Hoe kan de back-upstrategie voor de Azure PostgreSQL en MySQL databases bij Forvis Mazars geoptimaliseerd worden door het gebruik van immutabele opslag en automatische back-ups?: Een Proof-of-Concept met immutabele opslag en automatische back-ups.

Naoufal Bouazzaoui.

Scriptie voorgedragen tot het bekomen van de graad van
Professionele bachelor in de toegepaste informatica

Promotor: Martijn Saelens
Co-promotor: Rémy Tetaert
Academiejaar: 2024-2025
Eerste examenperiode

Departement IT en Digitale Innovatie .

HO
GENT

Woord vooraf

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Samenvatting

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

Lijst van codefragmenten

1

Inleiding

De beveiliging van gegevens is van cruciaal belang voor organisaties, vooral gezien de toenemende dreigingen van cyberaanvallen zoals ransomware. Gezien de digitale transformatie die veel bedrijven doormaken, zijn betrouwbare en veilige back-upoplossingen essentieel om de continuïteit van de bedrijfsvoering te waarborgen. Dit geldt in het bijzonder voor bedrijven die werken met cloudplatformen zoals Microsoft Azure, waar databases zoals PostgreSQL en MySQL vaak cruciaal zijn voor het dagelijks functioneren. Bij Forvis Mazars worden momenteel back-ups van Azure-databases gemaakt via een combinatie van automatische volledige back-ups en handmatige back-ups via scripts. Deze aanpak kent echter enkele beperkingen, zoals de onregelmatige uitvoering van de handmatige back-ups en een gebrek aan geautomatiseerde processen, wat de veiligheid en efficiëntie van het systeem in gevaar kan brengen.

1.1. Probleemstelling

In deze bachelorproef wordt de huidige back-upstrategie van Forvis Mazars geanalyseerd en geoptimaliseerd. De focus ligt hierbij op het verbeteren van de back-upstrategie voor de Azure PostgreSQL en MySQL databases, met bijzondere aandacht voor ransomware-resistentie en de integratie van immutabele opslagtechnieken. Het doel is om de bestaande strategie te versterken en de kans op dataverlies door cyberaanvallen te minimaliseren. Daarnaast zal er een proof of concept worden uitgevoerd om de effectiviteit van immutabele opslag te testen in een scenario waarbij een ransomware-aanval wordt nagebootst op mock-up bestanden. De probleemstelling van dit onderzoek is dat de huidige back-upstrategie bij Forvis Mazars niet voldoende robuust is om het risico op dataverlies door ransomware effectief te mitigeren. Dit onderzoek heeft tot doel de back-upstrategieën van Forvis Mazars te verbeteren door middel van geautomatiseerde processen en door ge-

bruik te maken van immutabele opslag voor extra beveiliging tegen dataverlies. De doelgroep van dit onderzoek bestaat uit Forvis Mazars

1.2. Onderzoeksvraag

De onderzoeksvraag van deze bachelorproef luidt:

Hoe kan de back-upstrategie voor Azure PostgreSQL en MySQL databases bij Forvis Mazars worden geoptimaliseerd met behulp van immutabele opslag en automatische back-ups?

1.3. Deelvragen

De onderzoeksvraag kan verder opgedeeld worden in de volgende deelvragen.:

- Hoe veilig en betrouwbaar zijn de huidige back-upoplossingen van Forvis Mazars voor Azure PostgreSQL en MySQL databases?
- Welke rol speelt immutabele opslag in het beschermen van back-ups tegen ransomware en andere vormen van dataverlies?
- Wat zijn de belangrijkste uitdagingen bij het integreren van immutabele opslag met Azure cloud back-upsystemen?
- Hoe kan er voor de Azure PostgreSQL en MySQL databases een automatische back-upstrategie worden geïmplementeerd?

1.4. Onderzoeksdoelstelling

Het doel van dit onderzoek is om de back-upstrategie van Forvis Mazars te optimaliseren door de huidige back-upmethoden te analyseren en te verbeteren. Het onderzoek richt zich specifiek op het implementeren van immutabele opslag om de bescherming tegen ransomware-aanvallen te versterken. Daarnaast wordt de automatisering van de manuele back-ups onderzocht en geïmplementeerd, aangezien deze momenteel niet frequent genoeg worden uitgevoerd. Een proof of concept (PoC) zal worden uitgevoerd door virtuele machines te gebruiken en een ransomware-aanval na te bootsen om de effectiviteit van de immutabele opslag te testen. Het doel van dit PoC is om een werkende oplossing voor immutabele opslag op te zetten in de Azure-omgeving van Forvis Mazars, en de voordelen van deze oplossing voor hun back-upstrategie te evalueren. Dit proefproject zal verder bijdragen aan het verbeteren van de bestaande automatische back-upstructuur door het toevoegen van meer geautomatiseerde processen, wat de efficiëntie en de veiligheid van het back-upbeheer binnen het bedrijf zal vergroten.

1.5. Opzet van deze bachelorproef

De rest van deze bachelorproef is als volgt opgebouwd:

Hoofdstuk 2 biedt een overzicht van de huidige kennis en technologieën rondom back-upstrategieën, ransomware-beveiliging en immutabele opslag. De literatuur helpt de basis te leggen voor het verbeteren van de back-upbeveiliging bij Forvis Mazars.

In hoofdstuk 3 worden de stappen van het onderzoek beschreven. Een requirementsanalyse werd uitgevoerd om de huidige back-upstrategie van Forvis Mazars te evalueren en verbeterpunten te identificeren. Vervolgens werd de opzet voor een Proof-of-Concept (PoC) uitgewerkt.

Hoofdstuk 4 onderzoekt de huidige back-upstrategie bij Forvis Mazars en stelt verbeteringen voor, zoals de automatisering van handmatige back-ups en het implementeren van immutabele opslag voor verhoogde veiligheid.

In dit hoofdstuk 5 wordt de uitvoering van het proof of concept beschreven, waarin immutabele opslag wordt getest door een ransomware-aanval na te bootsen op een virtuele machine en de effectiviteit van immutabele opslag te evalueren.

In hoofdstuk 6, tenslotte, wordt de conclusie gegeven en een antwoord geformuleerd op de onderzoeksvragen. Daarbij wordt ook een aanzet gegeven voor toekomstig onderzoek binnen dit domein.

2

Stand van zaken

2.0.1. Back-ups in het kader van bedrijfscontinuïteit en disaster recovery

Bedrijfscontinuïteit verwijst naar de aanpak en procedures dat een bedrijf gebruikt om de voortgang van zijn werkzaamheden te bewaren, zelfs in het geval van incidenten. Deze incidenten kunnen variëren van relatief kleine problemen, zoals een gebroken netwerkverbinding, tot grote natuurrampen zoals een ardbevingen. Omdat er zoveel soorten incidenten kunnen gebeuren is het moeilijk om een oplossing te vinden die ervoor zorgt dat bedrijven in alle gevallen beschermt zijn. In plaats daarvan gebruiken bedrijven een mix van strategieën en technologieën om de continuïteit van hun processen te beschermen.

De 2 belangrijkste concepten voor de bedrijfscontinuïteit zijn hoge beschikbaarheid en disaster recovery. Hoge beschikbaarheid duidt op het feit dat een bedrijf zodanig is ingericht dat het kan blijven draaien, zelfs als bepaalde systemen of componenten uitvallen. Een voorbeeld hiervan zijn twee routers die zijn geconfigureerd in een actieve-passieve opstelling. In deze configuratie is één router de primaire router die al het inkomende en uitgaande verkeer verwerkt, terwijl de andere router als reserve werkt. In het geval dat de primaire router faalt door een hardwarestoringen of netwerkprobleem, dan neemt de tweede router automatisch de rol van de primaire router over, zonder dat dit merkbare impact heeft op de netwerkverbindingen van de organisatie. Hierdoor blijft de beschikbaarheid van het netwerk gegarandeerd en blijft de downtime laag (Zhu e.a., 2015). Disaster recovery (DR) is een onderdeel van bedrijfscontinuïteit dat zich specifiek richt op het herstellen van bedrijfsactiviteiten na een incident zoals een cyberaanval of ernstige verstoring. Terwijl bedrijfscontinuïteit zich richt op bredere preventieve maatregelen om de continuïteit te waarborgen, focust disaster recovery zich juist op de praktische stappen en hulpmiddelen die nodig zijn om de organisatie na een verstoring weer snel operationeel te maken. Het doel van disaster recovery is om schade zoveel

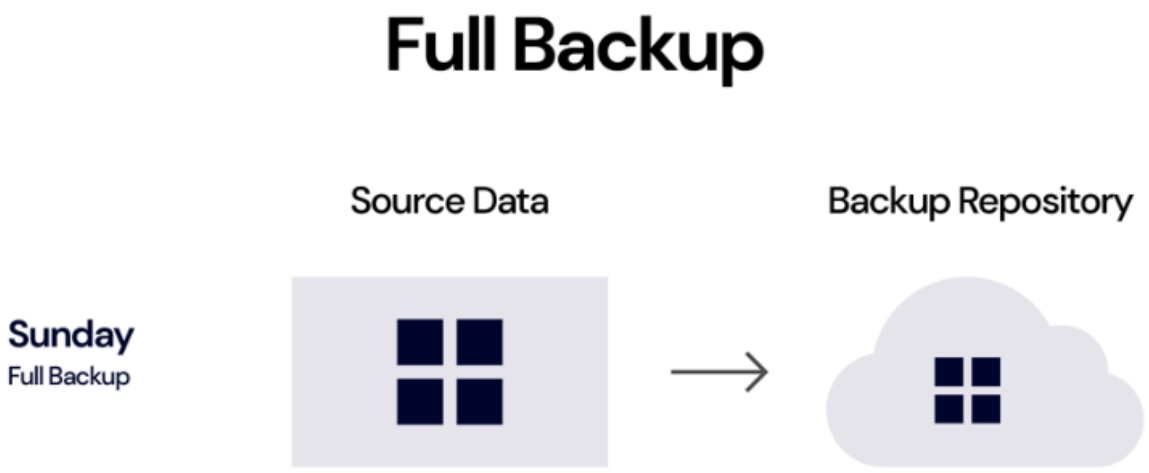
mogelijk te beperken en de normale gang van zaken zo snel mogelijk te herstellen. Back-ups spelen een belangrijke rol voor de continuïteit van een bedrijf en zijn vaak de eerste stap bij het opstellen van een disaster recovery plan (DRP). Bij een optimale situatie is er na een incident geen data verloren en is alle data relatief snel terug beschikbaar. Indien een bedrijf geen back-ups heeft van de belangrijke data zal de data in het geval van een incident verloren raken. Zonder back-ups zal het ook een grotere uitdaging zijn voor het bedrijf om de normale bedrijfsactiviteiten terug uit te voeren. Een belangrijke doelstelling van een bedrijf is winst maken. In het geval van een incident waarbij de bedrijfsactiviteiten niet normaal kunnen verlopen zal deze doelstelling verhindert worden en zal er dus financieel verlies optreden. Bij specifieke bedreigingen, zoals ransomware-aanvallen spelen ransomware-resistente back-ups een cruciale rol. Door back-ups te beveiligen tegen ransomware-aanvallen kunnen bedrijven hun data herstellen zonder losgeld te betalen. Dit benadrukt het belang van back-ups die niet alleen snel toegankelijk zijn, maar ook bestand zijn tegen digitale bedreigingen (Ghazi & H. O. Nasereddin, 2013).

2.0.2. Back-upmethoden en -technieken

Back-ups zijn een belangrijk onderdeel voor het managen en beveiligen van data binnen organisaties. Back-ups zorgen voor de continuïteit van bedrijfssystemen in het geval van een incident zoals een cyberaanval. Back-ups zijn snapshots van gegevens die op een bepaald tijdstip zijn gemaakt, opgeslagen in een wereldwijd gebruikelijk formaat en gedurende een bepaalde periode van bruikbaarheid worden bijgehouden, waarbij elke volgende kopie van de gegevens onafhankelijk van de eerste wordt bewaard(Nelson & Brown, 2011). Door een aparte kopie van de gegevens te bewaren, kunnen bedrijven en individuen na een incident hun systemen of bestanden herstellen naar een eerdere, veilige staat. Hierbij kunnen back-ups zowel volledige datasets als selectieve bestandstypen omvatten, afhankelijk van de strategie en de specifieke behoeften van de organisatie. Back-ups zijn een preventieve maatregel en het doel ervan is om dataverlies tegen te gaan. Dataverlies kan optreden door menselijke fouten, cyberaanvallen, en natuur- of bedrijfsrampen. Daarbij speelt beveiliging een belangrijke rol in een tijd waarin ransomware-aanvallen en datalekken frequenter voorkomen. Door back-ups versleuteld op te slaan en te beveiligen tegen ongeautoriseerde toegang, kunnen bedrijven zich beschermen tegen het verliezen van data.

Full back-ups

Een full back-up is een back-upmethode waarbij alle gegevens van een systeem op een specifiek moment volledig worden gekopieerd en opgeslagen. Dit betekent dat elk bestand zonder uitzonderingen wordt gekopieerd, zodat er een exacte kopie van de volledige dataset ontstaat (Beard, 2018). Wanneer er zich een probleem voordoet, zoals het falen van een harde schijf, kan het hele bestandssysteem vanaf

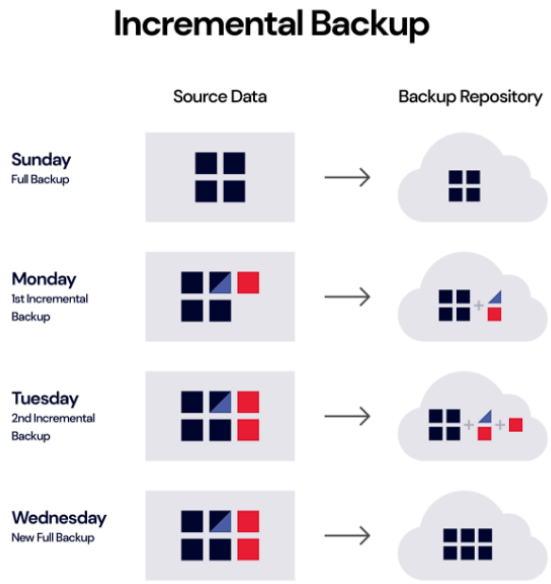


Figuur 2.1: Representatie van een full back-up (Rivas, 2022)

deze back-up volledig worden hersteld op een nieuwe schijf. Daarnaast kunnen ook individuele bestanden die verloren zijn gegaan, gemakkelijk worden teruggehaald uit de back-up. Dit soort back-up zorgt ervoor dat alle gegevens veilig zijn opgeslagen (Chervenak e.a., 1998). Full back-ups vormen vaak de basis van een back-upstrategie en worden regelmatig uitgevoerd om ervoor te zorgen dat alle gegevens volledig hersteld kunnen worden. Het concept en de implementatie van een full back-up is relatief eenvoudig omdat alle gegevens op één locatie zijn opgeslagen. Aan de andere kant is er het probleem van opslagcapaciteit. Stel bijvoorbeeld dat een bedrijf elke nacht een full back-up maakt van zijn servers naar een cloudopslagdienst, waarbij per keer 500 GB aan data wordt opgeslagen. Na een week is er al 3,5 terabyte aan gegevens in de cloud opgeslagen. Aangezien cloudproviders vaak kosten in rekening brengen op basis van gebruikte opslagcapaciteit en dataverkeer, kan dit snel leiden tot aanzienlijke maandelijkse kosten. Bedrijven met een beperkt IT-budget kunnen hierdoor in de problemen komen of worden gedwongen om strenger te selecteren welke gegevens ze precies opslaan in de back-up, omdat de opslagkosten oplopen naarmate de hoeveelheid opgeslagen data toeneemt. Daarbij kan het proces zelf ook veel tijd innemen. Dit kan voor problemen zorgen bij bedrijven waarbij de systemen aan moeten blijven. Vaak worden full back-ups gecombineerd met andere back-upmethodes. Daarnaast kost een full back-up veel tijd, wat een uitdaging kan zijn in omgevingen waar snelle gegevensbeschikbaarheid nodig is. Stel bijvoorbeeld dat een groot bedrijf tijdens kantooruren een full back-up wil maken van alle gegevens. Omdat deze back-up meerdere uren in beslag kan nemen, worden de systemen gedurende die tijd zwaar belast. Dit kan ertoe leiden dat andere processen vertraging oplopen of dat de server tijdelijk minder goed beschikbaar is voor werknemers die ook van die systemen afhankelijk zijn voor hun dagelijkse taken. Vanwege deze nadelen is het

vaak beter om full back-ups aan te vullen met andere methoden (Nelson & Brown, 2011).

Incrementele back-up

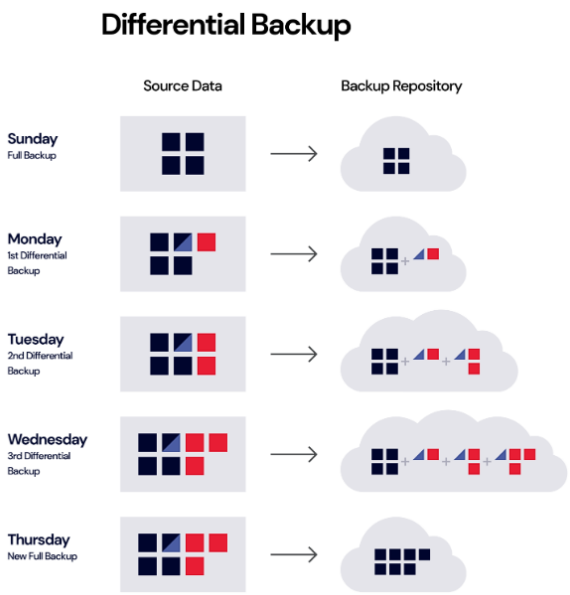


Figuur 2.2: Representatie van een incremental back-up (Rivas, 2022)

Een incrementele back-upstrategie houdt in dat na een initiële full back-up slechts de gegevens worden opgeslagen die sinds de laatste back-up zijn gewijzigd (Zhao e.a., 2024). Dit betekent dat een incrementele back-up alleen de veranderingen in de bestanden opneemt, in plaats van telkens een volledige kopie te maken van alle gegevens. Dit is vooral handig voor bedrijven die relatief vaak back-ups moeten maken, maar de opslag- en tijdskosten van een full back-up willen vermijden. Bijvoorbeeld, stel dat een bedrijf op maandag een full back-up uitvoert met al hun gegevens. Op dinsdag doet het bedrijf een incrementele back-up, waarbij enkel de wijzigingen sinds maandag worden opgeslagen. Dit gaat elke dag zo verder, elke dag wordt enkel de nieuwe of gewijzigde data opgeslagen ten opzichte van de dag ervoor. Omdat bedrijven steeds meer data beheren, biedt deze methode een efficiënte manier om opslagkosten te beperken, vooral wanneer gebruik wordt gemaakt van een cloudservice. Stel dat een bedrijf dagelijks slechts 1% van zijn gegevens wijzigt; in plaats van elke dag een volledige kopie van bijvoorbeeld 1 TB te maken, slaat een incrementele back-up slechts de nieuwe 1% op, wat 990 GB aan opslagruimte per dag bespaart. Dit maakt incrementele back-ups heel aantrekkelijk voor bedrijven die grote hoeveelheden data verwerken en frequente back-ups willen uitvoeren. Naast de besparing op opslagcapaciteit, zorgen incrementele back-ups voor kortere back-uptijden omdat alleen de gewijzigde bestanden worden opgeslagen. Dit betekent dat bedrijven vaker back-ups kunnen uitvoeren zonder hun systemen te vertragen. Een mediabedrijf dat met grote bestanden werkt,

kan hierdoor bijvoorbeeld elk uur een incrementele back-up maken, in plaats van dagelijks een volledige back-up. Dit minimaliseert het risico op dataverlies, omdat in het geval van een storing, slechts maximaal een uur aan data verloren gaat in plaats van een hele dag. Hoewel incrementele back-ups voordelen bieden op het gebied van opslag en back-uptijden, brengen ze ook nadelen met zich mee, zoals langere hersteltijden (Chervenak e.a., 1998). Om een systeem te herstellen, heb je de laatste volledige back-up en alle volgende incrementele back-ups nodig en dit kan veel tijd kosten. Een financiële instelling die bijvoorbeeld op vrijdag een een systeemherstel moet uitvoeren, zal de volledige back-up van maandag plus alle incrementele back-ups tot en met donderdag moeten doorlopen. Dit kan relatief lang duren, wat leidt tot langere downtime, vooral in een noodsituatie waarin snelle hersteltijd van belang is. Een ander nadeel is de complexiteit van het beheer. Elke incrementele back-up hangt af van de vorige, wat betekent dat een fout in één back-up de hele herstelketen kan verstoren. Een IT-bedrijf dat dagelijks incrementele back-ups maakt, kan bijvoorbeeld problemen ondervinden als de back-up van woensdag beschadigd blijkt te zijn. Alle latere back-ups zijn afhankelijk van die ene back-up, wat het herstelproces moeilijker maakt. Dit vraagt om extra monitoring en beheer, zodat eventuele beschadigingen of herstelproblemen tijdig kunnen worden opgemerkt en opgelost.

Differentiële back-ups



Figuur 2.3: Representatie van een differentiële back-up (Rivas, 2022)

Een differentiële back-up is een soort back-up waarbij enkel de data die sinds de laatste full back-up is veranderd of toegevoegd, wordt gekopieerd. In tegenstelling tot een incrementele back-up, die enkel de veranderingen sinds de laatste back-up opslaat, wordt er bij een differentiële back-up enkel de wijzigingen opge-

slagen sinds de laatste full back-up (Zhu e.a., 2015). Een differentiële back-up zal dus elke keer groter en groter worden naarmate er meer wijzigingen zijn omdat elke wijziging sinds de full back-up opgeslagen wordt. Een eerste voordeel van deze soort back-up is dat er in het geval van een recovery slechts twee back-ups nodig zijn: de laatste full back-up en de meest recente differentiële back-up. Wanneer hersteltijden belangrijk zijn zullen differentiële back-ups dus handig zijn. Bijvoorbeeld, een organisatie die dagelijks een differentiële back-up uitvoert, heeft na een week slechts de volledige back-up van de eerste dag en de laatste differentiële back-up nodig om alles te herstellen. Dit zorgt voor een relatief eenvoudig en snel herstelproces. Incrementele back-ups daarentegen slaan alleen de veranderingen op die sinds de laatste back-up zijn gemaakt van eender welke soort, of het nu een volledige of incrementele back-up is. Hierdoor zijn incrementele back-ups meestal kleiner en sneller uit te voeren dan differentiële back-ups, omdat ze alleen de allerlaatste wijzigingen bevatten. Een eerder besproken nadeel is echter dat bij herstel alle opeenvolgende back-ups nodig zijn om de data volledig terug te zetten: de laatste volledige back-up en alle incrementele back-ups tot de meest recente back-up. Dit maakt incrementele back-ups soms trager en complexer bij recovery, omdat elk back-upbestand moet worden doorlopen. Een voorbeeld om het verschil tussen incrementele back-ups en differentiële back-ups duidelijk te maken: stel dat een bedrijf aan het begin van de week een volledige back-up maakt. Bij het gebruik van een differentieel back-upschema zou elke back-up in de loop van de week groter worden, omdat elke back-up alle wijzigingen sinds die eerste dag bevat. Bij een incrementeel schema daarentegen blijft elke dagelijkse back-up klein, omdat elke nieuwe back-up alleen de nieuwste wijzigingen bevat. Als het systeem aan het einde van de week moet worden hersteld, zou met een differentieel schema enkel de full back-up en de laatste differentiële back-up nodig zijn. Bij het gebruik van incrementele-backups zijn alle back-ups van de week vereist (Beard, 2018).

Cloud back-ups

Cloud back-ups zijn een populaire methode waarbij data op externe servers wordt opgeslagen, beheerd door een derde partij. In plaats van lokale fysieke opslagapparaten te gebruiken, worden de gegevens overgebracht naar een cloud-omgeving, zoals die van Amazon Web Services, Microsoft Azure of Google Cloud. Cloud back-ups bieden verschillende voordelen, zoals schaalbaarheid, eenvoud in beheer en de mogelijkheid om gegevens veilig op afstand op te slaan (Rahumed e.a., 2011). Bedrijven hoeven hierdoor geen geld te investeren in fysiek hardware. Stel dat een bedrijf snel groeit of opeens veel meer data heeft, dan kan het makkelijk zijn cloud-opslag uitbreiden zonder de IT-infrastructuur aan te passen wat veel geld en moeite zou kosten. Een van de belangrijkste voordelen van cloud back-ups is toegankelijkheid. Aangezien de gegevens zich op een externe server bevinden, kan een bedrijf op elk moment en vanaf elke locatie toegang krijgen tot zijn data, zolang er een internetverbinding is. Dit is vooral handig voor bedrijven die meerdere

fysieke locaties hebben. Stel dat een bedrijf op internationaal vlak actief is: de medewerkers kunnen overal ter wereld op dezelfde back-ups vertrouwen die up-to-date zijn, dit zorgt voor een soepele samenwerking en helpt de continuïteit van het bedrijf zelfs in geval van nood. Daarnaast biedt cloud-opslag een hoge mate van beveiliging, aangezien cloud-providers meestal robuuste beveiligingsprotocollen implementeren, zoals encryptie, firewalls en multi-factor authenticatie. Voor relatief kleine bedrijven betekent dit dat zij kunnen profiteren van een hoger beveiligingsniveau zonder te investeren in geavanceerde beveiligingsinfrastructuur. Stel dat een middelgroot marketingbureau zijn klantgegevens in de cloud opslaat; de back-ups zijn dan beschermd tegen onvoorziene omstandigheden, zoals fysieke schade aan hun eigen kantoren. Echter, cloud back-ups hebben ook nadelen, waaronder de afhankelijkheid van een stabiele internetverbinding. Omdat cloud back-ups vereisen dat data over het internet wordt verzonden, kunnen problemen met de internetverbinding de back-uptijd vertragen of de overdracht volledig onderbreken. Voor een organisatie die bijvoorbeeld grote hoeveelheden videobestanden moet opslaan, kan dit tijdsverlies betekenen, vooral wanneer zij gevestigd zijn op een locatie met beperkte bandbreedte. Dit kan een probleem vormen wanneer er een strikte back-upfrequentie vereist is. Een ander nadeel is de kostprijs, vooral wanneer grote hoeveelheden gegevens vaak worden geüpdatet en opgeslagen (Obrutsky, 2016). Cloud-providers vergoeden meestal de hoeveelheid opslagruimte, het dataverkeer en extra functies zoals betere encryptie of de frequentie van de back-ups. Voor een bedrijf dat veel wijzigingen aanbrengt in grote databases, zoals een online retailer met dagelijks nieuwe productinformatie, kunnen de maandelijkse kosten aanzienlijk oplopen. Dit maakt het noodzakelijk om een weloverwogen keuze te maken over de frequentie en omvang van back-ups om de kosten beheersbaar te houden. Tot slot biedt de cloud niet altijd dezelfde mate van controle als on-premise oplossingen. Hoewel cloudproviders doorgaans goede service garanderen, blijft het bedrijf afhankelijk van de beschikbaarheid en het onderhoudsbeleid van de provider. Dit betekent dat, in het geval van een storing bij de cloudprovider, bedrijven geen directe toegang hebben tot hun eigen back-ups. Een juridische firma die vertrouwelijke documenten in de cloud opslaat, kan bijvoorbeeld beperkte toegang hebben tot deze gegevens als de cloudprovider technische problemen ondervindt. Dit benadrukt het belang van goed service level agreements (SLA's) en mogelijk zelfs een hybride strategie die cloudopslag combineert met een bepaalde vorm van lokale back-ups om het risico te spreiden.

On-premise back-ups

On-premise back-ups zijn lokale back-ups die op fysieke servers binnen het bedrijf zijn opgeslagen. Het bedrijf is dus zelf verantwoordelijk voor het beheer, de beveiliging en het onderhoud van de back-upomgeving (Trovato e.a., 2019). Dit biedt bedrijven vrijheid en flexibiliteit, maar vereist wel een hoger niveau van technische kennis en onderhoud. On-premise back-ups bieden volledige controle over de ge-

gevens, wat vooral belangrijk is in sectoren waar veiligheid en privacy cruciaal zijn, zoals de gezondheidszorg en financiële sector. Een groot voordeel is dat er geen nood is aan het internet, waardoor de snelheid van het back-upproces afhangt van de hardware dat het bedrijf bezit. Dit is ideaal voor bedrijven die snel grote hoeveelheden data moeten opslaan. Toch hebben on-premise back-ups ook nadelen. Ze vereisen een hoge initiële investering in hardware en onderhoud, zoals servers en netwerkinfrastructuur. Daarnaast zijn ze kwetsbaar voor fysieke risico's zoals brand, diefstal of natuurrampen, wat vraagt om extra beveiligingsmaatregelen, zoals off-site back-ups. Daarbij is er ook een IT-expert nodig voor de implementatie van deze back-upsystemen, dit is soms moeilijk voor kleinere organisaties die geen speciale IT-expert hebben die dit kan doen.

2.0.3. Ransomware

Ransomware is een groeiende dreiging dat ervoor kan zorgen dat bedrijven hun gegevens voor een bepaalde tijd kwijt zijn of in het slechtste geval voor altijd kwijt zijn. Daarom moeten bedrijven zich sterk inzetten op het implementeren van een sterke back-upstrategie. Back-ups zijn het laatste redmiddel tegen ransomware-aanvallen, omdat ze een veilige kopie van data kunnen herstellen zonder te doen wat de aanvallers willen. Ransomware is een type malware dat data vergrendelt of de toegang tot gegevens blokkeert door middel van privé-sleutel encryptie, tot-dat er losgeld wordt betaald, meestal in Bitcoin (Richardson & North, 2017). Malware is een softwareprogramma dat opzettelijk voldoet aan de schadelijke bedoelingen van kwaadwillende aanvallers (Yanfang e.a., 2017). Deze aanvallen kunnen niet alleen bestanden versleutelen, maar soms ook volledige systemen blokkeren, waardoor de toegang tot cruciale data verloren gaat. De gevolgen zijn vaak ernstig, omdat slachtoffers pas weer controle krijgen als ze aan de eisen van de aanvallers voldoen. Zelfs wanneer het losgeld betaald wordt, is er geen garantie dat de toegang wordt hersteld of dat de gegevens niet zijn beschadigd. Het betalen van de criminelen biedt echter geen garantie voor de toegang van de data en dit kan eindigen in een eindeloze cirkel waarbij de aanvaller elke keer opnieuw geld vraagt.

Evolutie

De evolutie van ransomware laat een gestage groei zien sinds het einde van de jaren '80. In 1989 verscheen het eerste ransomwarevirus, de AIDS Trojan, die eenvoudige versleuteling gebruikte. In 2005 kwam de moderne ransomware met Trojan.Gpcoder, die nog zwakke encryptie toepaste. Vanaf 2006 nam de populariteit van ransomware toe, met varianten zoals Trojan.Cryzip en Trojan.Archiveus. Rond 2011 begon ransomware wereldwijd uit te breiden dankzij anonieme betalingsdiensten. In 2013 werd CryptoLocker gelanceerd, een beruchte ransomware die complexe encryptie gebruikte en grote sommen losgeld eiste. Dit leidde tot een explosieve groei in ransomware-aanvallen en verfijnde technieken. Tegen 2016 bereikte ransomware een piek, waarbij het zich richtte op meerdere platformen, waaron-

der Linux en MacOS, en geavanceerdere strategieën gebruikte om detectie te vermijden en meer schade aan te richten. Een belangrijk aspect van deze evolutie was de introductie van Bitcoin als betaalmethode voor losgeld. De anonimiteit van Bitcoin-transacties maakte het moeilijker voor autoriteiten om aanvallers te traceren, wat bijdroeg aan de populariteit van ransomware. Bitcoin werd snel de standaard valuta voor losgeldbetalingen, wat leidde tot een verdere toename van ransomware-aanvallen. De inzet van cryptocurrencies zoals Bitcoin blijft een cruciaal onderdeel in de succesvolle verspreiding van moderne ransomware (Richardson & North, 2017).

Impact van ransomware op organisaties

Ransomware-aanvallen hebben een aanzienlijke impact op organisaties. Ten eerste is er de financiële schade, die kan oplopen door gegevensverlies, dure herstelprocessen en de mogelijke betaling van losgeld. Naast directe kosten kunnen bedrijven ook te maken krijgen met verloren klantenvertrouwen en juridische gevolgen, wat de financiële impact verder vergroot. Ten tweede zorgen ransomware-aanvallen voor operationele verstoringen: systemen worden vaak volledig vergrendeld, wat leidt tot stilstand van cruciale bedrijfsprocessen en verlies van productieve tijd. Deze verstoringen kunnen ernstige gevolgen hebben, vooral in sectoren waar tijdige toegang tot gegevens essentieel is. Tot slot kunnen dergelijke aanvallen aanzienlijke gevolgen hebben voor de reputatie van een organisatie. Een aanval kan publieke bezorgdheid en wantrouwen opwekken, vooral als gevoelige klantinformatie wordt gelekt (Connolly & Borrion, 2020).

2.0.4. Ransomware-resistente back-upoplossingen

Immutable storage

Immutable storage is een techniek waarbij opgeslagen gegevens na het opslaan niet kunnen worden gewijzigd of verwijderd gedurende een vooraf vastgelegde periode. Dit zorgt voor een sterke bescherming tegen ransomware-aanvallen omdat de opgeslagen data niet meer kan worden aangepast (Wahl, 2023). Het concept van immutable storage komt vooral van pas bij organisaties die te maken hebben met zeer gevoelige gegevens en die moeten kunnen garanderen dat hun data altijd veilig en betrouwbaar blijft. Één van de grootste uitdagingen is opslagcapaciteit. In een immutable opslagomgeving blijven gegevens permanent behouden, zelfs als ze verouderd of onnodig zijn. Dit zorg ervoor dat er meer opslagruimte nodig is en dit verhoogt de kosten. Een tweede nadeel heeft te maken met data throughput. Data throughput is de snelheid waarmee data kan worden overgedragen of verwerkt binnen een bepaald tijdsperiode (Miao e.a., 2016). Immutable opslag kan trager zijn bij het schrijven van gegevens omdat de immutability extra processen vereist om ervoor te zorgen dat data niet kan worden aangepast. Dit kan de snelheid van gegevensoverdracht vertragen, vooral bij systemen die software-gebaseerde immutability gebruiken, waar een extra laag van computationele con-

trole nodig is. Ten derde zorgt het implementeren van immutable storage vaak voor een verhoogde management overhead. Hoe meer opgeslagen data er is, hoe complexer het is om dit te beheren. Administrators moeten hierdoor meer tijd en middelen besteden aan het onderhouden van een efficiënt en veilig opslagbeheer. Ten vierde kan beveiliging ook een aandachtspunt zijn in het geval dat de er met fysieke opslagapparaten gewerkt wordt. Bij software-gebaseerde immutability kan er sprake zijn van gevaar indien het hele besturingssysteem is aangevallen. Ten slotte kunnen de kosten snel oplopen. De initiële investering in immutable opslag kan hoog zijn, vooral als er gekozen wordt voor dure opslagmedia of gespecialiseerde hardware. Naarmate de hoeveelheid gegevens toeneemt, nemen ook de kosten voor opslag en onderhoud toe (Hasan e.a., 2005).

Air-gapped storage

Air-gapped back-ups bieden sterke bescherming tegen ransomware door back-ups fysiek of virtueel te isoleren van het netwerk. Dit betekent dat, zelfs als het netwerk wordt aangevallen, de back-ups veilig blijven omdat ze niet verbonden zijn met de geïnfecteerde systemen. Deze back-ups worden vaak opgeslagen op externe media zoals harde schijven (Bryant, 2015). Air-gapping zorgt ervoor dat het onmogelijk is voor ransomware om de back-ups te infecteren, waardoor een bedrijf snel kan herstellen van een aanval en de bedrijfscontinuïteit kan behouden. Het maakt bedrijven minder afhankelijk van cloud-opslag en netwerkverbindingen, wat de risico's vermindert. Hoewel air-gapped back-ups een goede bescherming bieden tegen ransomware, kunnen ze minder snel toegankelijk zijn wanneer gegevensherstel nodig is. Deze back-ups moeten namelijk fysiek worden opgehaald en aangesloten, wat veel tijd kan kosten. Desondanks bieden air-gapped back-ups een extra laag van beveiliging die van groot belang is voor organisaties die gevoelig zijn voor ransomware-aanvallen (Park e.a., 2023).

Offline back-ups

Offline back-ups worden opgeslagen op externe media zoals harde schijven die na het back-uppen van het netwerk worden losgekoppeld(Edwards, 2022). Dit maakt ze immuun voor online bedreigingen zoals ransomware, in tegenstelling tot on-premise back-ups die meestal verbonden blijven met het netwerk. Het grootste voordeel van offline back-ups is de extra beveiliging tegen cyberaanvallen, aangezien ze fysiek losgekoppeld zijn en daardoor buiten bereik van hackers blijven. Dit biedt bedrijven met gevoelige gegevens, zoals advocatenkantoren, een betrouwbare manier om data te beschermen tegen digitale bedreigingen. Een ander voordeel is de fysieke controle over de opslaglocatie, waardoor bedrijven precies kunnen bepalen wie toegang heeft tot de gegevens. Toch hebben offline back-ups ook nadelen: ze moeten handmatig worden bijgewerkt, wat tijdrovend is, en zijn kwetsbaar voor fysieke schade zoals brand of diefstal. Daarnaast kan het herstelproces langer duren, omdat de gegevens fysiek aangesloten en overgezet moeten

worden, wat minder efficiënt is voor bedrijven die snel dataherstel nodig hebben (James, 2019).

2.0.5. Technologische basis voor de Proof-of-Concept

Voor de Proof-of-Concept wordt gebruik gemaakt van verschillende technologische tools en platforms. Deze worden ingezet om de geplande back-upstrategie en de beveiligingsmaatregelen te testen en te optimaliseren. Hierbij wordt specifiek gewerkt met tools zoals Azure, VirtualBox en Vagrant. Deze technologieën worden gekozen vanwege hun flexibiliteit, schaalbaarheid en ondersteuning bij het simuleren van realistische scenario's.

Azure

Azure wordt gezien als het openbare cloudplatform van Microsoft en maakt gebruik van virtualisatietechnologie (Ekuan e.a., 2023). Door middel van virtualisatietechnologieën, ook wel hypervisors genoemd (Een hypervisor is software waarmee meerdere virtuele machines (VM's), elk met hun eigen besturingssysteem (OS), op één fysieke server kunnen draaien (Susnjara & Smalley, 2024).), is het mogelijk voor Azure om hardware na te bootsen in software. Dit gebeurt in datacenters die zijn opgebouwd uit serverrekken met onder andere netwerkswitches en voldoende stroomvoorzieningen. Binnen een Azure-datacenter bevinden zich serverrekken, die elk uit meerdere serverblades bestaan. Deze serverrekken bevatten ook netwerkhardware, zoals netwerkswitches, en een PDU (Power Distribution Unit), die stroomvoorziening biedt. Voor extra schaalbaarheid en efficiëntie worden deze serverrekken vaak gegroepeerd in clusters. Servers met speciale software, zoals infrastructuurcontrollers, zorgen ervoor dat services efficiënt worden toegewezen en storingen worden opgelost. Azure is meer dan alleen een verzameling servers. Het is een complex netwerk van toepassingen die samenwerken om gevirtualiseerde hardware en software te configureren en beheren. Dit maakt Azure een krachtig en flexibel platform voor gebruikers.

Azure Blob Storage is de objectopslagoplossing van Microsoft voor de cloud, geoptimaliseerd voor het opslaan van grote hoeveelheden ongestructureerde data (Dubey e.a., 2023). Azure Blob Storage biedt immutable storage in een WORM-status (Write Once, Read Many), waarmee data niet kan worden aangepast of verwijderd gedurende een ingestelde periode. Dit is ideaal voor sectoren met strenge nalevingsvereisten, zoals financiën en gezondheidszorg. Er zijn twee immutability policies beschikbaar:

- **Tijdgebonden retentiebeleid:** Data blijft gedurende een specifieke periode onveranderlijk. Na afloop kunnen bestanden worden verwijderd, maar niet overschreven. Dit beleid kan op account-, container- of versieniveau worden toegepast en kan van "unlocked" naar "gelocked" worden gezet voor naleving van regelgeving. Eenmaal gelocked, kan de retentieperiode alleen worden

verlengd.

- **Legal holds:** Houdt data onveranderlijk tot de hold expliciet wordt opgeheven. Dit is nuttig bij onbepaalde bewaartermijnen, zoals juridische onderzoeken, en kan worden toegepast op container- of blobversieniveau (Estabrook e.a., 2024).

Azure ondersteunt immutability op twee vb niveaus: container-level, waarbij alle blobs in een container hetzelfde beleid volgen, en version-level, dat flexibiliteit biedt voor individuele blobs met verschillende retentievereisten. Een blob (Binary Large Object) is een type dataopslag dat gebruikt wordt om grote hoeveelheden ongestructureerde gegevens op te slaan, zoals tekst, afbeeldingen, video's, audio of binaire bestanden (Kemp, 2007). Samen zorgen deze opties voor veilige en conforme opslag.

Vagrant

Vagrant is een open-source tool ontwikkeld door HashiCorp die het proces van het beheren en configureren van virtuele machines automatiseert (Hashicorp, z.d.). HashiCorp is een bedrijf dat tools maakt voor infrastructuurbeheer.

Het zorgt ervoor dat gebruikers virtuele machines snel kunnen creëren en configureren door gebruik te maken van gestandaardiseerde configuratiebestanden, genaamd Vagrantfiles. In de Vagrantfiles kun je allerlei configuraties kiezen zoals netwerkconfiguraties, besturingssystemen en softwarepakketten. Het biedt ondersteuning voor verschillende virtualisatieplatforms, zoals VirtualBox, VMware en Hyper-V, en kan worden geïntegreerd met provisioning-tools zoals Ansible. Vagrant wordt vaak gebruikt voor het opzetten van test- en ontwikkelomgevingen.

Virtualbox

VirtualBox is een open-source virtualisatiesoftware die ervoor zorgt dat gebruikers meerdere besturingssystemen tegelijkertijd op één fysieke machine kunnen draaien (Oracle, 2024). Virtualbox biedt veel functionaliteiten aan, waaronder ondersteuning voor diverse gastbesturingssystemen zoals Windows en Linux, daarnaast zijn de netwerkconfiguraties ook geavanceerd. VirtualBox maakt gebruik van virtuele netwerken, zoals NAT (Network Address Translation) en interne netwerken, waarmee gebruikers flexibele en gescheiden infrastructuren kunnen opzetten. Dankzij de grafische interface en command-line tools is het een toegankelijk platform voor zowel beginners als gevorderde IT-professionals. Daarbij is VirtualBox geschikt voor allerlei doelen zoals softwareontwikkeling, systeembeheer en educatieve simulaties voor scholen.

3

Methodologie

Het onderzoek begint met een uitgebreide literatuurstudie over back-upstrategieën, ransomware-resistente opslag, en immutable storage. Hierbij wordt een overzicht gegeven van de state of the art, waarbij de nieuwste technieken en strategieën voor databeveiliging in kaart worden gebracht. Deze literatuurstudie biedt de fundamentele kennis die nodig is om het bestaande back-upplan te analyseren en geeft een goed beeld van hoe organisaties effectief hun back-upsystemen kunnen beveiligen. In de tweede fase zal de huidige back-upstrategie van Forvis Mazars worden geanalyseerd en verbeterd. Momenteel wordt er elke dag één volledige back-up door Azure automatisch uitgevoerd, wat zorgt voor een basisbeveiliging. Naast de automatische back-ups beschikt Forvis Mazars ook over een script dat manuele back-ups uitvoert, maar deze worden niet frequent genoeg gedaan en missen een geautomatiseerde structuur. Door de bestaande methode te optimaliseren, wordt zowel de veiligheid als de efficiëntie van het back-upproces verhoogd.

3.0.1. Requirements-analyse

1. Must Have (Essentiële vereisten)

Deze vereisten zijn cruciaal voor de verbetering van de back-upstrategie en moeten absoluut worden geïmplementeerd om een werkbare en veilige oplossing te garanderen:

- **Automatisering van de manuele back-ups:** De huidige manuele back-ups moeten worden geautomatiseerd om de frequentie van back-ups te verhogen en de afhankelijkheid van menselijke interventie te verminderen. De automatische back-up moet dagelijks worden uitgevoerd en volledig geïntegreerd zijn in de bestaande Azure-omgeving van Forvis Mazars.
- **Beveiliging tegen ransomware:** De nieuwe back-upstrategie moet ransomware-resistent zijn, wat betekent dat back-ups moeten worden beschermd tegen

externe aanvallen die de back-ups zelf kunnen infecteren. Dit vereist de implementatie van technieken zoals *immutable storage*, zodat back-ups niet gewijzigd of verwijderd kunnen worden tijdens een ransomware-aanval.

- **Regelmatige en betrouwbare volledige back-ups:** Er moet gezorgd worden voor een betrouwbare en regelmatige uitvoering van volledige back-ups van de databases om te garanderen dat bij een systeemfout of cyberaanval altijd een up-to-date herstelpunt beschikbaar is.
- **Herstelcapaciteit (Restore from backup):** Het herstelproces moet efficiënt en snel kunnen worden uitgevoerd vanuit de back-ups. De back-upstrategie moet testen hoe snel en betrouwbaar de systemen kunnen worden hersteld in geval van dataverlies.

2. Should Have (Aanbevolen vereisten)

Deze vereisten dragen bij aan de effectiviteit van de back-upstrategie, maar zijn niet strikt noodzakelijk voor de eerste versie van de oplossing:

- **Differentiële en incrementele back-ups:** Hoewel volledige back-ups cruciaal zijn, moeten incrementele en/of differentiële back-ups overwogen worden om de belasting op de opslagcapaciteit en netwerkinfrastructuur te verminderen. Dit kan bijdragen aan de optimalisatie van de back-upstrategie door slechts gewijzigde gegevens te back-uppen in plaats van de volledige dataset.
- **Documentatie:** Er moet gedetailleerde documentatie beschikbaar zijn over het back-upproces, de gebruikte technieken, en de herstelprocedures.

3. Could Have (Wenselijke vereisten)

Deze vereisten kunnen de back-upstrategie verder verbeteren, maar kunnen in eerste instantie worden uitgesteld als er beperkingen zijn in tijd of middelen:

- **Versiebeheer van back-ups:** Het invoeren van versiebeheer voor back-ups maakt het mogelijk om verschillende versies van data op te slaan. Dit kan nuttig zijn voor het herstellen van data naar een specifieke eerdere versie (bijvoorbeeld na een fout die niet meteen werd opgemerkt).
- **Geautomatiseerd herstelproces:** Een geautomatiseerd herstelproces kan worden ontwikkeld, zodat de systemen automatisch kunnen worden hersteld in geval van dataverlies, wat de downtime minimaliseert.

4. Won’t Have (Niet noodzakelijke vereisten)

Deze vereisten worden niet opgenomen in de huidige verbeteringsronde van de back-upstrategie vanwege beperkingen in tijd, middelen, of prioriteit:

- **Complexe multi-cloud back-upoplossingen:** Hoewel multi-cloud back-upstrategieën voordelen kunnen bieden, is het implementeren van een complexe multi-cloud-oplossing voor Forvis Mazars op dit moment niet noodzakelijk, aangezien Azure al gebruikt wordt voor back-ups en de primaire focus ligt op het verbeteren van de huidige strategie binnen de Azure-omgeving.
- **Fysieke back-ups op externe schijven:** Aangezien Forvis Mazars gebruik maakt van een cloud-gebaseerde infrastructuur voor de back-ups, is het niet noodzakelijk om fysieke externe schijven of on-premise hardware-oplossingen in te zetten voor back-updoeleinden. Dit zou alleen meer complexiteit en kosten met zich meebrengen zonder aanzienlijke voordelen.

Conclusie

Deze requirementsanalyse geeft de noodzakelijke vereisten voor de verbetering van de back-upstrategie van Forvis Mazars weer, met een focus op beveiliging tegen ransomware, automatisering van de back-ups, en het herstelproces. Door de integratie van automatisering, immutable storage en verbeterde back-uptechnieken zal Forvis Mazars in staat zijn om zowel de veiligheid als de efficiëntie van hun gegevensbeheer te verhogen. Verdere verbeteringen, zoals incrementele back-ups en cloud-integratie, kunnen op een later moment worden geïmplementeerd, afhankelijk van de beschikbare middelen en de prioriteiten van het bedrijf.

3.0.2. Proof-Of-Concept

In de Proof-of-Concept zal er een virtuele omgeving opgezet worden in VirtualBox met immutable opslag. Binnen deze omgeving wordt een extra harde schijf geconfigureerd die als back-upschijf dient, met als doel aan te tonen hoe het implementeren van immutable storage kan helpen tegen ransomware-aanvallen. De PoC begint met het aanmaken van een nieuwe virtuele harde schijf in VirtualBox die enkel voor het opslaan van back-updata gebruikt zal worden. Deze schijf zal worden toegevoegd als tweede schijf aan de virtuele machine, zodat er een gescheiden opslagruimte voor back-ups beschikbaar is. Nadien wordt deze schijf van de virtuele machine ingesteld als een “read-only” schijf, zodat wijzigingen beperkt worden en data effectief beschermd is tegen ongewenste aanpassingen of verwijdering, dit simuleert immutable storage. Na het configureren van de read-only schijf, zal de back-updata opgeslagen worden op deze schijf. De back-updata blijft toegankelijk voor het systeem maar kan niet worden aangepast zonder speciale rechten, wat een basisniveau van immutabiliteit simuleert. In de ransomware-simulatiefase zal een testaanval worden uitgevoerd waarin bestanden op de primaire schijf worden versleuteld of verwijderd om het effect van een ransomware-aanval na te bootsen. Omdat de back-upschijf read-only is, zullen de bestanden op deze schijf intact blijven en ongewijzigd, wat de waarde van immutable storage aantoont voor herstel na een ransomware-aanval. Deze methode biedt een praktische Proof-of-Concept

waarmee kan worden aangetoond hoe immutable storage kan bijdragen aan de beveiliging en integriteit van back-ups in een organisatieomgeving.

4

Analyse van de back-upstrategie van Forvis Mazars

analyse analyse analyse

5

Proof-of-concept

Voor het praktische deel van deze bachelorproef werden er drie virtuele machines opgezet binnen VirtualBox met behulp van Vagrant om een gecontroleerde testomgeving te creëren. Deze virtuele machines (VM's) simuleren een scenario waarin een ransomware-aanval gericht wordt op databases die door het bedrijf worden beheerd. Het primaire doel van deze simulatie is aan te tonen dat het gebruik van immutable storage een effectieve maatregel kan zijn om belangrijke data te beschermen tegen ransomware-aanvallen.

Voor het opzetten van de virtuele machines in de Proof-of-Concept (PoC) werd gebruik gemaakt van een Vagrantfile. De Vagrantfile definieert de specificaties en configuraties van de VM's, zoals geheugen, CPU, netwerkadapters en besturingssysteem.

Listing 5.1: Vagrantfile voor drie VM's: Backup Server, Client, en Attacker

```
Vagrant.configure("2") do |config|

# Define the first VM - Primary
config.vm.define "primary" do |primary|
primary.vm.box = "ubuntu/jammy64"

# Network configuration
primary.vm.network "private_network", ip: "192.168.0.10", virtualbox__intnet: "
    internal_network"

# Hardware resources
primary.vm.provider "virtualbox" do |vb|
vb.memory = "2048" # 2GB RAM
vb.cpus = 1        # 1 CPU
end
end

# Define the second VM - Backup
```

```
18 config.vm.define "backup" do |backup|
19 backup.vm.box = "ubuntu/jammy64"
20
21 # Network configuration
22 backup.vm.network "private_network", ip: "192.168.0.20", virtualbox__intnet: "
       internal_network"
23
24 # Hardware resources
25 backup.vm.provider "virtualbox" do |vb|
26 vb.memory = "2048" # 2GB RAM
27 vb.cpus = 1        # 1 CPU
28 end
29 end
30
31 # Define the third VM - Attacker VM
32 config.vm.define "attacker" do |additional|
33 additional.vm.box = "ubuntu/jammy64"
34
35 # Network configuration
36 additional.vm.network "private_network", ip: "192.168.0.30", virtualbox__intnet: "
       internal_network"
37
38 # Hardware resources
39 additional.vm.provider "virtualbox" do |vb|
40 vb.memory = "1024" # 1GB RAM
41 vb.cpus = 1        # 1 CPU
42 end
43 end
44
45 end
```

In de onderstaande tabel worden de specificaties van de drie virtuele machines weergegeven die in de Proof of Concept zijn gebruikt. Elke VM heeft een specifieke functie binnen de gesimuleerde omgeving. De tabel bevat details over de hoeveelheid toegewezen RAM, het aantal CPU-cores, het gebruikte besturingssysteem, de toegewezen IP-adressen en de configuratie van de netwerkadapter. Deze configuratie zorgt ervoor dat de VM's binnen hetzelfde interne netwerk met elkaar kunnen communiceren, wat essentieel is voor het testen van de ransomware-aanval en de back-upstrategieën.

Functie	RAM	CPU Cores	IP	Besturingssysteem	Netwerkadapter
Primary server	2 GB	1	192.168.0.10	Ubuntu 22.04.5 LTS	Private Network
Back-up server	1 GB	1	192.168.0.20	Ubuntu 22.04.5 LTS	Private Network
Attacker VM	2 GB	1	192.168.0.30	Ubuntu 22.04.5 LTS	Private Network

6

Conclusie

Curabitur nunc magna, posuere eget, venenatis eu, vehicula ac, velit. Aenean ornare, massa a accumsan pulvinar, quam lorem laoreet purus, eu sodales magna risus molestie lorem. Nunc erat velit, hendrerit quis, malesuada ut, aliquam vitae, wisi. Sed posuere. Suspendisse ipsum arcu, scelerisque nec, aliquam eu, molestie tincidunt, justo. Phasellus iaculis. Sed posuere lorem non ipsum. Pellentesque dapibus. Suspendisse quam libero, laoreet a, tincidunt eget, consequat at, est. Nullam ut lectus non enim consequat facilisis. Mauris leo. Quisque pede ligula, auctor vel, pellentesque vel, posuere id, turpis. Cras ipsum sem, cursus et, facilisis ut, tempus euismod, quam. Suspendisse tristique dolor eu orci. Mauris mattis. Aenean semper. Vivamus tortor magna, facilisis id, varius mattis, hendrerit in, justo. Integer purus.

Vivamus adipiscing. Curabitur imperdiet tempus turpis. Vivamus sapien dolor, congue venenatis, euismod eget, porta rhoncus, magna. Proin condimentum pretium enim. Fusce fringilla, libero et venenatis facilisis, eros enim cursus arcu, vitae facilisis odio augue vitae orci. Aliquam varius nibh ut odio. Sed condimentum condimentum nunc. Pellentesque eget massa. Pellentesque quis mauris. Donec ut ligula ac pede pulvinar lobortis. Pellentesque euismod. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent elit. Ut laoreet ornare est. Phasellus gravida vulputate nulla. Donec sit amet arcu ut sem tempor malesuada. Praesent hendrerit augue in urna. Proin enim ante, ornare vel, consequat ut, blandit in, justo. Donec felis elit, dignissim sed, sagittis ut, ullamcorper a, nulla. Aenean pharetra vulputate odio.

Quisque enim. Proin velit neque, tristique eu, eleifend eget, vestibulum nec, lacus. Vivamus odio. Duis odio urna, vehicula in, elementum aliquam, aliquet laoreet, tellus. Sed velit. Sed vel mi ac elit aliquet interdum. Etiam sapien neque, convallis et, aliquet vel, auctor non, arcu. Aliquam suscipit aliquam lectus. Proin tincidunt magna sed wisi. Integer blandit lacus ut lorem. Sed luctus justo sed enim.

Morbi malesuada hendrerit dui. Nunc mauris leo, dapibus sit amet, vestibulum et, commodo id, est. Pellentesque purus. Pellentesque tristique, nunc ac pulvinar adipiscing, justo eros consequat lectus, sit amet posuere lectus neque vel augue. Cras consectetuer libero ac eros. Ut eget massa. Fusce sit amet enim eleifend sem dictum auctor. In eget risus luctus wisi convallis pulvinar. Vivamus sapien risus, tempor in, viverra in, aliquet pellentesque, eros. Aliquam euismod libero a sem.

Nunc velit augue, scelerisque dignissim, lobortis et, aliquam in, risus. In eu eros. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Curabitur vulputate elit viverra augue. Mauris fringilla, tortor sit amet malesuada mollis, sapien mi dapibus odio, ac imperdiet ligula enim eget nisl. Quisque vitae pede a pede aliquet suscipit. Phasellus tellus pede, viverra vestibulum, gravida id, laoreet in, justo. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Integer commodo luctus lectus. Mauris justo. Duis varius eros. Sed quam. Cras lacus eros, rutrum eget, varius quis, convallis iaculis, velit. Mauris imperdiet, metus at tristique venenatis, purus neque pellentesque mauris, a ultrices elit lacus nec tortor. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent malesuada. Nam lacus lectus, auctor sit amet, malesuada vel, elementum eget, metus. Duis neque pede, facilisis eget, egestas elementum, nonummy id, neque.

A

Onderzoeksvoorstel

Het onderwerp van deze bachelorproef is gebaseerd op een onderzoeksvoorstel dat vooraf werd beoordeeld door de promotor. Dat voorstel is opgenomen in deze bijlage.

Bibliografie

Beard, B. (2018). *Full Backups*. Apress. https://doi.org/https://doi.org/10.1007/978-1-4842-3456-3_1

Bryant, W. D. (2015, juli 30). *International Conflict and Cyberspace Superiority*. https://books.google.be/books?id=LJ9GCgAAQBAJ&q=%22air+gapped%22&pg=PA107&redir_esc=y#v=onepage&q&f=false

Chervenak, A., Vellanki, V., & Kurmas, Z. (1998). Protecting file systems: A survey of backup techniques. *Joint NASA and IEEE Mass Storage Conference*, *99*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4b6cfd832c2eb61c60ae0ab956e

Connolly, L. Y., & Borrion, H. (2020). Your Money or Your Business: Decision-Making Processes in Ransomware Attacks. https://d1wqtxts1xzle7.cloudfront.net/104646029/Your_Money_or_Your_Business_Decision_Making_Processes_in_Ransomware_Attacks-libre.pdf?1690795001=&response-content-disposition=inline;+filename=Your_Money_or_Your_Business_Decision_Mak.pdf&Expires=1731789975&Signature=YLxZbqlgtDwAm--EU~t5uAQ3~VmDs9cRO8prg89csdzkaXV8wEnTV
eBdnb6gGwai8CItmLBefCrX45mtgS5fAxytyORihxMZgpGo7SzaiiHpjN8GMMHQfp12mdwAa
_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Dubey, A., Jewell, P., Estabrook, N., Haas, S., Myers, T., Martin, J., Callison, D., Fernández, J. Á., Coulter, D., Lee, D., Rabeler, C., Anderson, B., Fowler, C., Kohli, A., Hopkins, M., Sharkey, K., Kumar, R., Irwin, J., Shahan, R., & Pratt, T. (2023). Introduction to Azure Blob Storage. *Microsoft*. https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

Edwards, B. (2022). Why You Need an Offline Backup. *How-To Geek*. https://www.howtogeek.com/818193/why-you-need-an-offline-backup/

Ekuan, M., Buck, A., Zimmergren, T., Moore, G., Parker, D., & Coulter, D. (2023). Hoe werkt Azure? *Microsoft*. https://learn.microsoft.com/nl-nl/azure/cloud-adoption-framework/get-started/what-is-azure

Estabrook, N., Nottingham, C., Pavan, P., Singh, A., Martin, J., Yoshioka, H., & Myers, T. (2024). Store business-critical blob data with immutable storage in a write once, read many (WORM) state. *Microsoft*. https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview

Ghazi, K., & H. O. Nasereddin, H. (2013). Business Continuity Based on Backup. *American Academic Scholarly Research Journal*, *5*, 253–258. https://www.aasrc.org/aasrj/index.php/aasrj/article/viewFile/1385/547

Hasan, R., Stanton, P., Yurcik, W., Brumbaugh, L., Rosendale, J., & Boonstra, R. (2005). The Techniques and Challenges of Immutable Storage with applications in Multimedia. *National Center for Supercomputing Applications*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=578ff4957d4fa2e550ec2a819b6500820d72

Hashicorp. (z.d.). *What is Vagrant?* Verkregen december 10, 2024, van https://developer.hashicorp.com/vagrant

James. (2019). Offline backups in an online world. *National Cyber Security Centre*. https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

Kemp, K. (2007, december 26). *Encyclopedia of Geographic Information Science*. https://www.google.be/books/edition/Encyclopedia_of_Geographic_Information_S/FrUQHIzXK6EC?hl=nl&gbpv=0

Miao, G., Zander, J., Sung, K. W., & Slimane, S. B. (2016, maart 3). *Fundamentals of Mobile Data Networks*. https://books.google.be/books?id=ImeSCwAAQBAJ&printsec=frontcover&source=gbs_atb&redir_esc=y#v=onepage&q&f=false

Nelson, S., & Brown, R. (2011, februari 23). *Pro Data Backup and Recovery*. https://www.google.be/books/edition/Pro_Data_Backup_and_Recovery/0lfehRoBOPkC?hl=nl&gbpv=0

Obrutsky, S. (2016). Cloud storage: Advantages, disadvantages and enterprise solutions for business. *Conference: EIT New Zealand*. https://www.researchgate.net/profile/Santiago-Obrutsky/publication/305508410_Cloud_Storage_Advantages_Disadvantages_and_Enterprise_Solutions_for_Business/links/5792976508ae33e89f7cc136/Cloud-Storage-Advantages-Disadvantages-and-Enterprise-Solutions-for-Business.pdf

Oracle. (2024, november 1). *User Guide for Release 7.1*. Verkregen december 11, 2024, van https://docs.oracle.com/en/virtualization/virtualbox/7.1/user/preface.html

Park, J., Yoo, J., Yu, J., Lee, J., & Song, J. (2023). A Survey on Air-Gap Attacks: Fundamentals, Transport Means, Attack Scenarios and Challenges. *Sensors*, *23*(6), 3215. https://doi.org/https://doi.org/10.3390/s23063215

Rahumed, A., Chen, H. C. H., Tang, Y., Lee, P. P. C., & Lui, J. C. S. (2011). A secure cloud backup system with assured deletion and version control. *40th International Conference on Parallel Processing Workshops*, 160–167. https://www.researchgate.net/publication/221617563_A_Secure_Cloud_Backup_System_with_Assured_Deletion_and_Version_Control

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs

Rivas, K. (2022). What's the Diff: Full, Incremental, Differential, and Synthetic Full Backups. *Backblaze*. https://www.backblaze.com/blog/whats-the-diff-full-incremental-differential-and-synthetic-full-backups/

Susnjara, S., & Smalley, I. (2024). What are hypervisors? *IBM*. https://www.ibm.com/topics/hypervisors

Trovato, F., Sharp, A., & Siman, T. (2019). Cloud, co-location, on-premises and hybrid disaster recovery solutions: Pros, cons, and a cost comparison. *Journal of Business Continuity & Emergency Planning*, *13*(2), 120–135. https://www.ingentaconnect.com/content/hsp/jbcep/2019/00000013/00000002/art00004

Wahl, C. (2023). Recovering Fast from Ransomware Attacks: The Magic of an ImmutableBackup Architecture. *Rubrik*. https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf?ref=thestack.technology

Yanfang, Y., Tao, L., Donald, A., & Sitharama, I. (2017). A survey on malware detection using data mining techniques. *ACM Computing Surveys (CSUR)*, *50*(3), 1–40. https://dl.acm.org/doi/pdf/10.1145/3073559

Zhao, X., Bu, Y., Pang, W., & Cai, J. (2024). Periodic and random incremental backup policies in reliability theory. *Software Quality Journal*, *32*(3), 1325–1340. https://doi.org/https://doi.org/10.1007/s11219-024-09685-1

Zhu, W.-D., Allenbach, G., Battaglia, R., Boudreaux, J., Harnick-Shapiro, D., Kim, H., Kreuch, B., Morgan, T., Patel, S., & Willingham, M. (2015, april 13). *Disaster Recovery and Backup Solutions for IBM FileNet P8 Version 4.5.1 Systems*. IBM Redbooks. https://books.google.be/books?id=O1TAAgAAQBAJ