Ransomware TeslaCrypt, Locky, Wannacry, …

VEILIGE OPSLAG:
BESCHERMING TEGEN RANSOMWARE

Juni 2017 – Matthias Zahn (FAST LTA), Hannes Heckel (FAST LTA), Axel Booltink (COMEX)

Overzicht

Anders dan betalings- en toegangsgegevens hebben persoonlijke data voor criminele aanvallers geen directe verkoopwaarde. Zelfs specifieke bedrijfsinformatie is in de meeste gevallen niet verkoopbaar. Voor de eigenaren van de data is de opgeslagen informatie echter vaak zeer waardevol en het verlies ervan kan het voortbestaan van een bedrijf in gevaar brengen.

Nieuwe computervirussen verhinderen daarom de toegang tot deze gegevens door encryptie en de beheerders van deze virussen proberen een losgeld voor het vrijgeven van de data af te persen. Deze vorm van afpersing noemen we ransomware.

Volledige bescherming tegen deze aanvallen wordt steeds moeilijker. Alleen regelmatige ‘koude’ back-ups bieden de mogelijkheid een onaangetaste dataset te herstellen.

Het juiste storagesysteem kan dit proces vereenvoudigen en gegevens écht betrouwbaar tegen ongeautoriseerde encryptie beveiligen.

De motivatie voor een aanval

Malware wordt om verschillende redenen ontwikkeld en ingezet. In de filmklassieker ‘War Games’ hackt een puber de commandocentrale van het militair van de VS en veroorzaakt bijna een wereldoorlog – in de huidige tijd zeker geen realistisch scenario.

Toch zijn er net zoals in de film steeds nog niet-criminele hackers die op zich geen schade willen veroorzaken en het hacken meer als een sport zien. Inlichtingendiensten ontwikkelen en verspreiden voor sabotage en spionage meer of min legaal malware.

Economische interesses

De meeste aanvallen gebeuren echter om economische redenen. Hierbij is het voor de aanvallers meestal niet belangrijk wie het slachtoffer is, zolang er maar een mogelijkheid bestaat om er financieel profijt uit te halen.

Lange tijd was phishing de meest gebruikte methode; het achterhalen van creditcardgegevens en toegangscodes voor onlinebanking is hierbij een directe financiële bedreiging voor het slachtoffer.

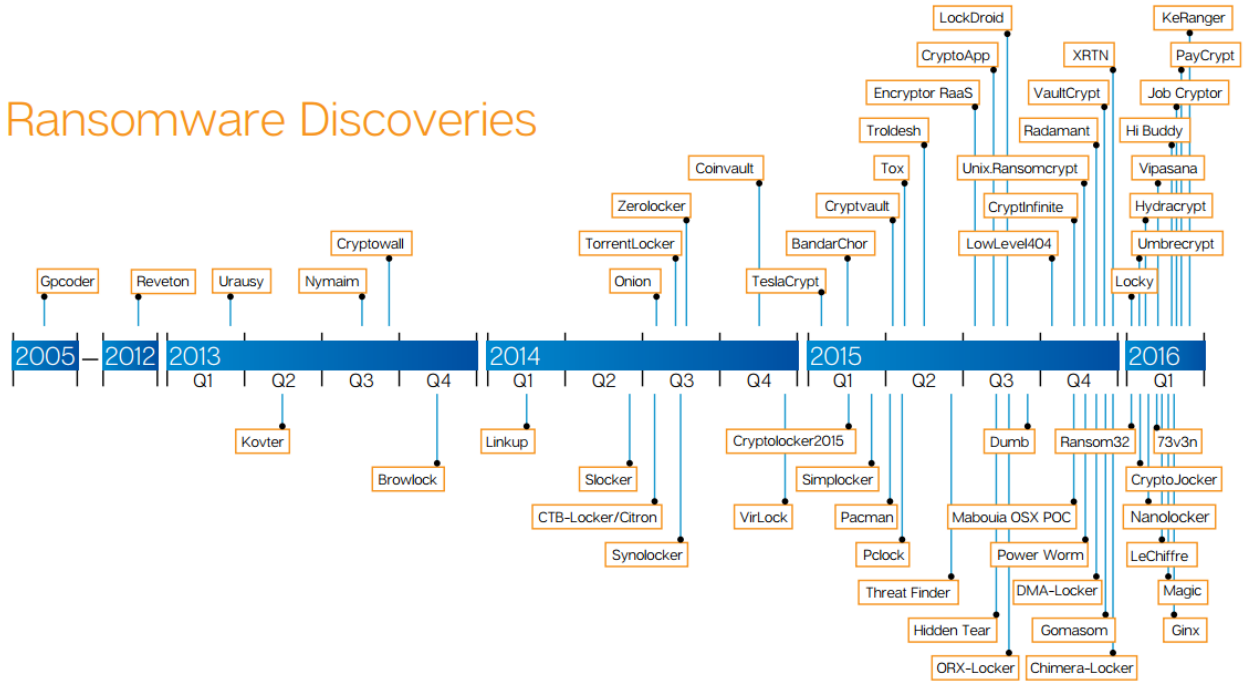
De waarde van gegevens

Deze toegangsgegevens hebben daarom een directe **marktwaarde:** creditcardgegevens worden massaal op Darknet verhandeld. Toegangscodes en creditcardgegevens zijn echter goed identificeerbare data die in de massa van alle opgeslagen gegevens een kleine fractie uitmaken. Ze zijn daarom eenvoudig en met overzienbare effort tegen misbruik te beveiligen.

Het overgrote deel van de op desktopcomputers, servers en mobiele apparaten opgeslagen data heeft voor de aanvaller generlei waarde – **wél voor de eigenaar van de gegevens.**

Hieruit ontstaat het nieuwe businessmodel: afpersing.

Ransomware is dan ook sterk in ontwikkeling, zoals in het actuele rapport van Symantec te zien is:[1]



Het Duitse 'Bundesamt für Sicherheit in der Informationstechnik' (BSI, een soort ministerie voor veiligheid in de IT) spreekt zelfs van een toename van meer dan 1000 procent in Duitsland.[2]

En terwijl de schade door gestolen creditcard-gegevens relatief beperkt is en geen noemenswaardige invloed op de bedrijfscontinuïteit heeft, is dit bij afpersing door ransomware anders. Je kunt hier niet langer de ogen voor sluiten, aldus het BSI in hetzelfde document.

Ransomware

Ransomware (van het Engelse ransom = losgeld) gebruikt dit businessmodel van afpersing. Er zijn twee soorten ransomware: lockout en crypto. Lockout blokkeert de toegang tot het gehele computersysteem en geeft deze pas na betaling van een 'kostenbijdrage' weer vrij. Vaak beweert de malware van een officiële instantie (FBI, politie) afkomstig te zijn en het

[1] Symantec Internet Security Threat Report V21 - https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[2] Ransomware: Bedrohungslage, Prävention & Reaktion - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf

systeem te blokkeren omdat er illegale activiteiten (zoals kinderporno of illegale downloads) gevonden zijn.

Sterk groeiend zijn echter de aanvallen door crypto-trojanen. Deze malware versleutelt delen van de op de pc, server of het mobieltje aanwezige bestanden zodat deze niet meer toegankelijk zijn. De vitale functies van het bezette systeem blijven werken, zodat enerzijds de schade pas later ontdekt wordt en anderzijds het systeem werkbaar blijft – bijvoorbeeld om een betaling te verrichten.

De hiervoor gebruikte encryptie wordt voortdurend verbeterd en aan de nieuwste wetenschappen aangepast – en is daardoor zelfs door experts niet meer te omzeilen.

Doelgroep: 100%

Omdat het hierbij niet meer om de handelswaarde van de gegevens gaat, groeit de doelgroep voor deze malware naar bijna 100 procent van de potentiële doelen. Immers zijn de gegevens voor de eigenaar waardevol, ook als ze voor anderen bijna geen waarde hebben.

Voor een aanvaller maakt het dus niet uit wie het slachtoffer is. Particulieren zijn gehecht aan persoonlijke herinneringen (foto's, video's en aantekeningen bijvoorbeeld), voor ondernemingen zijn sommige data nodig voor het voortbestaan en overheden kunnen zonder de nodige gegevens vaak dagenlang helemaal niet of beperkt werken.

Probleem geldoverdracht: opgelost

Nog een andere ontwikkeling werkt in het voordeel van de aanvallers: anonieme betalingen zijn door de invoering van blockchain-valuta zoals BitCoin veel eenvoudiger geworden. Het is nagenoeg onmogelijk deze betalingen te volgen en de ontvanger te traceren.

Door deze twee randvoorwaarden wijzigt de situatie voor malware compleet. Dat besturingssystemen met vele duizenden kwetsbaarheden per jaar in gevaar zijn is niet nieuw – dat het onmiddellijk en bij iedereen schade veroorzaakt die financiële consequenties heeft, is wél nieuw.

Tegenmaatregelen

De eerste natuurlijke stap is om de toegang te beveiligen. Door te voorkomen dat een virus de pc bereikt, kan het virus ook geen schade veroorzaken. Moderne virusscanners, regelmatige veiligheidsupdates, goed ingestelde firewalls en beperkte gebruikersbevoegdheden in het reguliere bedrijf behoren tot de absoluut noodzakelijke maatregelen.

Niettemin zal er altijd een potentiële zwakke plek zijn die geen firewall kan sluiten: de mens.

Voorbeeld: NSA

De IT-omgeving van de NSA behoort zeker tot de best beveiligde ter wereld. Toch is het een adviseur – Edward Snowden – gelukt om duizenden kritische en geheime documenten uit het systeem te kopiëren. Geen virusscanner sloeg alarm.

En als enkele mensen toegang tot bedrijfskritische IT-bereiken hebben – en dat moeten ze, anders zouden wij niet met de gegevens kunnen werken – kunnen via deze weg ook virussen het systeem binnendringen.

Deze problematiek wordt nog versterkt door de BYOD-trend: "Bring Your Own Device" is de ingebouwde achterdeur in bijna elke onderneming of organisatie. Medewerkers nemen laptops mee naar huis, brengen hun smartphones en tablets mee naar het werk of benaderen via cloudservices en vpn's de data en netwerken van het bedrijf. Het compleet afsluiten van deze externe verbindingen is vaak niet mogelijk – en meestal ook helemaal niet gewenst. Buitendienstmedewerkers zijn hierop aangewezen en ook outsourcing of home office zou niet mogelijk zijn.

Koude back-ups

Omdat de toegang tot data dus nooit 100 procent afgedicht kan worden, is het raadzaam aanvullend ‘koude’ back-ups te maken.

Opslagmedia worden koud genoemd als ze geen mogelijkheid bieden overschreven of gewist te worden – omdat ze offline bewaard worden of omdat ze alleen eenmalig beschrijfbaar zijn (WORM – Write Once Read Many). Gegevens op deze gegevensdragers zijn dus tegen aanvallen beveiligd.

Er moet natuurlijk worden zeker gesteld dat zowel de back-up als het terugzetten in niet-geïnfecteerde systemen geschied.

Een vaak onderschat gevaar schuilt hierbij in de zogenaamde metadata. De meeste bestandssystemen, ook die op back-upmedia, vertrouwen op een centrale index ter identificatie van de data op de gegevensdragers. Deze index staat meestal op een eigen partitie en bevat alle informatie die nodig is om vanuit de op de gegevensdrager gefragmenteerd opgeslagen datapakjes de oorspronkelijke bestanden weer samen te voegen. Voor een aanvaller is het daarom voldoende, bijvoorbeeld bij geautomatiseerde back-upprocessen, deze index te infecteren om een terugzetten onmogelijk te maken – ook bij blijkbaar intacte back-ups.

De FBI waarschuwt inmiddels voor malware die heel gericht naar netwerkback-ups zoekt en deze wist of ontoegankelijk maakt.[3] Dit is ook logisch, netwerkback-ups zijn immers allesbehalve koud omdat ze permanent met het operatief systeem verbonden zijn.

En ook al worden netwerk- en disk-to-disk-back-ups vaak aanvullend naar (koude) magnetische tapes gekopieerd, kan dit soort aanvallen toch het verlies van waardevolle gegevens betekenen, afhankelijk van de planning van de back-ups.

Trend: permanente beschikking over alle data

Koude back-ups worden echter momenteel minder populair omdat alle gegevens permanent en direct beschikbaar moeten zijn. Methodes zoals ‘Big Data’-analyses, de noodzaak van ‘Business Continuity’ bij een calamiteit en de capaciteitssprongen bij snelle harddiskopslag dwingen de koude back-up in de meeste gevallen in de rol van allerlaatste uitweg. Het terugzetten van gegevens uit deze back-ups is ingewikkeld en gaat langzaam.

Vaak worden ook delen van de beschikbare netwerkopslag, waar data meervoudig gespiegeld en horizontaal over vele fysieke gegevensdragers verdeeld zijn, als WORM gedeclareerd. Simpel gezegd gebeurt dit via een vinkje die dit gedeelte als een ‘read-only’ medium aan het bestandssysteem meldt. Zo’n ‘Soft-WORM’ is alleen op basis van administratorrechten beveiligd en ook hier geldt: wat ‘goede’ mensen kunnen, kunnen ook ‘slechte’ mensen of algoritmes. En als meerdere mensen administratorrechten hebben, wordt het risico alleen maar groter.

[3] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf

Veilige opslag

Hoe moet nu een opslagsysteem opgebouwd zijn dat aan de actuele eisen voldoet en toch veilig is?

Structuurzekerheid

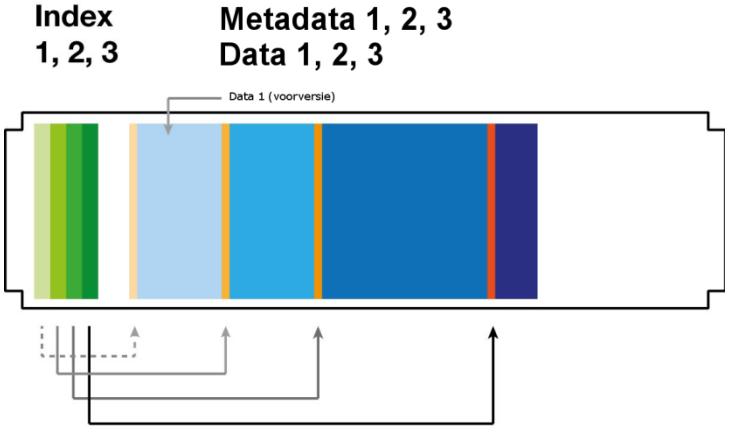
De voorwaarde voor een veilige opslag is de structuurzekerheid, dat wil zeggen de onafhankelijkheid van de gegevens van een centrale index of van metadata. De datastructuur moet blijvend zeker gesteld zijn.

Deze eis is met de gebruikelijke opslagmethodes en bestandssystemen echter nagenoeg niet in te vullen. Harddisk- en flash-opslagsystemen bewaren gegevens gefragmenteerd met een centrale index omdat alleen op deze manier de gevraagde snelheid en levensduur gewaarborgd wordt. Een ‘wissen’ van de gegevens markeert de overeenstemmende delen van het opslagsysteem in de index als ‘vrij’, zodat deze delen opnieuw overgeschreven kunnen worden. De gegevens zelf zijn tot aan het overschrijven nog op het opslagsysteem aanwezig, maar niet meer benaderbaar. Dit geldt met name bij meer complexe opslagsystemen met meerdere redundantie (bijvoorbeeld RAID) die gegevens juist over veel gegevensdragers verdelen. Terwijl bij een per ongeluk gewist SD-kaartje de data nog relatief eenvoudig terug te halen zijn, is dit bij een complex opslagsysteem niet meer mogelijk.

Structuurzekere opslag daarentegen bewaart de metadata altijd samen met de opgeslagen gegevens en maakt aanvullend een centrale index aan. Om snelheidsredenen wordt gedurende normaal gebruik de centrale index gebruikt, een herstel van gegevens is echter ook rechtstreeks uit de gegevens zonder de centrale index mogelijk.

Lineaire opslag

Structuurzekerheid werkt niet met verdeelde en gefragmenteerde opslag omdat anders de metadata bij elk gegevensfragment mee opgeslagen moeten worden. Verder worden bij ‘random write’ juist vrijgekomen delen van de opslag opnieuw beschreven. Een herstel zou dus alleen zeer beperkt mogelijk zijn.



Een oplossing hiervoor is de **lineaire opslag**. Net zoals op een magnetisch tape worden bij elkaar horende datapakketten ook fysiek achter elkaar opgeslagen. Nieuwe gegevens worden steeds aan het einde van de data

toegevoegd, ongeacht of door wissen aan het begin theoretisch weer beschikbare ruimte vrijgekomen is. Pas een zogenaamde ‘garbage collection’ herstructureert de gegevens zodanig dat ongebruikte ruimte geen gaten meer achterlaat.

Als nu geen automatische garbage collection gebruikt wordt is weliswaar meer ruimte op het opslagmedium nodig, maar oudere versies van de gegevens zijn nog steeds te allen tijde beschikbaar – ook als ze niet meer in de centrale index vermeld zijn of deze index gemanipuleerd is. In combinatie met structuurzekerheid is een teruggaan naar oudere versies dus met weinig inspanning mogelijk.

Door het gebruik van moderne redundantiemethodes, zoals Erasure Resilient Coding (ERC), kan dit principe ook op hoog-redundante harddisksystemen toegepast worden. Hierdoor blijft de snelle en willekeurige toegang (random access) naar alle gegevens mogelijk.

Bij zo’n systeem moet de aanvaller expliciet het gehele opslagmedium kunnen overschrijven om de toegang tot de opgeslagen gegevens te blokkeren. Het gewone ‘wissen’ van gegevens veroorzaakt geen schade omdat het alleen de centrale index wijzigt. En een encryptie van de gegevens door ransomware slaat alleen een nieuwe versie van de data op het medium op, de oudere versie blijft op het medium onaangetast en beschikbaar.

Niemand mag gegevens kunnen manipuleren

De structuurveilige opslag is een voorwaarde om gegevens weer terug te kunnen zetten, ook als de centrale index of het bestandssysteem defect of gemanipuleerd zijn.

De cruciale stap naar een écht veilig opslagsysteem is echter de eerder genoemde koude opslag, dus de beveiliging tegen manipulatie, wissen of overschrijven. Deze beveiliging vereist het loskoppelen van de opslag van alle software.

Is er maar één achterdeur en deze zal op termijn ook gebruikt worden, zie als voorbeeld het WannaCry virus van mei 2017. Dit is ook de reden waarom Apple weigert een achterdeur voor de FBI in het mobiele iOS-besturingssysteem in te bouwen.

Dat achterdeuren op termijn gebruikt gaan worden is niet nieuw. Het gebeurt niet alleen op digitaal niveau, maar ook in de analoge wereld – zie het verhaal van de veiligheidssleutels voor de Transport Security Administration (TSA). Van deze TSA-sleutels bestaan zes versies, de wat betere koffers hebben sloten met een van deze TSA-codes. De bedoeling is dat de veiligheidsinspectie op vliegvelden met de juiste TSA-sleutel de koffer kan openen zonder het slot open te breken. Op een gegeven moment drukte een tijdschrift in een bericht over deze sleutels een goede foto van de sleutels af en sindsdien kan iedereen deze sleutels eenvoudig namaken en in principe elke koffer openen[4].

Deze voorbeelden geven aan: waar een mogelijkheid ter omzeiling van veiligheidsmaatregelen bestaat, wordt deze ook gebruikt.

Het veilige opslagsysteem moet dus als hoogste prioriteit hebben: **niemand mag de mogelijkheid hebben de data te overschrijven.**

Hiervoor zijn twee mogelijkheden: data fysiek uit het werkende systeem nemen (offline) of opgeslagen gegevens via hardware-beveiliging zodanig te verzegelen dat overschrijven niet mogelijk is zonder het gehele medium te vernietigen – wat een afpersing de bodem zou ontnemen.

Offline met replicatie

Het eenvoudigst is het overschrijven van gegevens te voorkomen als de gegevens geen fysieke verbinding met het werkende systeem hebben, dus op media opgeslagen zijn die offline, zoals in een kluis, bewaard worden. Dit gaat goed met gegevens die niet meer nodig zijn. Data die verder beschikbaar moeten zijn, kunnen naar een koud medium gerepliceerd en dan uit het systeem genomen worden. Als de replicatie regelmatig en vaak genoeg gedaan wordt, gaan in het geval van een calamiteit geen of nauwelijks gegevens verloren.

[4] https://www.heise.de/make/meldung/Hack-mit-3D-Drucker-TSA-Generalschluessel-fuer-Gepaeck-2810177.html

Offline-media zijn echter meestal niet geschikt om in het geval van een calamiteit gegevens direct weer beschikbaar te maken als de primaire opslag aangevallen is. De gegevens moeten eerst van het offline-medium teruggezet worden – dit proces is langdurig en bovendien foutgevoelig.

Het veilige opslagsysteem moet daarom rechtstreeks met offline-geschikte media werken die desgewenst gerepliceerd en uit het systeem genomen kunnen worden. Als het primaire medium dan geïnfecteerd is, wordt het gewoon door de laatste replica in het (dan hopelijk schone) systeem geladen – de gegevens zijn dan per direct en zonder omslachtig terugzetten beschikbaar.

Omdat gebruikelijke opslagsystemen gebaseerd zijn op verdeling van gegevens en fragmentatie is dit alleen met de boven beschreven lineaire opslag mogelijk. In combinatie met Erasure Resilient Coding zijn zo echte offline-media met redundantie én hoge snelheid mogelijk.

WORM-opslag

Het overschrijven van gegevens kan ook door een **WORM-systeem** voorkomen worden. De opslagmedia moeten hiervoor niet uit het actieve systeem genomen worden. Zoals boven al gezien is de Soft-WORM-methode niet veilig en daarom onvoldoende. Het gebruik van een hardware-controller die op de aangesloten opslagmedia geen terugzetten van de schrijfpositie toelaat, beveiligt wel goed omdat daardoor het fysiek overschrijven via software onmogelijk wordt. Ook dit gaat alleen met lineaire opslag omdat alleen hier de media gelijkmatig en doorlopend ‘gevuld’ worden en data niet gefragmenteerd weggeschreven worden.

Om deze hard-WORM beveiliging te omzeilen zou een aanvaller de functionaliteit van deze speciale harddisk-controller moeten nabouwen en aanvullend de mogelijkheid van overschrijven in de controller implementeren. Vervolgens zou de aanvaller fysiek de harddisks van de WORM-controller moeten overzetten naar de zelfgebouwde controller om dan de gegevens te kunnen veranderen.

Toepassingen

De genoemde veiligheidsmaatregelen zijn niet voor elk opslagsysteem geschikt. Als data vaak gewijzigd worden, zoals bij databases, zou een lineair opslagsysteem snel vol raken en daarmee economisch niet aantrekkelijk zijn. Deze systemen moeten verder via regelmatige back-ups beveiligd worden.

Zeer geschikt is koude opslag echter voor gegevens die na het schrijven niet meer (mogen) wijzigen: back-ups, mediagegevens (foto, audio, video), archiefgegevens (afgesloten

projecten, studies, meetgegevens, surveillancegegevens), boekhoudgegevens, medische gegevens, enzovoort. Als aanvullend aantoonbaar is dat de ooit geschreven gegevens niet gemanipuleerd en ongewijzigd zijn, praten wij over zogenaamde revisiezekere opslag.

Opslagsystemen van FAST LTA

FAST LTA heeft met de **Silent Cubes** en de **Silent Bricks** twee opslagsystemen ontwikkeld die door lineaire opslagtechnologie met structuurveiligheid en moderne Erasure Resilient Coding met viervoudige redundantie voor koude opslag – Cold Storage – geoptimaliseerd zijn.

Drievoudige beveiliging tegen dataverlies

Naast de hoge ingebouwde veiligheid door lineaire opslag en structuurzekerheid bieden opslagsystemen van FAST LTA aanvullend een drievoudige beveiliging tegen dataverlies door harddisk-uitval.

Erasure Resilient Coding

FAST LTA gebruikt 12/8 Erasure Resilient Coding. Elk opslagmodule beschikt over twaalf gegevensdragers waarvan vier tegelijk mogen uitvallen zonder dat gegevens verloren gaan. Een belangrijk voordeel van ERC ten opzichte van RAID-systemen is hierbij de duidelijk lagere rebuild-tijd, naast de grotere veiligheid en de betere bruto/netto-verhouding:

> "**Als je harde schijven van grote capaciteiten in een RAID-array plaatst duurt een rebuild weken. Met Erasure Coding praat je over uren,"** zegt bijvoorbeeld George Crump, president van het IT-analyse-bedrijf Storage Switzerland.[5]

Dit is tevens een belangrijk beveiligingsaspect. Gedurende een rebuild is een RAID-systeem in een kritische toestand, uitval van een verdere harddisk kan al dataverlies betekenen. Erasure Resilient Coding met viervoudige redundantie heeft bij uitval van een harddisk nog drie aanvullende reserves zodat de rebuild, die toch al minder ingewikkeld is, met rust en weinig systeembelasting gedaan kan worden.

[5] http://searchstorage.techtarget.com/feature/Hot-data-storage-technology-trends-for-2016

Digital Audit

Het belangrijkste bij een back-up is een functionerende restore. Deze gemeenplaats veronderstelt dat de opgeslagen gegevens ook betrouwbaar leesbaar zijn. Daarom worden de gegevensdragers in de FAST LTA opslagsystemen regelmatig en automatisch op bit-niveau gecontroleerd – de zogenaamde Digital Audit. Fouten kunnen zo betrouwbaar herkend en bijvoorbeeld door vervanging van de gegevensdrager gecorrigeerd worden.

Disk Mix

Het gebeurt altijd wel eens dat een hele serie van harddisks een fout heeft. Maar ook zonder fouten valt op dat harddisks uit dezelfde serie vaak vlak achter elkaar uitvallen.

Om te voorkomen dat dit effect invloed op de dataveiligheid heeft, worden in elke Silent Cube en in elke Silent Brick harddisks uit drie verschillende series van zoveel mogelijk verschillende fabrikanten[6] ingebouwd. Zelf als de vier harddisks van een serie uitvallen gaan door het 12/8 Erasure Resilient Coding geen gegevens verloren.

De onafhankelijkheid van bepaalde soorten gegevensdragers en fabrikanten heeft tevens voordelen bij het vervangen van defecte harddisks: als bepaalde modellen of fabricaten na jaren niet meer leverbaar zijn, is een vervanging door andere modellen nog altijd zonder problemen mogelijk.

[6] Helaas zijn er voor sommige capaciteiten van harddisks en SSD's geen drie verschillende fabrikanten meer.

Silent Cubes: revisiezekere archiefopslag met WORM-verzegeling

De **Silent Cube** beschermt gegevens aanvullend met een WORM-verzegeling tegen wijziging en verlies. Omdat deze verzegeling op het laagste hardware-niveau geschiedt – de speciaal ontwikkelde harddiskcontroller kan alleen doorlopend schrijven maar niet wissen of elders schrijven – kan geen administrator, ook niet FAST LTA, gegevens wijzigen of wissen.

Deze WORM-verzegeling garandeert de Silent Cubes ook de revisiezekerheid die voor een rechtsgeldige archivering bijvoorbeeld volgens KNMG, AVG en anderen nodig is.

Silent Bricks: flexibel en veilig opslagsysteem voor back-up en archief met uitneembare storagecontainers

De **Silent Brick Library** doelt op minder speciale toepassingen. Als Cold Storage systeem is de library ideaal voor back-up, maar ook voor een actief archief of als netwerkopslag.

De basis vormen de **Silent Bricks**, uitneembare storagecontainers met twaalf harddisks die intern via Erasure Resilient Coding beveiligd zijn. Met de flexibele replicatie op basis van enkele Silent Bricks zijn offline-media en remote replica's eenvoudig en goedkoop aan te maken. In tegenstelling tot de gebruikelijke redundantie door spiegeling naar een tweede locatie kan hier de replicatie van de Silent Bricks individueel voor elke Silent Brick geconfigureerd worden. Het systeem op de tweede locatie blijft hierbij volledig operationeel en kan zelf ook Silent Bricks naar het eerste systeem repliceren (cross-over replicatie).

De Silent Bricks zijn uitgerust met harddisks of snelle FLASH-geheugens en leverbaar in verschillende capaciteiten met of zonder WORM-verzegeling.

De Silent Brick Controller biedt vijf slots voor Silent Bricks en kan via rechtstreeks verbonden uitbreidingseenheden met elk veertien slots uitgebreid worden.

De **Silent Brick Drive** is met zijn twee slots al een ideaal systeem voor kleinere opslagbehoeftes zoals een veilig netwerkback-up met interne replicatie naar een tweede Silent Brick.

Over FAST LTA

Passie voor dataopslag

We secure Petabytes – dit is het motto van FAST LTA AG uit München, Duitsland. Deze slogan bevat de belofte op de gegevens van de klanten te letten. En dit weerspiegelt in elk detail van de door Matthias Zahn en zijn medewerkers ontwikkelde opslagproducten.

De eigen ambitie is: er mogen geen gegevens verloren gaan. Daarom worden alle kritische onderdelen zelf ontwikkeld, uitgebreid getest en permanent verbeterd. Hierbij hoort ook de implementatie van het Erasure Resilient Coding, een redundante codering ter bescherming van gegevens die de gebruikelijke RAID ver voorbij gaat. Deze technologie wordt door FAST LTA vergezeld door Digital Audit, de automatische zelfcontrole van de systemen, en door de aanvullende beveiliging via Disk Mix, het gebruik van drie verschillende harddiskmodellen in ieder storagemodule. Opslagsystemen van FAST LTA zijn zo veilig dat – aangenomen dat de locatie veilig is – geen aanvullende beveiliging door back-up nodig is.

Silent Cubes, het revisiezekere WORM-systeem voor alle data die in geen geval verloren mogen gaan, is sinds de introductie 2008 in duizenden installaties in gebruik. Onder andere de zorgsector, musea, bibliotheken en overheden, de industrie en handel, banken en verzekeringen gebruiken Silent Cubes. De handige storage-kubus is voor talloze applicaties gecertificeerd en met alle opslagnormen compliant.

De Silent Brick Library, het flexibele COLD Storage-systeem met transportabele storagecontainers is evenwel uitgerust met de drievoudige beveiliging door Erasure Resilient Coding, Digital Audit en Disk Mix. De combinatie uit lineaire datastructuur en harddisktechnologie maakt fysiek gescheiden opslag mogelijk en biedt bijzonder lage grenskosten. De Silent Brick Library is met name geschikt voor grote actieve archieven, als back-upopslag en als mediaopslag zoals videoproducties.

FAST LTA is ISO 9001 gecertificeerd.

Over COMEX

Comex is sinds 1992 distributeur voor digitale opslagsystemen en vertegenwoordigt FAST LTA sinds 2008 in Nederland.

Contactgegevens:
www.comex.eu | office@comex.eu | +31-43-3088400