen, uitgedrukt in tijd sinds de laatste bruikbare back-up?

Beide cijfers klinken technisch, maar zijn in essentie **businessbeslissingen**.
Twee voorbeeldjes om dat duidelijk te maken.

RTO 5 minuten

- \+ technisch haalbaar
- \- prijskaartje voor de meeste workloads niet te rechtvaardigen

RPO 24 uur

- \+ voor archiefsysteem volkomen aanvaardbaar
- \- voor een orderverwerkingssysteem onhoudbaar

Niet elke workload verdient dezelfde bescherming

De meest voorkomende fout is dan ook een uniforme aanpak: dezelfde back-upfrequentie en hersteltijd voor alle systemen, ongeacht hun belang.

Dat leidt tot twee problemen tegelijk: kritische systemen zijn onvoldoende beschermd, terwijl minder belangrijke systemen onnodig veel budget opslorpen. Een classificatie naar businesskriticiteit is de eerste stap naar een kostenefficiënte en tegelijk robuuste strategie.

Type workload	Typische RTO / RPO-verwachting
Bedrijfskritisch (ERP, orderverwerking, productieaansturing)	**RTO:** minuten tot enkele uren **RPO:** minuten
Belangrijk (interne applicaties, fileservers, e-mail)	**RTO:** enkele uren tot één werkdag **RPO:** enkele uren
Minder kritisch (testomgevingen, archief, historische data)	**RTO:** meerdere dagen **RPO:** 24 uur of meer

Deze cijfers zijn uiteraard indicatief. De juiste waarden voor jouw organisatie hangen af van je sector, je contractuele verplichtingen tegenover klanten, en de reële financiële impact die je in hoofdstuk 1 hebt berekend.

Het gesprek dat directie en IT moeten voeren

RTO en RPO zijn geen technische parameters die je als CIO of IT-manager zelf kan vastleggen. Het zijn afwegingen tussen kost en risico die op managementniveau thuishoren.

Een aantal vragen die het gesprek met management concreet kunnen maken:

Welke systemen zijn werkelijk bedrijfskritisch, en welke voelen enkel zo aan omdat iedereen ze dagelijks gebruikt?

Wat is de financiële en contractuele impact als een specifiek systeem één uur, één dag, of één week onbeschikbaar is?

Wie beslist, tijdens een incident, welke systemen als eerste worden hersteld?

Welk budget staat tegenover welke RTO/RPO-doelstelling, en is dat een bewuste keuze of een toevallig gegroeide situatie?

De juiste hersteltechniek bij de juiste doelstelling

Eenmaal de doelstellingen vastliggen, bepaalt dat mee welke technische aanpak nodig is:

Voor business-kritische oplossingen en systemen (nagenoeg geen downtime)

replicatie naar een standby-omgeving of Disaster Recovery as a Service (DRaaS), waarbij een kritisch systeem binnen enkele minuten kan worden overgenomen door een secundaire omgeving.

Belangrijke oplossingen en systemen (beperkte downtime)

snelle restore-technieken zoals instant recovery, waarbij een virtuele machine rechtstreeks vanaf de back-uprepository kan worden opgestart terwijl de volledige data op de achtergrond wordt teruggezet.

Voor minder kritische oplossingen en systemen (bv. archieven)

klassieke, kostenefficiënte back-ups met langere retentie, waarbij een langere hersteltijd aanvaardbaar is.

Disaster Recovery as a Service (DRaaS)

Voor organisaties met workloads die nagenoeg geen downtime verdragen, biedt een DRaaS-oplossing een antwoord op het moment dat een volledige omgeving, of een volledige locatie, wegvalt.

In plaats van te herstellen vanaf back-ups, wordt een actuele kopie van je omgeving continu operationeel gehouden in een tweede omgeving, klaar om binnen een vooraf afgesproken tijd de rol van de primaire omgeving over te nemen.

CONCLUSIE

RTO en RPO zijn businessbeslissingen, geen technische specificaties

De vraag “hoeveel downtime en dataverlies kunnen we ons veroorloven?” is te belangrijk om enkel door IT te laten beoordelen, en te technisch om enkel bij het management te laten liggen. Het is een gesprek dat beide partijen samen moeten voeren, met de rekening voor downtime uit hoofdstuk 1 als gemeenschappelijke taal.

HOOFDSTUK 4

Back-up als compliance-instrument

Voor veel organisaties is back-up niet enkel een technische verdedigingslinie. Het is ook een van de meest concrete, auditeerbare bewijsstukken voor een organisatie haar wettelijke verplichtingen rond gegevensbescherming en cyberveiligheid ernstig neemt.

GDPR, NIS2 en sectorspecifieke regelgeving formuleren zelden exacte technische vereisten. Ze formuleren wel duidelijke verwachtingen: kan je aantonen dat data beschikbaar, herstelbaar en beschermd is? Dit hoofdstuk vertaalt die verwachtingen naar concrete, auditeerbare maatregelen.

GDPR: beschikbaarheid als beveiligingsvereiste

Artikel 32 van de GDPR verplicht organisaties om, rekening houdend met de stand van de techniek, passende technische en organisatorische maatregelen te nemen om onder andere de beschikbaarheid en resilience van verwerkingssystemen te waarborgen, én om bij een incident tijdig toegang tot persoonsgegevens te kunnen herstellen.

Een back-upstrategie is met andere woorden geen randvoorwaarde bij GDPR, maar een expliciet vermelde beveiligingsmaatregel. Een datalek waarbij persoonsgegevens niet tijdig hersteld kunnen worden, is dus zowel een operationeel als een juridisch probleem.

NIS2: back-upbeheer als verplichte maatregelcategorie

NIS2 gaat een stap verder. Artikel 21 van de richtlijn somt tien categorieën van verplichte risicobeheersmaatregelen op, en “back-upbeheer, disaster recovery en crisisbeheer” is daar één van, expliciet en met naam genoemd. Dit is geen impliciete verwachting, maar een letterlijk vermelde verplichting.

In België wordt NIS2 gehandhaafd door het Centrum voor Cybersecurity België (CCB), via het CyberFundamentals-kader (CyFun). Organisaties in de aangeduide sectoren, doorgaans vanaf 50 medewerkers of meer dan 10 miljoen euro omzet, vallen onder de verplichting. Essentiële entiteiten (energie, gezondheidszorg, digitale infrastructuur, overheid, en meer) krijgen strenger, proactief toezicht. Belangrijk om te weten: NIS2 introduceert ook een vorm van persoonlijke verantwoordelijkheid voor het management wanneer cybersecurity-maatregelen niet worden goedgekeurd of opgevolgd.

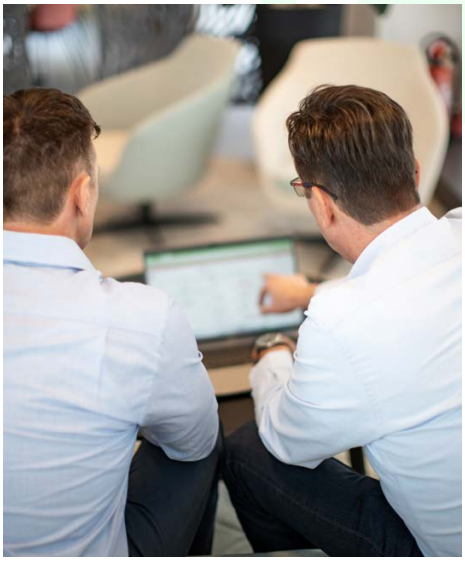
Wat auditors concreet verwachten

1. **Een gedocumenteerd back-upbeleid**, met expliciet vastgelegde RTO- en RPO-doelstellingen per systeem.
2. **Toepassing van de 3-2-1-1-0-regel:** meerdere kopieën, verschillende media, een offsite kopie, een immutable of offline kopie, en periodieke foutloze restore-testen.
3. **Encryptie van back-updata**, zowel onderweg als in rust.
4. **Een volledige scope:** niet enkel on-premise servers, maar ook cloudomgevingen en SaaS-toepassingen zoals Microsoft 365 (e-mail, SharePoint, OneDrive, Teams), die vaak ten onrechte als “al beveiligd door de provider” worden beschouwd.
5. **Gedocumenteerde restore-testen** met effectief gemeten hersteltijden, niet enkel automatische back-uprapporten.
6. **Certificeringen en auditrechten bij je hosting- of back-uppartner**, zoals ISO 27001, en duidelijke afspraken bij een beveiligingsincident.

De vaak vergeten dimensie: datasoevereiniteit

Voor organisaties met gevoelige data, of in sectoren zoals zorg, financiële dienstverlening, juridische dienstverlening of overheid, is niet enkel de vraag óf data hersteld kan worden relevant, maar ook wáár die data en de bijhorende back-ups zich bevinden.

Het Schrems II-arrest en de extraterritoriale werking van Amerikaanse wetgeving zoals de CLOUD Act maken dat een back-up die fysiek in Europa staat, niet automatisch buiten het bereik van buitenlandse overheden valt als de onderliggende provider Amerikaans is.



Van technische maatregel naar aantoonbare controle

Het verschil tussen “we hebben back-ups” en “we kunnen aantonen dat onze back-ups voldoen aan de wettelijke vereisten” zit in documentatie en traceerbaarheid.

Wie kan aantonen dat elke restore-test gedocumenteerd is, dat retentietermijnen bewust zijn vastgelegd in functie van wettelijke en sectorale vereisten, en dat toegang tot de back-upomgeving beperkt en gelogd is, staat sterker tegenover een auditor, een toezichthouder, of, in het slechtste geval, tegenover een rechter na een incident.

CONCLUSIE

Compliance is het resultaat van goede architectuur, niet een aparte checklist

Wanneer je back-upstrategie op een architecturaal degelijke manier is opgebouwd, met immutability, gescheiden kopieën en periodieke tests, voldoe je in de praktijk al aan het grootste deel van wat NIS2 en GDPR vereisen. Compliance wordt dan geen extra project naast de technische realiteit, maar een logisch gevolg ervan.

HOOFDSTUK 5

De menselijke kant van een IT-incident

Dit hoofdstuk gaat niet over technologie. Het gaat over wat een IT-incident met mensen doet: met de IT-manager die om 6 uur 's ochtends een telefoontje krijgt, met medewerkers die niet kunnen werken, en met een directie die binnen enkele uren beslissingen moet nemen waarvoor ze zich nooit had voorbereid.

Onderstaand scenario is een samengesteld, geanonimiseerd beeld op basis van ervaringen die we doorheen de jaren bij meerdere organisaties hebben gehad. Het is representatief voor hoe een incident zich in de praktijk voltrekt, eerder dan een letterlijk verslag van één specifieke klant.

Hoe het begint...

Maandagochtend, 6u34. Een IT-manager bij een middelgrote organisatie krijgt een automatische melding: ongebruikelijke activiteit op de servers. Tegen de tijd dat hij inlogt, blijkt het te laat. Bestanden zijn versleuteld, met een dreigbrief in elke map. De eerste reactie is er één van ongeloof: "dit gebeurt bij anderen, niet bij ons."

Het volgende uur is chaotisch. Welke systemen zijn precies geraakt? Zijn de back-ups nog intact? Moet het management nu al ingelicht worden, of wachten we tot we meer weten? Zullen medewerkers kunnen werken vandaag? Moeten we klanten verwittigen?

Wat stress doet met beslissingen

Onderzoek van Veeam bij organisaties die een ransomware-aanval doormaakten, bevestigt wat de meeste IT-managers uit ervaring al weten: 45% van de betrokkenen rapporteert een sterk verhoogde werklast na een incident, en 40% ervaart een duidelijke toename van stress.

Datzelfde onderzoek toont een tweede, minstens even belangrijk patroon: organisaties die vóór een aanval overtuigd waren goed voorbereid te zijn, zagen dat vertrouwen na een incident met meer dan 20% dalen.

Bijna alle bevraagde organisaties (98%) hadden een ransomware-draaiboek, maar minder dan de helft had daarin de essentiële technische elementen opgenomen, zoals geverifieerde back-upfrequenties of een vooraf vastgelegde commandostructuur. Een draaiboek dat op papier bestaat, maar niet is doorleefd, biedt weinig houvast op het moment zelf.

Beslissingen die in normale omstandigheden weloverwogen worden genomen, worden tijdens een crisis vaak overhaast genomen, precies op het moment dat zorgvuldigheid het meest telt.

De impact op één enkele medewerker

Niet elk incident is een aanval van buitenaf. Soms is de oorzaak van dataverlies een persoonlijke fout of een fout in een interne procedure, en is de impact beperkt tot één individu, wat het niet minder ingrijpend maakt.

Een medewerker van een IT-bedrijf vertelde ons hoe hij op een ochtend merkte dat zijn Microsoft 365-account niet meer bereikbaar was. Door een fout in een offboarding-procedure was hij, terwijl hij nog steeds in dienst was, meegenomen in het offboarding-traject van zijn (grote) werkgever.

Gevolg: zijn volledige account, inclusief mailbox, was verwijderd. Zijn organisatie had geen aparte back-up van Microsoft 365-data, een aanname die veel organisaties nog steeds maken, in het geloof dat Microsoft dit al afdekt.

Ondanks herhaalde pogingen, zowel intern als rechtstreeks bij Microsoft, duurde het een volledige week voor er iets kon worden gerecupereerd. Wat uiteindelijk terugkwam, was slechts een zeer beperkt deel van zijn mailbox. Zijn notities in OneNote was hij definitief kwijt. Vooral het verlies van de koppeling tussen die notities, documenten en de bijhorende e-mails woog zwaar.

Dit voorbeeld illustreert een dimensie die in de businesscase voor back-up vaak onderbelicht blijft: de impact van dataverlies is niet enkel een kwestie van bedrijfsbrede downtime.

Ze kan zich evengoed beperken tot één medewerker, wiens productiviteit, projectkennis en werkcontext plots weken worden teruggezet, zonder dat er ooit sprake was van een aanval, een ransomware-incident of zelfs maar een technische storing.

Wat het verschil maakt

In organisaties die goed voorbereid zijn, ziet diezelfde maandagochtend er fundamenteel anders uit.

Er is een vooraf afgesproken escalatieprocedure: iedereen weet wie wat beslist, en wanneer. Er is een partner die binnen het uur mee aan tafel zit om gestructureerd te werk te gaan: welke systemen zijn geraakt, welke back-ups zijn intact en onaangetast, wat is de snelste veilige weg naar herstel?

Het verschil zit niet in de afwezigheid van stress, want een incident blijft ingrijpend. Ook met de beste voorbereiding. Het verschil zit in de aanwezigheid van houvast: een duidelijk stappenplan, een partner die de technische kant beheerst zodat het interne team zich kan focussen op communicatie en besluitvorming, en de zekerheid dat er een betrouwbare, onaangetaste back-up bestaat om vanuit te herstellen.

Wat goede voorbereiding concreet verandert

Een organisatie met een getest herstelplan en immutable back-ups moet tijdens een incident niet meer de vraag stellen “kunnen we onze data ooit nog terugkrijgen?”

De vraag verschuift naar “hoe snel kunnen we, volgens plan, weer operationeel zijn?”

Dat is een fundamenteel ander gesprek, met een fundamenteel ander effect op de mensen die het moeten voeren.

CONCLUSIE

Voorbereiding beschermt mensen, niet enkel data

Een back-up- en herstelstrategie wordt vaak uitsluitend in technische en financiële termen besproken.

Maar de meest tastbare impact van een goede voorbereiding is misschien wel de meest onderschatte: minder paniek, minder overhaaste beslissingen, en een team dat weet dat er, ook op het slechtste moment, een uitweg is voorzien.

SLOTBESCHOUWING

Downtime is geen kwestie van als, maar van wanneer

Geen enkele organisatie is immuun voor een incident, ongeacht de grootte, de sector, of het budget dat naar IT-beveiliging gaat.

Wat wél binnen je controle ligt, is hoeveel dat incident je kost, hoe lang het duurt, en hoe goed je team en je organisatie ervoor staan op het moment zelf.

Met dit ebook willen we je het kader geven om dat gesprek te voeren: een rekenmodel om de kost van stilstand te becijferen, inzicht in waarom back-ups net op het beslissende moment falen, een framework om RTO en RPO als businessbeslissing te bespreken, een leidraad om back-up in te zetten als aantoonbare compliance-maatregel, en een eerlijk beeld van wat een incident menselijk met een organisatie doet.

YOU FOCUS, WE MANAGE.

Hoe kan Epact helpen?

Bij Epact combineren we Veeam-technologie met immutable, offsite opslag en, waar gewenst, volledig beheerde back-up- en herstelplanning, zodat back-up niet langer een onbeantwoorde vraag is op het moment dat het telt.

Van Zero Effort Server- en M365-back-ups, over Veeam Data Cloud, tot Disaster Recovery as a Service: we bouwen mee aan een herstelstrategie die aansluit bij de RTO- en RPO-doelstellingen van jouw organisatie, en aan de compliance-eisen die daarbij horen.

Wil je weten of je huidige back-upstrategie daar een geloofwaardig antwoord op biedt? We denken graag met je mee, vrijblijvend.

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