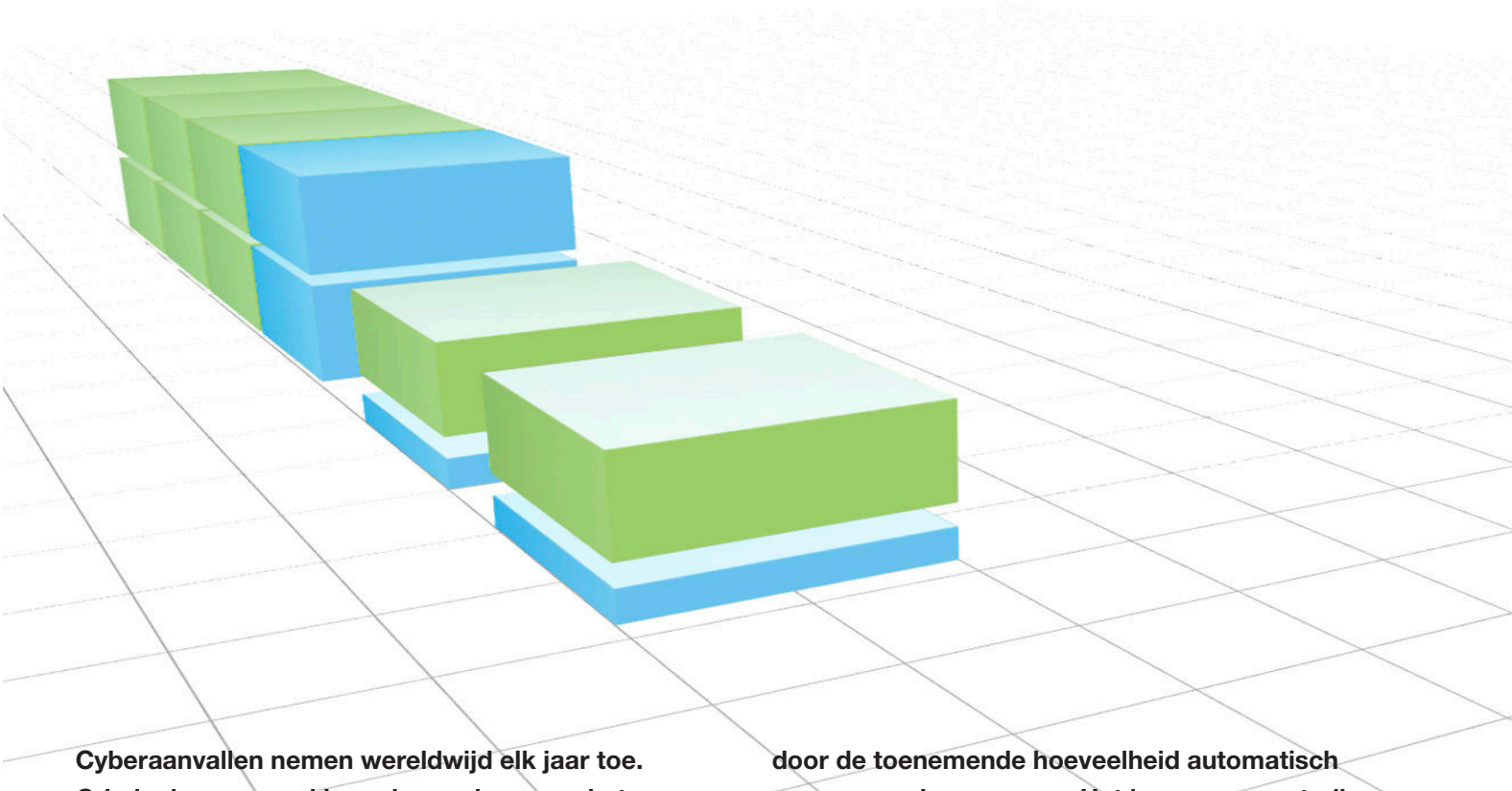
FAST LTA

Minder (back-up) is meer (zekerheid):

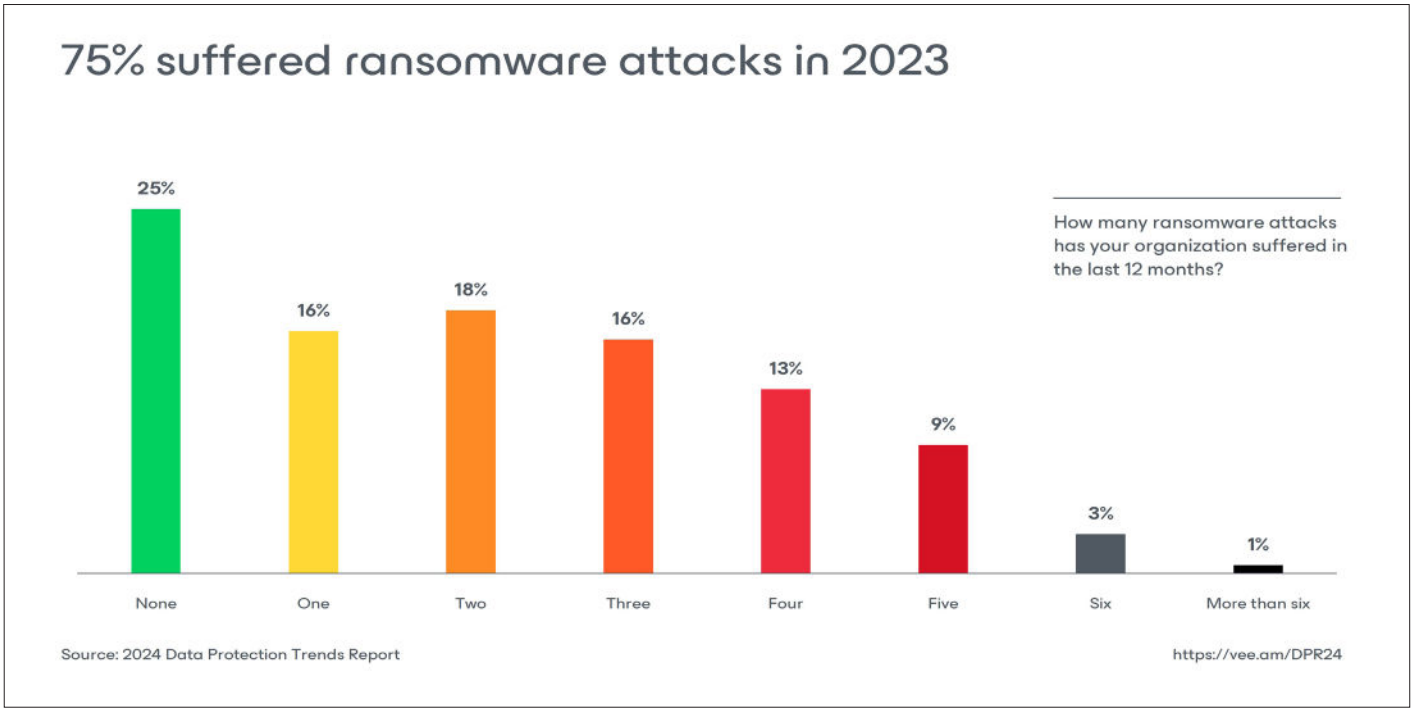
Het actieve WORM-archief als onderdeel van de gegevensback-up



Cyberaanvallen nemen wereldwijd elk jaar toe. Criminelen geven al lang de voorkeur aan het aanvallen van gegevensback-ups als middel om snel herstel na een aanval te voorkomen. Daarom worden back-up- en herstelstrategieën steeds complexer en duurder. Tegelijkertijd blijft de capaciteit waarvan een back-up moet worden gemaakt toenemen door de toenemende hoeveelheid automatisch gegenereerde gegevens. Het in een vroeg stadium uitbesteden van grote hoeveelheden data aan een WORM-archief kan helpen om de complexiteit en de kosten onder controle te houden, de beveiliging op lange termijn te garanderen en de inspanning die nodig is voor herstel aanzienlijk te verminderen.

Initiële situatie

De nationale cyber security centra in Europa blijfen adviseren om "werkende back-ups" te gebruiken tegen de gevolgen van een cyberaanval. De overgrote meerderheid van professionele gebruikers zal deze aanbeveling nu waarschijnlijk opvolgen. Een werkende back-up moet geavanceerde beschermingsmechanismen, regelmatige en uitgebreide hersteltests en "offline" gedocumenteerde noodplannen omvatten. Rekening houdend met en voortdurend aangepast aan de classificatie van verschillende gegevenstypen en -bronnen, resulteert dit in back-upstrategieën waarvan de implementatie moet worden gecategoriseerd binnen de klassieke conflictdriehoek van prestaties, capaciteit en budget. Verschillende gebieden worden verschillend beoordeeld en geïmplementeerd, afhankelijk van de respectievelijke RTO- en RPO-richtlijnen. De fundamentele wens om een back-up te maken van alle gegevens met maximale prestaties en het hoogste beveiligingsniveau mislukt in de overgrote meerderheid van de gevallen vanwege het beschikbare budget, maar ook vanwege wettelijke hindernissen die bijvoorbeeld regelmatige fysieke isolatie (air gap) vereisen.



Aanvalsscenario

Zoals Florian Lohoff beschrijft in zijn bijdrage aan het "Storage in Focus" evenement (Storage in Focus - 26 oktober 2023), vinden cyberaanvallen plaats in verschillende stadia. In de regel zijn aanvallers actief in de IT-infrastructuur lang voordat iemand een aanval opmerkt en krijgen ze toegang tot allerlei systemen zonder directe schade aan te richten. Gegevens worden pas actief afgeluisterd, versleuteld en/of verwijderd als er een dreiging van ontdekking is of een geschikt moment voor de aanvallers. De snelheid waarmee de toegang voor bestaande gebruikers en beheerders dan onmiddellijk verloren gaat, verbaast zelfs professionals keer op keer. Vaak is de enige onmiddellijke maatregel het onmiddellijk loskoppelen van alle systemen waartoe je direct toegang hebt van het netwerk en de stroomvoorziening. Dit is het begin van schadebeperking, inventarisatie, forensisch onderzoek en herstel.

Bescherming door Immutability

Aangezien bijna alle aanvallers nu proberen om eerst de back-up van gegevens te compromitteren en zo te voorkomen dat deze snel kan worden hersteld, vereisen back-upgegevens ook speciale maatregelen om ze te beschermen tegen manipulatie en verwijdering. De term "immutability", d.w.z. de onveranderlijkheid van de back-upgegevens, is hier ingeburgerd. Eenvoudig gezegd, de back-upgegevens zijn beveiligd tegen overschrijven en kunnen pas na een bepaalde tijd worden gewist. Afhankelijk van het systeem, de opslaglocatie en de implementatie biedt deze functionaliteit meer of minder goede bescherming voor back-upgegevens. In de meeste gevallen is het een softwarefunctie van de back-upsoftware of het opslagsysteem of de serviceprovider die speciale gebruikersrechten vereist en daarom "buiten" de omgeving ligt die toegankelijk is voor de aanvaller - dat is tenminste de belofte. Zoals alle softwarefuncties is dit alleen zo veilig als de implementatie, realisatie en zorg toelaten.

Speciale vormen van immutability berusten op hardwarebescherming. Een fysieke scheiding van de back-upgegevens (air gap) zorgt er bijvoorbeeld voor dat toegang eenvoudigweg niet meer mogelijk is. Zolang het betreffende medium geen verbinding heeft met een live systeem, kan er geen manipulatie of verwijdering plaatsvinden. Aangezien deze bescherming verder kan worden beveiligd door media op een veilige locatie op te slaan, bijvoorbeeld in een bankkluis, zijn deze scenario‘s zelfs verplicht voor veel bedrijven en overheden. Het gebruik van Air Gap brengt echter ook beperkingen met zich mee die snel herstel en kostenreductie in de weg staan. Na een aanval moeten opgeslagen media eerst worden gecontroleerd en vervolgens worden hersteld naar een "schoon" systeem. Afhankelijk van het beveiligingsniveau en medium is dit een tijdrovende en kostbare procedure. Bovendien moeten de gegevens op zo‘n medium "op zichzelf staand" zijn, d.w.z. ze mogen niet afhankelijk zijn van andere gegevens op andere media. Dit betekent dat eigenlijk alleen volledige back-ups kunnen worden opgeslagen op air-gap media, wat de benodigde tijd en capaciteit verhoogt. Als gevolg hiervan moeten de media zo goedkoop mogelijk zijn, wat de reden is waarom tape meestal wordt gebruikt - wat op zijn beurt de hersteltijd aanzienlijk verlengt in vergelijking met media zoals Silent Bricks, die zijn gebaseerd op harde schijven of SSD‘s.

Een andere hardwaremethode is immutability via hardware WORM. In tegenstelling tot softwaremethoden kan dit type schrijfbeveiliging niet worden uitgeschakeld en is het dus 100% veilig. Hardware WORM is echter niet geschikt voor klassieke back-upscenario‘s om precies deze reden. Back-upgegevens hebben per definitie een beperkte levensduur en worden op een gegeven moment verwijderd of overschreven. Als back-ups op WORM-media zouden worden gerealiseerd, zouden de kosten voor de aanschaf en het gebruik van steeds grotere opslagsystemen voortdurend stijgen.

Toch worden tapes met volledige back-ups nog steeds vaak misbruikt als "archief" en voor lange tijd opgeslagen. De gunstige prijs per TB van de media verleidt mensen vaak om de zin van deze maatregel in twijfel te trekken zonder de latere kosten in overweging te nemen. Vanwege de slechte achterwaartse compatibiliteit van LTO (tapes van de ene generatie kunnen alleen worden gelezen door drives van de volgende generatie), is het noodzakelijk om de juiste, onderhoudsgevoelige drives te blijven gebruiken. Omdat tapes geen inherente beveiligingsmechanismen hebben, moeten gegevens op tapes regelmatig worden gecontroleerd en vervolgens gekopieerd vanwege mechanische slijtage. Bovendien zijn gegevens op tapes in eerste instantie onbruikbaar, totdat ze hersteld worden naar een systeem dat productief gebruikt kan worden. Dit kan in uitzonderlijke gevallen nog steeds zinvol zijn als een "last line of defense full back-up", maar archiefgegevens op tapes muteren in pure datakerkhoven.

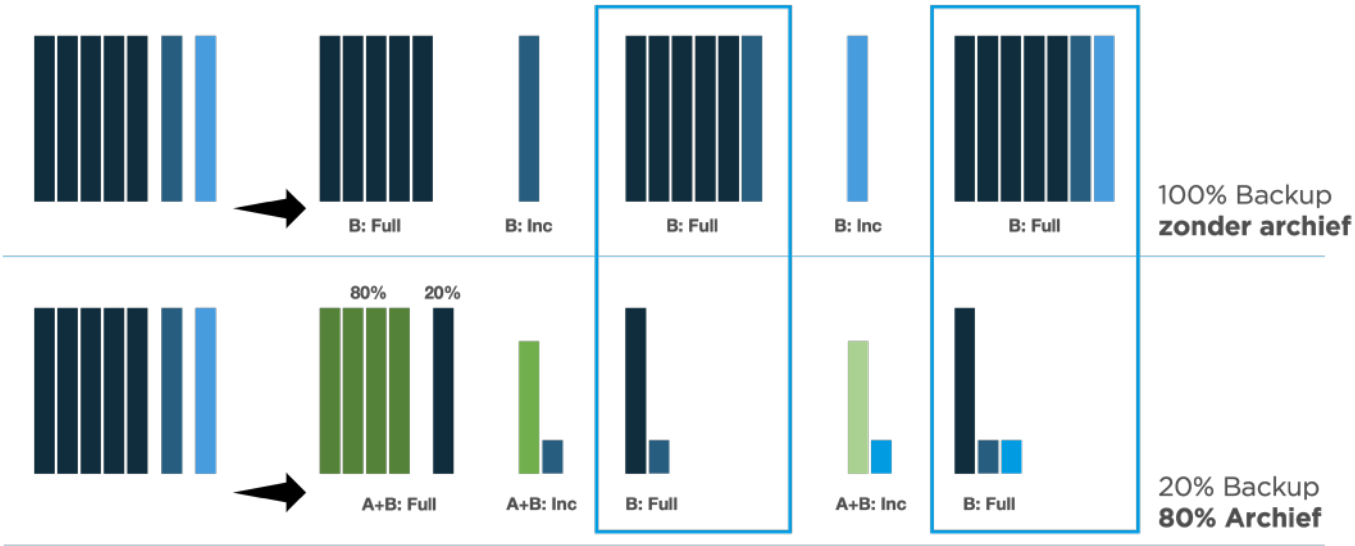
Achtergrond van Immutable Storage:
https://www.comex.eu/wp-content/uploads/2024/02/nl-2022-08-Immutable-Storage-2023-4c.pdf

Het archiefdilemma

WORM opslag is relevanter voor archieven waar de focus ligt op lange termijn opslag. In tegenstelling tot back-ups worden gegevens niet gedupliceerd, maar verplaatst van het productieve systeem. Dit leidt echter tot het klassieke archiefdilemma: welke gegevens kunnen van de productieve opslagsystemen worden verwijderd en naar archiefopslag worden verplaatst - en wie beslist hierover? De manier waarop archieven tot nu toe zijn geïmplementeerd, speelt hier een beslissende rol. Gegevens in "koude" tape-archieven zijn feitelijk uit de opslag verwijderd en zijn niet langer toegankelijk. Voordat gegevens toegankelijk zijn, moeten ze worden gelokaliseerd, gecontroleerd en hersteld vanaf de relevante media.

Als dit, zoals hierboven beschreven, ook een volledige back-up is (en geen gearchiveerde data), moet de restore ook via het back-upsysteem worden uitgevoerd - alleen dan kunnen de gegevens opnieuw worden gebruikt. Voor de gebruiker staat zo'n archief dus in de meeste gevallen gelijk aan het wissen van de data. Ook daarom zullen noch gebruikers noch IT-beheerders massaal data naar een archief verplaatsen; het "risico" dat individuele data opnieuw nodig zijn is te groot. De basisregel is daarom: alleen de data die echt niet meer nodig is, maar (om welke reden dan ook) niet verwijderd mag worden, wordt naar een archief verplaatst.

Het resultaat: steeds grotere hoeveelheden statische gegevens "verstoppen" het back-upproces, wat leidt tot enorme back-upvensters, waardoor nieuwe opslagsystemen en steeds complexere beschermingsmechanismen nodig zijn. Over verwijderen gesproken: machine learning en AI-toepassingen zorgen ervoor dat gegevens over het algemeen toch niet meer worden verwijderd. Vooral het perspectief van lokale AI-systemen, waarvan de kwaliteit afhankelijk is van de beschikbaarheid van interne gegevens, voorkomt dat gegevens worden "opgeschoond". In "koude" archieven zijn deze gegevens echter ook niet toegankelijk en moeten ze tegen hoge kosten worden hersteld, wat de bruikbaarheid verder beperkt.



Illustratie:
Volledige back-ups worden te vaak misbruikt als quasi-archief. Enerzijds zorgt dit voor een enorme toename in opslagcapaciteit. Anderzijds worden back-upvensters en vooral de hersteltijd voortdurend verlengd, waardoor het herstel na een cyberaanval aanzienlijk wordt vertraagd.

Heroverweging: het actieve archief

Dit kan worden voorkomen door archieven "actief" te maken. In plaats van pure offline media (tape), zijn actieve archieven gebaseerd op harde schijven of SSD's en zijn ze zowel energiebesparend als volledig bruikbaar binnen enkele seconden dankzij slim energiebeheer. Dit neemt de grootste hindernis weg voor de opslag van grote hoeveelheden gegevens en de bijbehorende stroomlijning van de eigenlijke gegevensback-up. Omdat applicaties (en dus gebruikers) op elk moment en transparant toegang hebben tot de gegevens die zijn opgeslagen in het actieve archief, is het voor IT-beheerders eenvoudig om veel meer gegevens te verplaatsen van de productiesystemen naar een gunstigere archiefopslag.

De nieuwe basisregel is daarom: **Het is beter om meer gegevens te verplaatsen en zo de gegevensback-up te reduceren.**

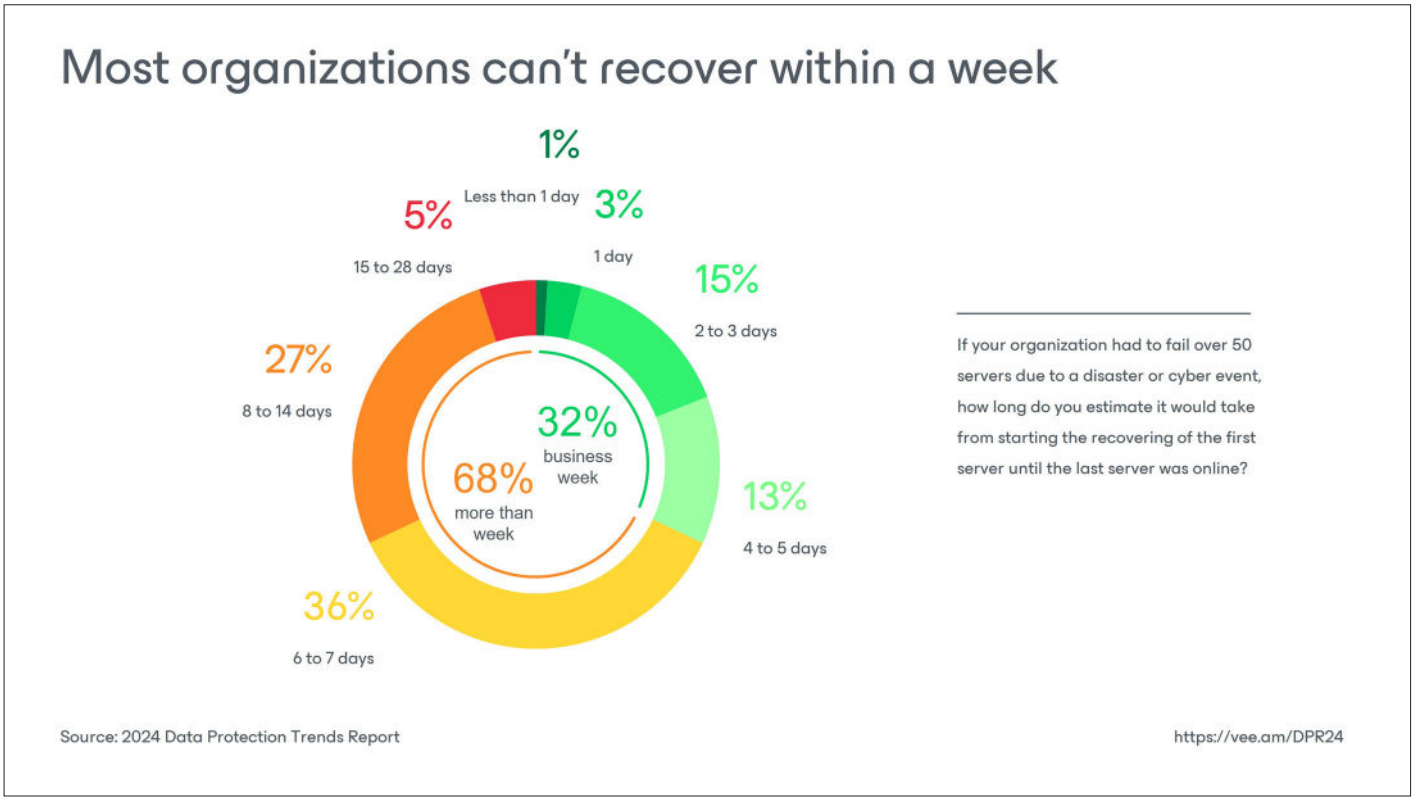
Als gevolg hiervan worden alle data die hoogstwaarschijnlijk niet meer onmiddellijk worden verwerkt, binnen milliseconden beschikbaar moeten zijn of alleen via back-ups kunnen worden opgeslagen, zoals databases, verwijderd uit het klassieke back-upproces. Aangezien steeds meer gegevens automatisch worden gegenereerd, bijvoorbeeld door sensoren, opnames, scans, logs, enz., kunnen deze gegevens al worden opgeslagen in het actieve archief, ongeacht het onmiddellijke gebruik ervan, aangezien ze toch niet mogen of moeten worden gewijzigd. Deze gegevens zijn ook onmiddellijk en op elk moment beschikbaar voor het trainen van AI-systemen of het opzetten van lokale AI-systemen.

Lange tijd zagen archieven er ongeveer zo uit: Datakerkhoven op offline media. Zoeken, vinden en herstellen stonden de daadwerkelijke toegang tot de gegevens in de weg. Archieven werden daarom vooral gebruikt om van gegevens "af te komen".

Actieve archieven maken deel uit van de actieve gegevensstructuur. Ze slaan gegevens transparant op en zijn op elk moment beschikbaar - zonder dat ze eerst moeten worden hersteld.

Voor bescherming: Hardware WORM

In tegenstelling tot een back-up, die per definitie een of meer kopieën van de brondata maakt, is data in het archief enkelvoudig omdat het uit de productiesystemen is verwijderd. Manipulatie of verwijdering van deze instantie betekent daarom een volledig verlies - een scenario dat in elk geval moet worden vermeden. Daarom is het gebruik van hardware WORM om de data in het actieve archief te verzegelen niet alleen verstandig, maar ook noodzakelijk. Om beschermd te zijn tegen alle andere mogelijke oorzaken van dataverlies, moeten de gegevens meerdere keren redundant worden geback-upt, op meerdere locaties worden verspreid en constant worden gecontroleerd op integriteit. Het opslagsysteem stelt daarom aanzienlijk hogere eisen aan de beveiliging dan conventionele back-upopslag. Schaalbaarheid en betrouwbaarheid op lange termijn spelen net zo'n belangrijke rol als levensduur en milieuvriendelijkheid. Energiebesparende, CO2-gecompenseerde en duurzame systemen kunnen een belangrijke bijdrage leveren aan het afremmen van de toenemende belasting van het milieu door steeds meer IT.



Minder back-up is beter

Minder gegevens in productiesystemen betekent dus minder back-up, slankere scenario's, minder complexiteit, minder kans op aanvallen en minder ruimte voor menselijke fouten. Dit alles kan leiden tot aanzienlijke besparingen of flexibelere investeringen, bijvoorbeeld in hogere prestaties voor primaire opslag en primaire back-upopslag, wat de hersteltijd weer aanzienlijk verkort.

Omdat het uitbesteden van grote hoeveelheden data aan een actief archief de back-up stroomlijnt, wordt niet alleen de back-up van data versneld, maar ook het herstel. Om na een aanval weer productief met data te kunnen werken, hoeft er veel minder data te worden hersteld vanuit de gestroomlijnde back-ups. Alle andere gegevens worden onveranderd en onveranderbaar opgeslagen in het archief - net zoals voor de aanval. In tegenstelling tot tape-gebaseerde archiefopslag, is toegang tot individuele data op elk moment en direct na herverbinding mogelijk, zonder tijdrovende restore.

De nieuwe Silent Cubes en Silent Cubes Pro in 19-inch formaat vervangen na ongeveer 15 jaar de klassieke Silent Cube.

Silent Cubes: de standaard voor een actief WORM-archief

Silent Cubes worden al meer dan 15 jaar gebruikt als auditbestendige en wettelijk conforme archiefopslag. De voormalige kubusvormige WORM-opslagunits zijn vooral populair geworden in ziekenhuizen en overheidsinstanties. Naast de nodige certificeringen hebben ze een aantal kenmerken die een probleemloze werking met weinig onderhoud gedurende tientallen jaren mogelijk maken.

De basis van het systeem, in principe ongewijzigd sinds 2007, is de opstelling met 12 gegevensdragers die alle gegevens effectief beschermen tegen manipulatie, wissen en verlies via een speciaal ontwikkelde WORM-controller met viervoudig redundante erasure coding. Tot vier van de 12 gegevensdragers per opslageenheid kunnen uitvallen zonder risico op gegevensverlies. Ter bescherming tegen uitval door batchfouten worden altijd vier datadragers uit verschillende batches gebruikt. Alle gegevens worden regelmatig gecontroleerd door een interne, zelfstandige "digitale audit" en overeenkomstig gerepareerd op basis van de blockchain-achtige codering. De opslageenheden worden bestuurd door een centrale hoofdeenheid. De geïntegreerde optie om systemen te repliceren naar andere locaties via gesloten VPN-tunnels is net zo een standaardvoorziening als het uitgebreide monitoring. Alle systemen worden rechtstreeks ondersteund door FAST LTA voor een periode van 10 jaar of meer onder het "FAST LTA CARE" onderhoudscontract. Terwijl Silent Cubes oorspronkelijk vooral werden gebruikt waar data onveranderlijk moest worden opgeslagen om juridische redenen, zijn ze nu steeds meer in trek als actieve WORM archieven in alle gebieden van de economie. De hoge mate van veiligheid en betrouwbaarheid maken het mogelijk om grote actieve archieven te creëren die alle cyberaanvallen kunnen weerstaan en volledig onder eigen controle blijven dankzij lokaal "off-cloud" gebruik.

Silent Cubes zijn ook CO2-neutraal als elektriciteit uit CO2-neutrale of CO2-positieve bronnen wordt gebruikt. Silent Cubes onderscheiden zich ook op het gebied van energieverbruik. Het slimme energiebeheer in combinatie met de modulaire configuratie zorgt ervoor dat opslagruimtes die niet nodig zijn, volledig kunnen worden uitgeschakeld. Indien nodig is de data echter in slechts enkele seconden weer volledig en individueel beschikbaar dankzij het snelle netwerk van harde schijven.

Sinds 2023 zijn de systemen uitgevoerd in 19-inch formaat voor datacenters en zijn ze ook beschikbaar als Pro-modellen met een snelle 10G-netwerkverbinding.

Hallo.

Onze producten en diensten helpen onze MKB-klanten gegevensbescherming en gegevensmigratie te vereenvoudigen, risico's op het gebied van wet- en regelgeving te minimaliseren en het risico op gegevensverlies op de lange termijn te verkleinen.

Wij zorgen voor je.

Services en onderhoudscontracten zijn elementaire onderdelen van onze aanbiedingen. Flexibele SLA's met 24/7 beschikbaarheid, on-site vervanging van defecte componenten en een looptijd tot 10 jaar tegen dezelfde voorwaarden garanderen maximale gegevensbeveiliging voor onze klanten.

Wij zorgen voor rechtszekerheid.

Zonder de bijbehorende software is een opslagsysteem niet meer dan een stapel harde schijven (of SSD's). Onze software maakt maximale flexibiliteit mogelijk, helpt u te voldoen aan wet- en regelgeving en is gecertificeerd voor de toonaangevende back-up- en archiveringstoepassingen.

Wij ontwikkelen voor uw bescherming.

Onze opslagsystemen zijn speciaal. Speciaal ontwikkeld en geoptimaliseerd om uw gegevens tientallen jaren te beschermen. Speciaal ontwikkelde harddiskcontrollers, modelonafhankelijkheid voor schijven en SSD's, verplaatsbare opslagcontainers zonder offline energievereisten en optionele hardware WORM verzegeling zijn slechts enkele van onze ontwikkelingen.

COMEX | Vogt 21 | NL-6422 RK Heerlen | office@comex.eu | **www.comex.eu**

FAST LTA

FAST LTA | Rüdesheimer Str. 11 | 80686 München | info@fast-lta.de | **www.fast-lta.de**