

Whitepaper

Back-ups beschermen tegen ransomware



Deze (engelse) video is te vinden op <https://youtu.be/xTSpDBfXS50>

Ransomware-aanvallen zorgden in 2020 wereldwijd voor een kostenpost van meer dan 20 miljard dollar. Dit is ruim het dubbele van twee jaar eerder¹. De gemiddelde kosten door downtime bedragen 283.000 dollar per slachtoffer². In het verleden schoten cybercriminelen altijd met hagel. Ze hadden geen duidelijk doelwit. Tegenwoordig voeren ze echter gerichte aanvallen uit met ransomware, soms als onderdeel van een grotere aanval.

Dit artikel gaat in op moderne ransomware-aanvallen op back-ups en maatregelen die je kunt treffen om gegevensverlies te voorkomen.

1 <https://purplesec.us/resources/cyber-security-statistics/ransomware/>

2 <https://www.munichre.com/topics-online/de/digitalisation/cyber/cyber-insurance-risks-and-trends-2021.html>

De motivatie voor ransomware-aanvallen

Het gevaar van ransomware blijft toenemen. In 2020 bereikte de IT-wereld een beangstigend record: 20.000 nieuwe meldingen van beveiligingslekken. Dit is deels veroorzaakt door de opkomst van thuiswerken in de coronacrisis. Hierdoor is het aantal kwetsbaarheden voor mobiele apparaten met 50% toegenomen. Dit maakte bedrijven ook vatbaarder voor cyberaanvallen³.

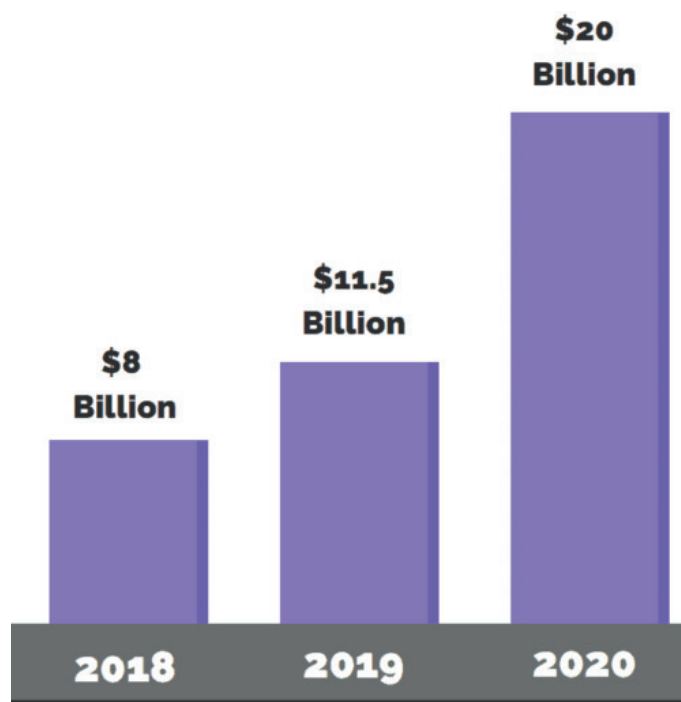
Tegenwoordig moeten niet alleen bedrijven ransomware-aanvallen vrezen. De afgelopen maanden steeg het aantal aanvallen op vitale infrastructuren hard. Bijvoorbeeld in de gezondheidszorg. Uit een enquête onder 130

ziekenhuizen en andere zorginstellingen bleek dat bijna de helft in de eerste helft van 2021 hun netwerk moest uitschakelen door een ransomware-aanval⁴. Schadeclaims door ransomware-aanvallen bereiken ondertussen ook recordhoogtes. Zo zag cyberverzekeraar Coalition het gemiddelde bedrag van claims tegen zijn polishouders in de eerste helft van 2021 met 1,2 miljoen dollar stijgen door ransomware-aanvallen. In de eerste helft van 2020 was dit nog 'slechts' 450.000 dollar⁵.

3 <https://www.skyboxsecurity.com/trends-report/> (Vulnerability and Threat Trends Mid-Year Report 2021)

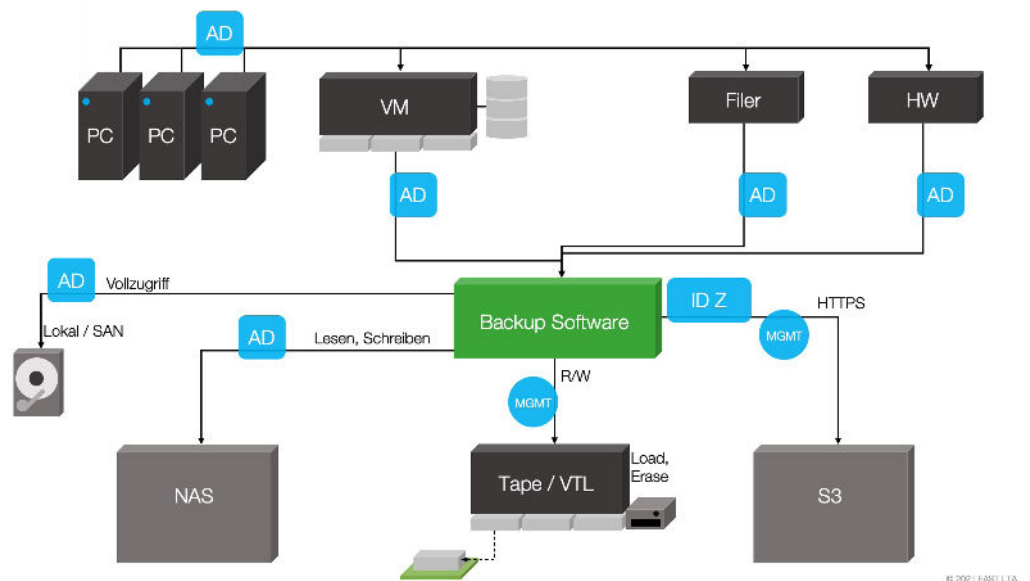
4 <https://www.munichre.com/topics-online/de/digitalisation/cyber/cyber-insurance-risks-and-trends-2021.html>

5 [idem]



*Estimated global damage from ransomware.

Doelwitten voor ransomware



Voorbeeld van een IT-infrastructuur met back-up

De klassieke IT-infrastructuur bestaat onder meer uit computers, virtuele machines, file servers en netwerkhardware. De verschillende soorten data binnen deze omgeving stellen evenzoveel eisen aan de IT-opslag. Dit vraagt bovendien uiteenlopende beveiligingsniveaus. Want als een infrastructuur niet voldoende beveiligd is met firewalls en dergelijke, staat de deur wagenwijd open voor cybercriminelen.

Binnen de IT-infrastructuur beschermen back-ups tegen dataverlies. Ook hierbij zijn er uiteenlopende back-upbestemmingen die op hun beurt afhankelijk zijn van het soort gegevens en de eisen:

- Lokaal/SAN: De storage-omgeving is rechtstreeks verbonden met de back-upserver
- NAS: De storage-omgeving is via het netwerk met de back-upserver verbonden
- Tape/virtual tape library (VTL): Een (virtuele) tape library waarvan de fysieke of virtuele opslageenheden kunnen worden uitgeworpen en soms te verwijderen zijn (air gapping)
- Object store (zoals S3): Een optimaal schaalbare storage-omgeving die lokaal (on premises) of bij een dienstverlener staat (in de cloud)

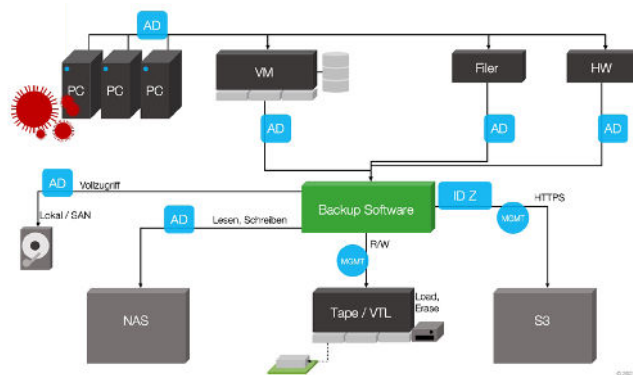
De 'klassieke' ransomware-aanval via de IT-infrastructuur

Bij **ransomware-aanvallen via een pc** zijn de toegangsrechten van de gebruiker cruciaal. Veel bedrijven geven speciale gebruikers, zoals managers en afdelingshoofden, alle beheerdersrechten. Zij hebben zo toegang tot een deel van de IT-infrastructuur of soms zelfs de complete omgeving.

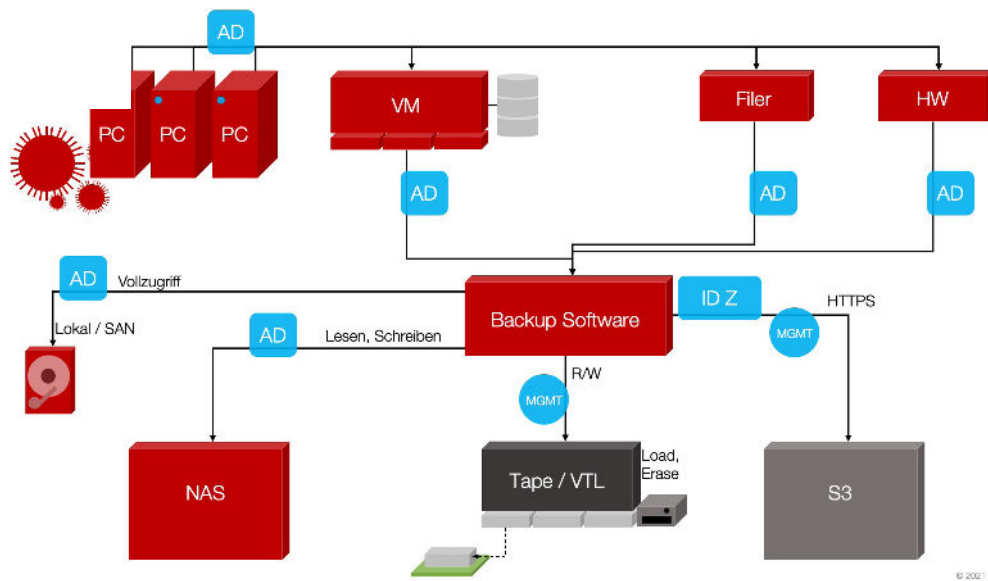
Voor een gebruiker met speciale toegangsrechten ziet het aanvalsgebied van ransomware er als volgt uit:

- De ransomware valt alle apparaten aan die via het netwerk toegankelijk zijn en besmet die. De malware richt zich eerst op gedeelde netwerkmappen op andere pc's, file servers en gedeelde mappen binnen hardwarecomponenten. Vervolgens verspreiden deze zich naar de back-upserver en de lokale en NAS-opslag. Ten slotte volgt de versleuteling van alle gegevens op de besmette apparaten.

Na zo een omvangrijke encryptie is het belangrijk te achterhalen hoe de ransomware de IT-omgeving binnenkwam en wat er precies besmet en versleuteld is. In dit scenario bieden back-ups via (virtuele) tape libraries een uitweg uit deze penibele situatie.

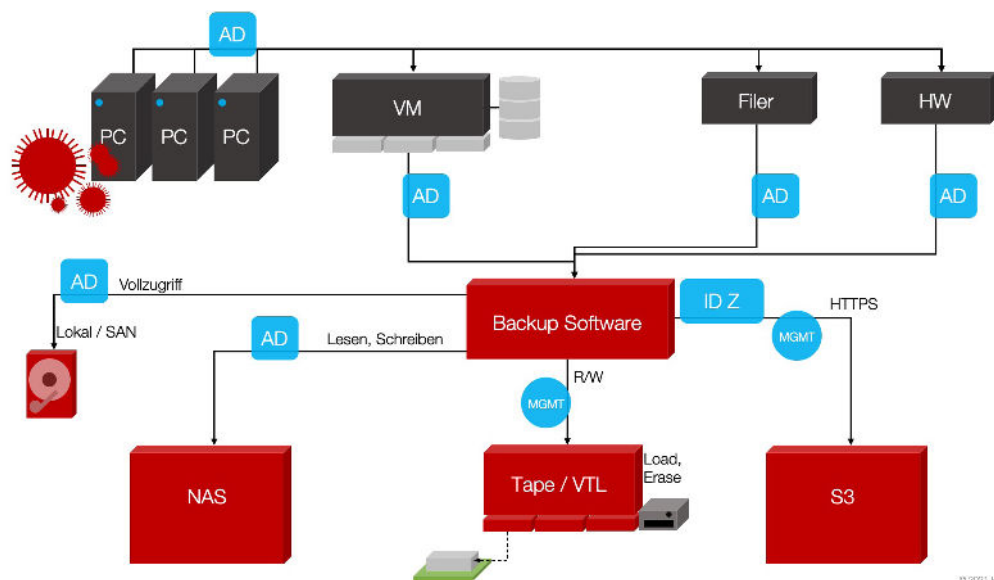


Ransomware-aanvallen gebeuren vaak via individuele gebruikers/pc's



'Klassieke' ransomware-aanvallen infecteren en versleutelen alles wat via het netwerk toegankelijk is

Ransomware-aanvallen speciaal gericht op back-ups



Targeted attacks first spy on access rights and then first infect backups

Bij een **gerichte ransomware-aanval** willen cybercriminelen eerst onherstelbare schade aan de back-upomgeving veroorzaken om te zorgen dat reservekopieën niet langer te herstellen zijn. Pas dan volgt de aanval op de reguliere IT-omgeving. Zo blijft de aanval zo lang mogelijk verborgen. Gebruikers en beheerders krijgen de melding dat hun data versleuteld is en dat ze losgeld moeten betalen voor toegang.

- Ook in dit geval loopt de aanval meestal via individuele gebruikers of pc's. In tegenstelling tot een klassieke ransomware-aanval begint een gerichte aanval niet met een grootscheepse verspreiding van deze malware. Eerst wordt de IT-infrastructuur van het doelwit grondig verkend. De belangrijkste IT-component om zoveel mogelijk systemen te besmetten is de Active Directory. Dit systeem ondersteunt centraal beheer van de toegangsrechten van alle gebruikers.
- Als cybercriminelen toegang krijgen tot een beheerder-saccount voor Active Directory (ook wel een 'gouden ticket' of 'loper' genoemd), ligt daarmee de complete IT-infrastructuur voor hen open.

- Eerst worden de back-upserver en zijn lokale en NAS-opslag besmet.
- Het grote voordeel van een (virtuele) tape library is in dit geval een groot nadeel: cybercriminelen met toegang tot de back-upsoftware krijgen daarmee de volledige regie over de back-upomgeving in handen. Ze kunnen alle data op geïnstalleerde opslagmedia dan relatief eenvoudig wissen. Dat betekent dat alleen back-ups op media die fysiek uit het systeem zijn verwijderd nog veilig zijn voor ransomware.
- Cybercriminelen kunnen de toegangsrechten voor object storage-systemen meestal niet zo makkelijk achterhalen. Maar als zij ID's en toegangscodes hebben, krijgen ze toegang tot het systeem en kunnen ze complete buckets te wissen.
- Na het versleutelen of verwijderen van alle benaderbare back-ups kunnen ze ook de rest van de IT-infrastructuur versleutelen.

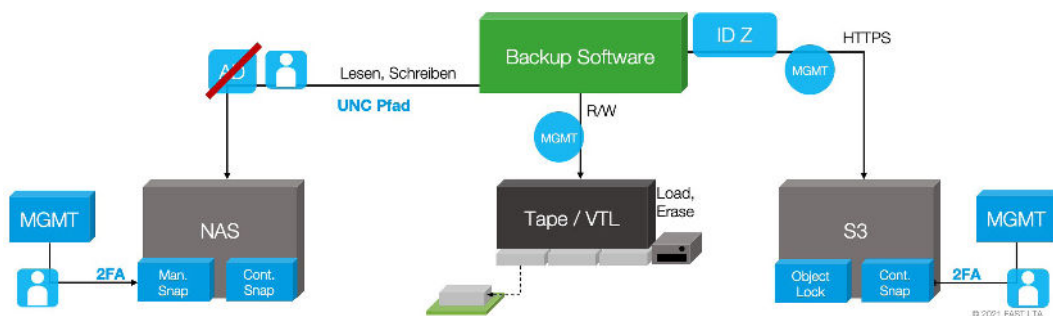
Na zo'n succesvolle aanval is datatoegang of -herstel geen optie meer.

Back-ups beveiligen

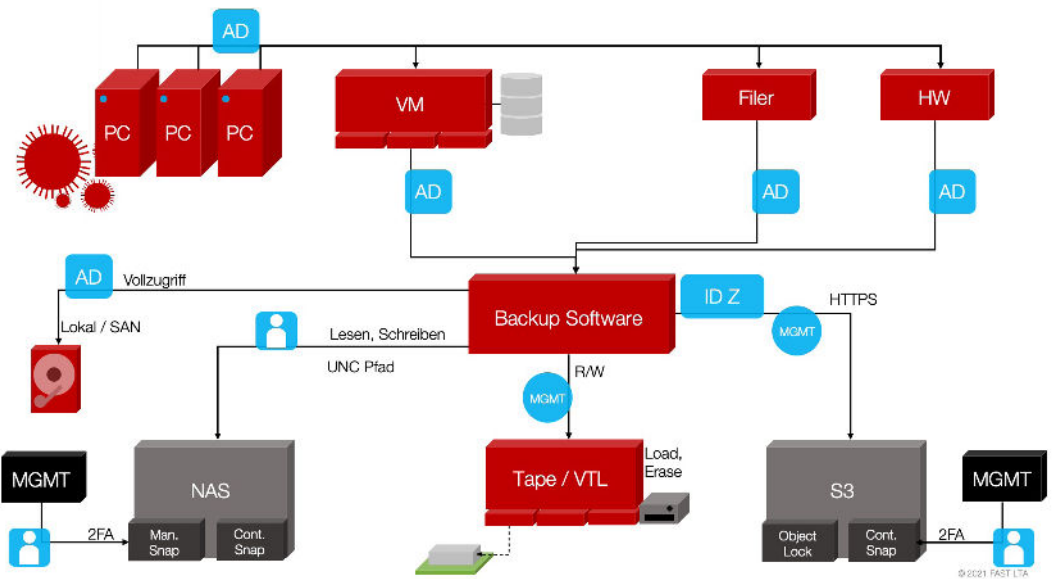
Bescherming tegen deze aanvallen vraagt diverse aanpassingen van het back-upstelsel. Kort gezegd is het zaak alle toegangsrechten voor databescherming te isoleren van het algemene beheer van toegangsrechten en deze extra te beveiligen.

- Het is aan te raden de NAS-opslag niet direct als schijf in de back-upinfrastructuur te installeren en niet via Active Directory te beheren. Beter is om een extra drempel voor cybercriminelen op te werpen met afzonderlijke toegang tot de NAS-opslag, inclusief een beschermd UNC-pad dat alleen de back-upsoftware kent.
- Ook het beheer van de NAS-opslag en object storage moet worden gescheiden van Active Directory en bij afzonderlijke gebruikers worden ondergebracht. Deze gebruikers hebben alleen toegang tot het back-upstelsel met twee-factor-authenticatie (2FA). Alleen een beheerder met het juiste token krijgt toegang tot de snapshots en kan deze wijzigen of de snapshotlogica stopzetten of hervatten.
- In het geval van een ransomware-aanval op NAS- of S3-opslag, beschermen mechanismen binnen in plaats van buiten de storage-oplossing de data.

Voor de NAS-opslag gebruikt FAST LTA snapshots. Die zijn handmatig aan te maken of automatisch door het back-upstelsel. Snapshots worden volledig binnen het systeem aangemaakt en zijn niet van buitenaf te benaderen via het UNC-pad of de back-upsoftware. De object store biedt verder de mogelijkheid om data tegen verwijdering te beschermen. Aanvullend op het beschermen van afzonderlijke objecten met een object lock te beschermen biedt FAST LTA continuous snapshots. Deze beschermen de complete bucket door de gegevens onwijzigbaar ('immutable') te maken.



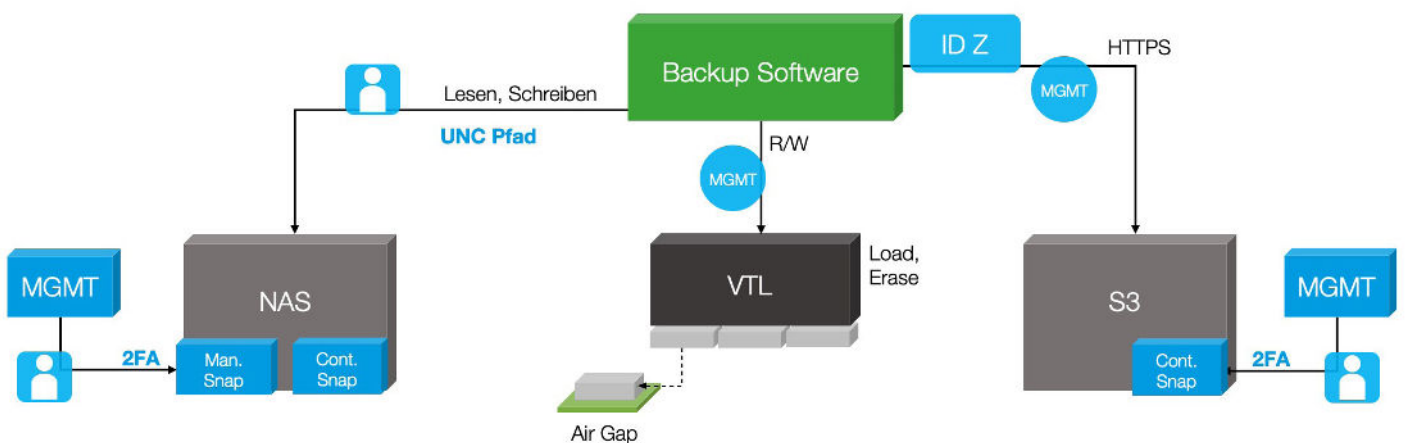
Isolatie en extra beveiliging van de opslag van back-ups bieden bescherming tegen ransomware-aanvallen



Ransomware kan de NAS-opslag, offline media en object stores niet langer besmetten

Als deze aanpassingen gedaan worden, blijven bij een aanval een offline opslagmedium van de (virtuele) tape library (tape of een uitgeworpen Silent Brick), de NAS-opslag en de object storage beschikbaar voor het herstellen van gegevens. De combinatie van continuous snapshots en air gapping beschermt back-ups tegen dataverlies.

Dit is mogelijk met het Silent Brick System van FAST LTA. Zoals eerder aangestipt zijn er uiteenlopende typen gegevens die verschillende eisen aan de IT-opslag stellen. FAST LTA biedt voor elk back-upscenario een passend Silent Brick System.



Silent Brick Flash



Silent Brick (VTL)



Silent Brick DS

Een moderne back-upoplossing: air gapping met Silent Bricks

Een moderne back-upoplossing kan wel zonder tapes, maar niet zonder air gapping. Het Silent Brick System is een storage-oplossing die tegemoet komt aan alle eisen voor databescherming en kan fungeren als archief, back-upstelsysteem en file server.

De Silent Bricks, de feitelijke opslagunits, zijn beschikbaar als stationair opslagmedium (Silent Brick DS) en als verwijderbaar en transporteerbaar opslagmedium voor offline gebruik (Silent Brick). Hierdoor zijn alle moderne back-upscenario's te realiseren, inclusief air gapping met medirotatie en zelfs hardwarematige write once read many (WORM)-beveiliging.

Contacteer ons voor aanvullende informatie:

- » Feitencheck "Wat kost een ransomware-aanval?"
- » Feitencheck "Wat kost een veilige backup?"
- » Het YouTube-kanaal van FAST LTA – <https://fastlta.com/youtube>



Silent Brick Controller met één Silent Brick Flash en één Silent Brick, onder de Silent Brick DS



Silent Brick (offline)



FAST LTA

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

FAST LTA | Ruedesheimer Str. 11 | 80686 Munich, Germany | info@fast-lta.de | www.fast-lta.com