

# VIJF BEST PRACTICES VOOR HET BESCHERMEN VAN BACK-UPGEGEVENS

Back-up encryptie moet een van de vele maatregelen zijn waaruit een uitgebreide beveiligingsstrategie bestaat. In veel organisaties heeft opslag een tijdlang buiten het blikveld van beveiligingsmedewerkers gelegen, aangezien ze primair waren gericht op gebieden als perimeterbeveiliging, opsporing/preventie van binnendringing en bescherming van host-systemen. Met als gevolg dat de infrastructuur voor dataopslag - primaire opslag en vooral kopieën van primaire opslag - waarschijnlijk de achilleshiel vormt op het gebied van beveiliging. Beleid voor gegevensbeveiliging is een zaak van de onderneming en moet een fundamenteel element van de beveiligingsstrategie van het bedrijf vormen. Strategisch beveiligingsbeleid kan vervolgens leiden tot tactisch en operationeel beleid, waarbij er gezamenlijke inspanningen worden geleverd door de teams verantwoordelijk voor het netwerk, de infrastructuur en de dataopslag. Daarom moet dataopslag een integraal onderdeel van de beveiligingsstrategie van de onderneming worden.

Om deze doelstellingen te bereiken, moet een beleid worden geformuleerd op vijf fundamentele gebieden:

- 01** Toewijzen van verantwoordelijkheid, aansprakelijkheid en autorisatie
- 02** Beoordelen van risico
- 03** Ontwikkelen van een programma voor databeveiliging
- 04** Het programma communiceren
- 05** Het programma uitvoeren en testen

## 01 WIJS VERANTWOORDELIJKHEID, AANSPRAKELIJKHEID EN AUTORISATIE TOE

Maak dataopslag een onderdeel van het totale informatiemanagement beleid en architectuur. Ook wanneer er wordt besloten dat de verantwoordelijkheden voor de beveiliging van back-ups of opslag bij een separaat team moeten liggen, dan moeten deze beveiligingsmaatregelen toch worden geïntegreerd met de maatregelen waarmee de rest van de infrastructuur wordt beveiligd.

Verdeel taken op plaatsen waar gegevens zeer gevoelig zijn. Het is verstandig om ervoor te zorgen dat de persoon die autorisatie geeft voor toegang niet de persoon is die verantwoordelijk is voor de uitvoering.

**90%**  
van de bedrijven die  
zeer veel gegevens  
verliezen, gaat binnen  
twee jaar failliet.

**SOURCE:** LONDON CHAMBER OF COMMERCE

## 02 BEOORDEEL OPSLAGRISICO ALS ONDERDEEL VAN INFORMATIEBEVEILIGING

### VOER EEN RISICOANALYSE UIT VAN HET GEHELE BACK-UPPROCES

Managers moeten iedere stap van hun back-upmethodologie onderzoeken op beveiligingskwetsbaarheden. Kan een tapebeheerder heimelijk kopieën van back-uptapes maken? Zijn er dozen met tapes die vrij toegankelijk zijn? Is er sprake van een volledig gesloten bewakingsketen voor uw back-uptapes? Indien back-ups van gegevens in gewone tekst worden gemaakt en ze ook zo worden getransporteerd, dan kunnen dergelijke kwetsbaarheden ertoe leiden dat missiekritieke gegevens een eenvoudig doelwit worden.

### VOER EEN KOSTEN/BATENANALYSE UIT VOOR DE ENCRYPTIE VAN BACK-UPGEGEVENS

Als een risicoanalyse een groot aantal kwetsbaarheden aan het licht brengt, dan moeten organisaties zich serieus afvragen of encryptie wordt gerechtvaardigd. Dit project moet verder gaan dan alleen de kosten voor softwarelicenties en apparaten. Het moet tevens de kosten bevatten van encryptie gerelateerde operationele taken bij processen voor het maken van back-ups en het herstel na rampen, plus de gevolgen van encryptie voor de hersteltijd. De totale kosten van encryptie moeten worden vergeleken met de potentiële risico's en de waarschijnlijkheid van een beveiligingsinbreuk. Om zo te bepalen of het financieel gezien zin heeft om encryptie op grote schaal, kleine schaal of geheel niet te implementeren. Gezien de recente publiciteit is tape-encryptie van gevoelige gegevens een lonende investering.

### GEVOELIGE GEGEVENS HERKENNEN

Weet welke bestanden en databases door de bedrijfsafdelingen als gevoelige informatie worden beschouwd. Op basis hiervan kunnen de bijkomende kosten voor bescherming worden gerechtvaardigd. En weet waar uw gegevens zich bevinden. Gegevens worden vaak gekopieerd binnen de eigen omgeving. Het is belangrijk om beleid en procedures te hebben die een goed inzicht bieden in de locatie van de gegevens op ieder tijdstip. Bedrijven beschikken bijvoorbeeld over informatie op laptops die mogelijk ook op een netwerkstation of in een back-upbewaarpplaats op de pc voorkomt.

## 03 ONTWIKKEL EEN PROGRAMMA VOOR INFORMATIEBESCHERMING

### NEEM EEN BEVEILIGINGSAANPAK IN GEBRUIK DIE UIT MEERDERE LAGEN BESTAAT

Neem een aanpak van gegevensbescherming in gebruik die uit meerdere lagen bestaat door best practices van het gegevensnetwerk toe te passen op het opslagnetwerk. Voeg aparte lagen toe die toegespitst zijn op gegevens die niet worden gebruikt (inactieve data).

- **AUTHENTICATIE** Pas authenticatie op meerdere niveaus en technieken toe. Ter voorkoming van misbruik en misleiding.
- **AUTORISATIE** Voer autorisatieniveaus in die zijn gebaseerd op rollen en verantwoordelijkheden, in plaats van volledige administratieve toegang. Maak indien mogelijk optimaal gebruik van rolgebaseerde administratieve capaciteiten van opslagbeheerapplicaties - met name back-up.
- **ENCRYPTIE** Alle gevoelige gegevens moeten bij het opslaan en kopiëren van encryptie worden voorzien. Tevens moeten alle management-interfacegegevens die worden verzonden over netwerken die niet privé zijn van encryptie worden voorzien. Gevoelige gegevens worden meestal gedefinieerd als informatie die ofwel persoonlijke informatie ofwel bedrijfsgeheimen bevat.
- **CONTROLE** Er moeten logboeken met de administratieve handelingen van alle gebruikers worden bijgehouden om opsporing te bevorderen en verantwoordelijkheid te garanderen.

### MAAK KOPIEËN VAN UW BACK-UP TAPES

Vertrouwen op één kopie van gegevens is nooit een goed idee. Hoewel tapemedia een lange levensduur kan hebben, is de media ontvankelijk voor omgevingsomstandigheden en fysieke schade. De aanbevolen best practice is het kopiëren van back-uptapes en deze vervolgens extern bewaren. De aanbevolen methode voor het kopiëren van back-uptapes is het schrijven van een nieuwe tape door de originele tape te lezen. Deze methode heeft als voordeel dat er wordt gecontroleerd of de back-upgegevens kunnen worden gelezen en dat het enige moment waarop er fouten kunnen ontstaan bij het maken van de back-uptape wordt geëlimineerd.

Vanuit praktisch standpunt kost het maken van back-ups te veel tijd. Vanuit praktisch standpunt kost het maken van back-ups te veel tijd, waardoor het lastig is de gegevens op tijd te kopiëren. Er zijn verschillende methodes om dit probleem op te lossen. De eerste methode begint met het optimaliseren van het back-upstelsel om de hoeveelheid tijd die nodig is voor het voltooiën van de originele back-up terug te dringen. Vervolgens kunnen er meerdere zeer snelle tapestations worden gebruikt voor het maken van de tweede kopie voor bewaring off-site. Een andere methode is het gebruiken van de functionaliteit van sommige back-upsoftwarepakketten voor het gelijktijdig maken van zowel een origineel als een kopie.



Hoewel deze methode niet over het verificatievoordeel beschikt dat in de vorige paragraaf werd besproken, bespaart u hiermee de tijd die nodig is voor het maken van kopieën - elk type kopie is beter dan geen kopie. Ongeacht de grootte van uw organisatie kan een combinatie van zeer snelle tapeapparaten, virtuele tapebibliotheken en professionele services helpen bij het voldoen aan deze belangrijke eis.

### **IMPLEMENTEER EEN VEILIGE, VOLLEDIG GESLOTEN BEWAKINGSKETEN VOOR MEDIABEHEER.**

Een bewakingsketen verwijst naar de handeling, methode, beheer, toezicht en/of controle van media of informatie (gewoonlijk, maar niet altijd, tape). Het uiteindelijke doel van een succesvolle bewakingsketen is het behouden van de integriteit van de bronnen. Bij de bewakingsketen moet rekening gehouden worden met zaken die hieronder beschreven worden.

Verwisselbare media moet worden getraceerd met behulp van barcodes. Duidelijke rapportages moeten inzichtelijk maken waar de media zich bevinden. Een best practice is het genereren van een dagelijkse rapportage met een overzicht van de tapes die extern worden opgeslagen en tapes die moeten worden opgevraagd uit off-site opslag om te worden gerecycled of vernietigd. Er moeten gedocumenteerde standaardprocedures zijn om te garanderen dat deze maatregelen worden uitgevoerd.

De beveiliging van de off-site locatie en het proces dat wordt gebruikt voor toegang tot de off-site opslag moet worden geanalyseerd. Media moet in afgesloten containers (koffers) worden geplaatst voordat ze het computercentrum verlaten. Het traceren gebeurt vervolgens op "containerniveau". Om optimaal te kunnen traceren, dient de barcode van de tapecontainer bij elke handeling en of verplaatsing te worden gescand. Dus ook in computercentra en op de externe opslaglocaties. Medewerkers moeten tekenen voor de overdracht van mediacontainers. En de containers mogen nooit onbewaakt gelaten worden.

Vergelijk de inventaris van media die extern wordt opgeslagen regelmatig (ten minste maandelijks) met de inventaris van tapes die in eigen beheer worden bewaard. Aan het einde van de maand moet

een fysieke scan van de off-site opslag worden vergeleken met de records van de back-up/archiveringsapplicatie om inconsistenties op te sporen. Bij onbekende media moeten er gepaste stappen worden genomen.

Zodra de media is verouderd of de integriteit ervan niet meer kan worden gegarandeerd, moet deze op geschikte wijze worden vernietigd. Vernietiging van magnetische media wordt meestal uitgevoerd door middel van een vernietigingsproces voor de cartridge, ofwel door de gegevens op de tape onleesbaar te maken, of door de tape in zijn geheel te vernietigen waardoor hij onbruikbaar wordt. Gegevensvernietiging kan on-site worden uitgevoerd met de geschikte demagnetiseerapparatuur of via een service van een externe partij. (Bij het on-site vernietigen van gegevens dient te worden gecontroleerd of de demagnetiseerapparatuur geschikt is voor de desbetreffende media.) Gegevensvernietiging kan het beste worden uitgevoerd door een organisatie die over een vernietigingscertificaat beschikt.

### **BEGRIJP DE BEWAKINGSKETEN VAN UW GEGEVENS**

Een ander kritiek element is dat de partij waar de tapes extern worden opgeslagen ook de best practices volgen. Hier volgt een overzicht van belangrijke basispunten:

- **KWETSBAARHEID ON-SITE** Laat tapes niet achter in een niet afgesloten container, zoals een open kartonnen doos, bij de receptie voordat ze worden afgehaald. De pick-up moet voldoen aan een standaardprocedure waarbij een verantwoordelijke IT-medewerker de tapes overdraagt en een handtekening krijgt van een bekende vertegenwoordiger van de leverancier die zich kan legitimeren.
- **ACHTERGRONDCONTROLES** Wanneer een bedrijf uw kritieke gegevens opslaat, moet u er zeker van zijn dat het bedrijf haar medewerkers grondig screent.
- **HET BEDRIJF MOET OVER EEN GESLOTEN BEWAKINGSKETEN BESCHIKKEN** Bespreek met de aanbieder van off-site opslag het gehele proces van hoe er van begin tot einde met de media wordt omgegaan. Let op speciale aandacht voor fysieke beveiliging plus audit- en controlemechanismen om te garanderen dat het

proces wordt nageleefd. Het is aan te raden om gevoelige gegevens te verplaatsen in een voertuig met de naam van de aanbieder, zodat duidelijk zichtbaar is dat er gevoelige gegevens worden vervoerd.

- **BEVEILIGDE CONTAINEROPSLAG** Bij beveiligde containeropslag vindt er tracking plaats van bakken of dozen, maar niet van hun inhoud. De meeste off-site opslagaanbieders ondersteunen dit type van beveiligde opslag.
- **FYSIEKE BEVEILIGINGSCONTROLES** Opslagfaciliteiten moeten op geschikte wijze worden beveiligd. Niet-geautoriseerde personen mogen geen toegang kunnen krijgen tot de kluizen.
- **OMGEVINGSCONTROLES** Tapes en andere media mogen nooit worden opgeslagen in de kofferruimte van een voertuig of op een andere locatie waar de omgevingsfactoren oncontroleerbaar zijn.. Bij tapeopslag moet rekening worden gehouden met optimale bewaarcondities, zoals een optimale temperatuur en luchtvochtigheid plus statische controle. Stof is de vijand van de meeste media en mediaopnameapparatuur. De back-up- en archiefomgeving moet schoon en stofvrij blijven. Er moet een zachte, niet statische doek worden gebruikt om de buitenkant van de cartridges te reinigen en het stof moet worden verwijderd uit de sleuven van een bibliotheek of opslagrek door middel van perslucht uit een spuitbus. De tapes moeten worden vervoerd in een elektrostatische houder en mogen niet in een bak of een kartonnen doos worden opgestapeld. Hoewel ze zeer duurzaam lijken, kunnen tapes op eenvoudige wijze worden beschadigd als er niet goed mee wordt omgegaan.

### **OVERWEEG ELEKTRONISCHE BEVEILIGDE OPSLAG**

U kunt overwegen gegevens elektronisch op te slaan, zodat het niet langer nodig is informatie op fysieke media in een voertuig te transporteren. Er zijn diverse bedrijven die de mogelijkheid bieden om back-ups van gegevens via internet te maken. De back-up gegevens kunnen van encryptie worden voorzien en via internet naar een extern datacentrum worden verzonden. Elektronische beveiligde opslag is wellicht geen praktische

oplossing voor alle bedrijfsgegevens, maar het kan handig zijn voor gegevens die worden gedistribueerd op file servers en pc's. Gedistribueerde gegevens kunnen 60% van de informatie van een bedrijf uitmaken en het IT-beheer ervan is lastig.

Verzeker u ervan dat de aanbieder van deze services de gegevens van encryptie voorziet tijdens de overdracht en de opslag. Bespreek tevens met de aanbieder hoe de informatie beschikbaar wordt gehouden. Wordt de informatie op tape gezet? Wordt de informatie gekopieerd naar een andere locatie? Bespreek tevens met de aanbieder hoe de informatie beschikbaar wordt gehouden ter ondersteuning van herstel of rechtszaken.

**Wanneer u uw bedrijfskritieke gegevens bij een externe partij opslaat, moet u er zeker van zijn dat dit bedrijf haar medewerkers grondig screent.**

## 04 COMMUNICEER DE PROCESSEN MET BETREKKING TOT INFORMATIEBESCHERMING EN -BEVEILIGING

Nu het proces is voor databeveiliging en bescherming goed is gedefinieerd, is het belangrijk om u er van te verzekeren dat de mensen die verantwoordelijk zijn voor de veiligheid van de gegevens goed op de hoogte en getraind zijn. Beveiligingsbeleid is het belangrijkste aspect van het toewijzen van verantwoordelijkheid, aansprakelijkheid en autorisatie.

### INFORMEER BEDRIJFSMANAGERS OVER RISICO'S, TEGENMAATREGELEN EN KOSTEN

Gegevensverlies en diefstal van intellectueel eigendom zijn een zaak voor het bedrijf, niet voor IT. Daarom moet de Chief Information Security Officer (CISO) bij gegevensbeveiliging altijd beginnen met het informeren van leidinggevenden over de risico's, bedreigingen en potentiële verliezen als gevolg van beveiligingsinbreuken, plus de kosten van diverse beveiligingsopties met tegenmaatregelen. Op deze manier kunnen leidinggevenden weloverwogen beslissingen nemen met betrekking tot het kosten/batenprofiel van investeringen in gegevensbeveiliging.

### BEOORDEEL HET RISICO EN TRAIN MEDEWERKERS

Organisaties die risico's beoordelen en medewerkers trainen zijn eerder geneigd beveiligingsbeleid, procedures en technologieën te implementeren om cruciale bedrijfsmiddelen te beschermen. En een kwetsbare infrastructuur en ongeschoolde medewerkers vormen een potentieel probleem dat zich snel zal openbaren - het is dus zeker de moeite waard om het basiswerk voor beveiliging uit te voeren.

## 05 IMPLEMENTEER EN TEST HET PROGRAMMA VOOR INFORMATIEBEVEILIGING

Bij veilige gegevensbescherming draait het niet om de technologie maar om het proces. Daarom is het belangrijk om het proces te testen. Naarmate een bedrijf groeit, dient de informatie- en databeveiliging worden aangepast; vandaar dat de practices voor informatiebeveiliging ook moeten veranderen. Zodra het volledige plan is ontwikkeld, gedefinieerd en gecommuniceerd aan de desbetreffende mensen, is het tijd voor de uitvoering ervan. Verzeker u ervan dat de middelen, technologieën en methodes aanwezig zijn die moeten worden ingezet voor informatieclassificatie.

Test het proces zodra het in gebruik is genomen. Onthoud dat de test betrekking moet hebben op zowel back-up als herstel. Probeer iedere denkbare bedreiging in het proces te introduceren, inclusief server- en tapeverlies, netwerkproblemen, apparatuurproblemen, problemen met gegevensclassificatie en ieder ander scenario dat van invloed op het bedrijf kan zijn. Voer de test uit met medewerkers die minder bekend zijn met het proces. Zo kan er worden vastgesteld dat of het proces eenvoudig te volgen en uitvoerbaar is. Ook wanneer de normale medewerker niet beschikbaar is vanwege ziekte, vakantie of ontslag.

# Het kost **19 dagen** om 20 MB aan verloren gegevens opnieuw te typen.

BRON: REALTY TIMES

# Elke **15 seconden** crasht een harde schijf.

BRON: HARRIS INTERACTIVE

# Elke dag worden **2000 laptops** gestolen of verloren.

BRON: HARRIS INTERACTIVE

# INFORMATIEBEHEER IS EEN COMPLEXE UITDAGING... EN WIJ HELPEN U GRAAG MET UITGEBREIDE OPLOSSINGEN. ZODAT U ZICH KUNT RICHTEN OP UW KERNACTIVITEITEN!

Wij kunnen u helpen bij het vereenvoudigen van uw informatiebeheer, het besparen van kosten en het vergroten van de efficiëntie.



**ANALYSEREN  
EN ADVISEREN**



**OPSLAAN EN  
BEVEILIGEN**



**SCANNEN EN  
DIGITALISEREN**



**FLEXIBELE  
TOEGANG**



**VEILIGE  
VERNIEUWING**

## EEN PARTNER WAAROP U KUNT VERTROUWEN

Wij bieden gespecialiseerde service, ongeacht uw bedrijfsgrootte en sector, die is gebaseerd op de volgende kernprincipes:

### VERTROUWEN

Al bijna 60 jaar lang zijn wij de vertrouwde partner van bedrijven in alle soorten en maten. Wij zijn actief vanuit meer dan 1000 faciliteiten wereldwijd.

### BEVEILIGING

Met onze streng beveiligde vestigingen, gescreende teams en geoptimaliseerde processen is uw informatie altijd in veilige handen.

### EXPERTISE

Onze kracht en diepgaande kennis zijn onlosmakelijk verbonden met onze medewerkers, processen en technologieën. Doordat wij inzicht hebben in compliance kwesties kunnen wij u helpen uw informatiemiddelen optimaal te benutten en tegelijkertijd de kosten te verlagen.

### KLANTGERICHTHEID

Met 24 uur per dag ondersteuning streven we naar optimale klantenservice.

### DUURZAAMHEID

Door u te helpen de hoeveelheid te bewaren informatie te beperken en alle documenten te recyclen die u niet nodig hebt, kunnen wij u ondersteunen om aan uw eigen duurzaamheidsbeloften te voldoen.

## NEEM VANDAAG NOG CONTACT MET ONS OP

We geven u graag meer informatie of advies over hoe u uw informatiebeheer kunt optimaliseren.

[www.ironmountain.nl](http://www.ironmountain.nl)

0800 272 4433

[www.ironmountain.be](http://www.ironmountain.be)

02 712 20 20



© 2010 Iron Mountain Incorporated. Alle rechten voorbehouden. Iron Mountain en het ontwerp van de berg zijn geregistreerde handelsmerken van Iron Mountain Incorporated. Alle andere handelsmerken zijn eigendom van hun respectieve eigenaren.

NL-B-OSDP-02-0610-01-NL