De immutable back-up: onmisbaar wapen in de strijd tegen dataverlies

Nu organisaties steeds afhankelijker zijn van data, is de impact van dataverlies groter dan ooit. Daarom zoeken ze voortdurend naar nieuwe methoden om zich te beschermen tegen ransomware en vernietiging van data door menselijk handelen. Een effectief voorbeeld is de *immutable back-up*. In dit e-book leest u waarom dit inmiddels een echte *must have* is.

Wat het is en hoe het werkt

Het woord zegt het eigenlijk al: immutable betekent onveranderlijk of statisch. Bij een immutable back-up wordt data opgeslagen op disks die onderdeel zijn van een speciaal geconfigureerde server. Een machine die weinig meer kan dan data ontvangen. Het is niet mogelijk om data die daarop staat nog te veranderen of te deleten.

De enige manier om de data te verwijderen, is door fysiek toegang te krijgen. Daarvoor is het nodig om een monitor en een toetsenbord aan te sluiten. Dit vormt een extra drempel voor hackers. Zij zoeken immers naar kwetsbaarheden binnen een netwerk en proberen op afstand binnen te dringen. Als ze eenmaal toegang hebben verkregen, versleutelen ze zoveel mogelijk data. Om het herstel door de gebruikers definitief onmogelijk te maken, vernietigen cybercriminelen alle back-ups. Slachtoffers moeten dan wel losgeld betalen.

Waarom de immutable back-up in opkomst is

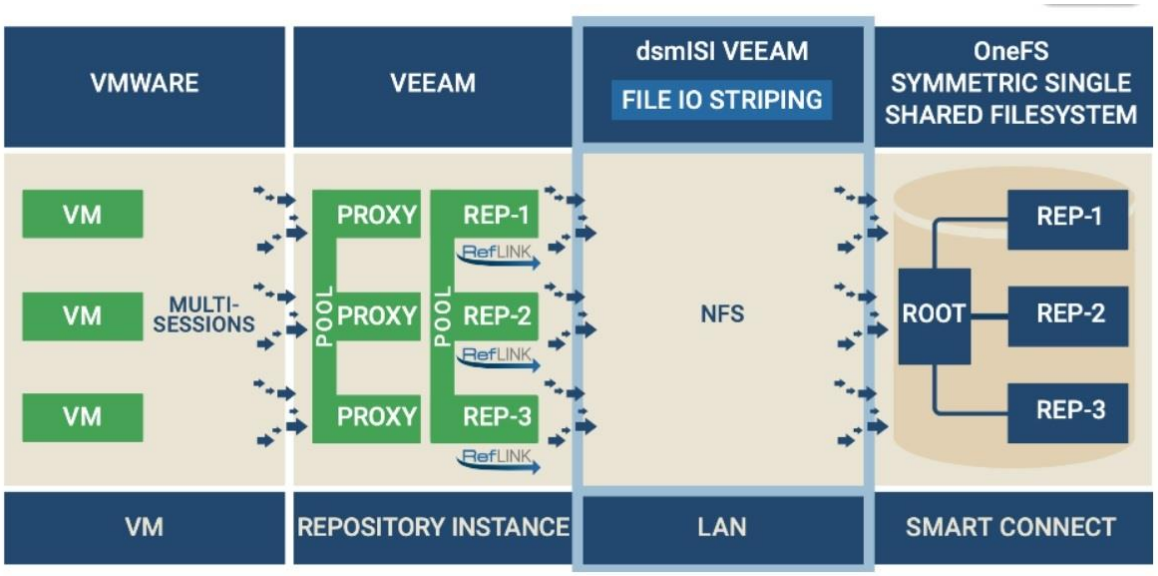
Een paar jaar geleden schoten hackers nog met hagel, maar inmiddels gaan ze veel doelgerichter te werk. Dat loont, want er worden steeds hogere bedragen betaald[1]. Nu meer organisaties datagedreven werken en de afhankelijkheid van data toeneemt, krijgt bescherming tegen ransomware meer prioriteit[2]. Het beveiligen van data is niet genoeg, er zijn ook maatregelen nodig om ervoor te zorgen dat er niet met back-ups kan worden geknoeid.

Een back-up server is in een traditionele opzet een kwetsbare plek. Deze server heeft namelijk toegang nodig tot alle andere servers, om bestanden op te slaan die zijn gewijzigd na de vorige back-up. Het is natuurlijk mogelijk om de beveiliging van deze server te verbeteren, door allerlei onnodige of niet gebruikte functies uit te schakelen en door een apart back-up netwerk te creëren. De kwetsbaarheid neemt dan af, maar de back-up server blijft een zwakke plek.

Met een server voor immutable back-ups ligt dit anders. Deze communiceert alleen met de back-up server en zonder fysieke toegang is het niet mogelijk data die erop staat te vernietigen. Organisaties beschikken zo als het ware over een extra slot op de deur. Een oplossing die een relatief lage investering vraagt, maar grote zekerheid biedt.

Bij een software ontwikkelaar als Veeam ziet een immutable back-upinfrastructuur er schematisch als volgt uit:

[1] https://blog.eclecticiq.com/the-ransomware-evolution-landscape-part-1-the-rise-of-the-biggest-cyberthreat
[2] https://www.forbes.com/sites/tomcoughlin/2021/03/31/2021-world-backup-day/



Data op servers (in de linker kolom *VMWARE*) wordt geback-upt in de Veeam-omgeving (de tweede kolom van links). De Veeam Server houdt in een database bij wat de laatst veranderde files zijn (in de derde kolom *File striping*) en brengt die over naar de zogeheten back-up repository (rechterkolom). Die repository is heel beperkt ingericht en kan weinig meer dan data ontvangen.

Doe recht aan de 3-2-1 regel

Deze netwerkarchitectuur voldoet aan de 'gouden' 3-2-1-regel voor back-ups. Die houdt concreet in dat het voor de beste bescherming van data nodig is om:

- Drie kopieën te maken van de belangrijkste data.
- Deze kopieën op te slaan op minstens twee verschillende media.
- Eén kopie buiten de deur te bewaren.

De kopie die zich *offsite* bevindt moet dan *air-gapped* of immutable zijn. Air-gapped wil zeggen dat er letterlijk lucht zit tussen het opslagmedium en het netwerk. Tape is daar geschikt voor, want cartridges kunnen in een kluis worden gelegd. Tape, het oudste opslagmedium, staat daarom weer volop in de belangstelling. Maar tape is ook kwetsbaar. Juist omgaan met tape (*tape handling)* is foutgevoelig en tijdrovend. Daarnaast moeten cartridges droog en schoon worden opgeslagen, bij de juiste temperatuur en ver van magnetische velden[3]. Bovendien duurt herstel vanaf tape lang.

Uitdagingen van immutable storage

Immutable storage is een andere optie om aan de 3-2-1-regel te voldoen. De opslag kan zich in principe overal bevinden. Omdat het bij back-ups vaak om grote hoeveelheden data gaat, is voor snelle back-up en restore een krachtige verbinding vereist. Verder moet rekening worden gehouden met het eerdergenoemde beperkte karakter van de server. Deze moet ingericht worden om puur en alleen data te ontvangen, door zoveel mogelijk functies uit te schakelen. Ook poorten staan zoveel mogelijk dicht, omdat deze aansluitingen een toegangspunt kunnen zijn voor hackers. Dat maakt deze servers weliswaar veilig, maar het betekent ook dat monitoring niet mogelijk is. Om storingen te achterhalen moet regelmatig iemand ter plaatse gaan om fysiek controles uit te voeren.

[3] https://www.ibm.com/docs/en/i/7.4?topic=cartridges-tape-handling-storage

Waarom ExtraVar?

ExtraVar is als disaster recovery-specialist groot voorstander van het maken van immutable back-ups en doet het zelf ook. De methode vergt een relatief geringe investering, zeker in vergelijking met de enorme bedragen die met losgeld zijn gemoeid.

Het is wel goed om te beseffen dat met een immutable back-up de kous niet af is. Bij een optimale beveiligingsstrategie komt veel meer kijken. Het is nog steeds nodig om aan preventie te doen. Een zero trust-benadering vormt hiervoor een goed uitgangspunt. Dat concept gaat ervan uit dat niets of niemand te vertrouwen is. Een belangrijke pijler is dat elk persoon en elk apparaat dat toegang wil tot data wordt gecontroleerd. Daarnaast wordt het netwerk opgedeeld in compartimenten, zodat een indringer niet direct toegang heeft tot álle data. Ook het actief monitoren van het netwerk om afwijkend gedrag op te sporen en dreigingen onschadelijk te maken (met intercept software) hoort daarbij.

Verder is het belangrijk om kwetsbaarheden in kaart te brengen en aandacht te hebben voor de mens. Die is vaak de zwakste schakel. Cybercriminelen gaan steeds geraffineerder te werk in het verleiden van mensen om op een linkje te klikken. Ze ontwikkelen steeds nieuwe methoden, die niet altijd bij ontwikkelaars van antivirussoftware bekend zijn.

Altijd een begaanbaar pad naar herstel

Zelfs met een uitgekiende strategie inclusief immutable back-up, is datarecovery na een ransomware attack geen eenvoudige opgaaf. Het is praktisch onmogelijk om het dataverlies terug te brengen tot nul. Wat wel kan, is proberen dit verlies en alle gevolgen die daarbij horen zoveel mogelijk te beperken. Wie ermee te maken krijgt, kan het gevoel hebben in een diep dal te zijn beland. Het is een zware tocht om hieruit te komen, maar ExtraVar weet de weg en biedt ondersteuning bij elke stap. Door advies te geven, oplossingen te testen, implementeren, beheren en onderhouden bieden we een begaanbaar pad naar herstel.

Wilt u meer weten over Disaster Recovery as a Service en immutable back-ups? Klik dan hier of neem vrijblijvend contact op.