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 aardbevingen. 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

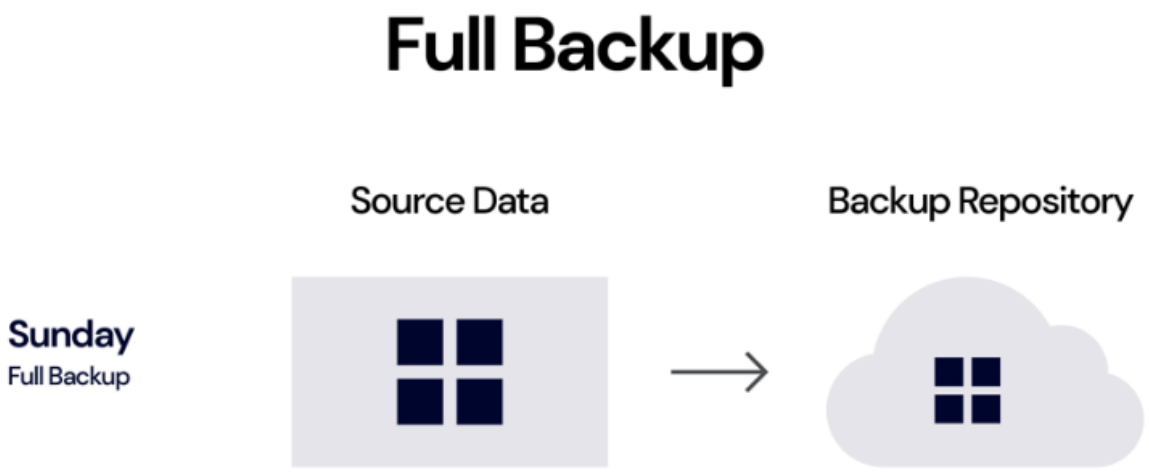
van zaken zo snel mogelijk te herstellen. Back-ups spelen een belangrijke rol voor de continuïteit van een bedrijf en zijn vaak de eerste stap bij het opstellen van een disaster recovery plan (DRP). Bij een optimale situatie is er na een incident geen data verloren en is alle data relatief snel terug 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 van datamanagement en databeveiliging 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 deze back-up volledig worden hersteld op een nieuwe schijf. Daarnaast kunnen

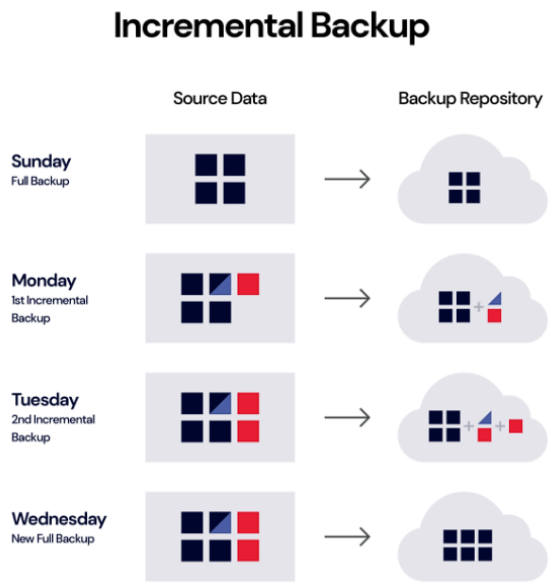


Figuur 2.1: Representatie van een full back-up (Rivas, 2022)

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

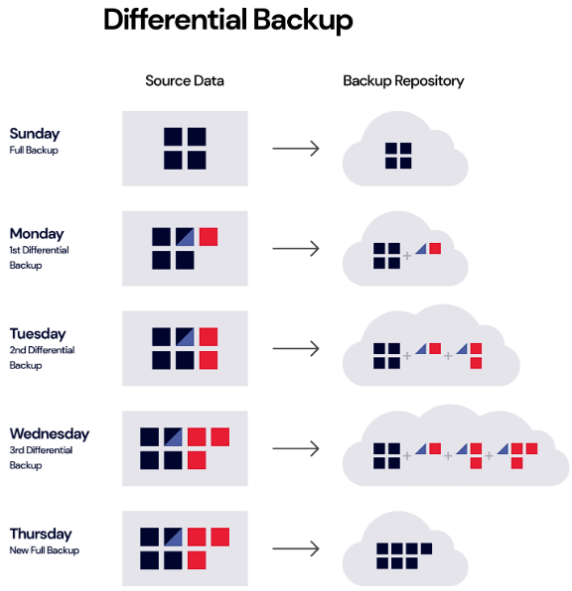


Figuur 2.2: Representatie van een incremental back-up (Rivas, 2022)

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 vol-

ledige 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 opgeslagen 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 me-

dewerkers 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 back-ups die lokaal worden opgeslagen op de fysieke servers en opslagapparaten binnen de infrastructuur van een bedrijf. Deze methode houdt in dat het bedrijf zelf verantwoordelijk is voor het beheren, beveiligen en onderhouden van de back-upomgeving. Voor organisaties die volledige controle willen over hun gegevens, bieden on-premise back-ups een direct en tastbaar voordeel: de data blijft in eigen beheer, wat vooral waardevol is in sectoren waar data

security en privacy van groot belang zijn, zoals de gezondheidszorg of financiële dienstverlening. Een van de grootste voordelen van on-premise back-ups is dat er geen afhankelijkheid is van een internetverbinding. Aangezien de back-up lokaal gebeurt, is de snelheid van het netwerk binnen het bedrijf bepalend voor de snelheid van het back-upproces. Voor een organisatie met een snelle interne netwerkinfrastructuur, zoals een mediabedrijf dat dagelijks grote videobestanden back-upt, kan dit het verschil maken tussen uren en minuten. Dit maakt on-premise back-ups een ideale keuze voor bedrijven die snel grote hoeveelheden data moeten opslaan zonder gehinderd te worden door internetbeperkingen. Daarnaast biedt on-premise opslag de mogelijkheid om de volledige back-up- en herstelstrategie te personaliseren en aan te passen aan de specifieke behoeften van de organisatie. Dit kan belangrijk zijn voor bedrijven die bepaalde compliance-eisen hebben of die willen experimenteren met specifieke back-uptechnieken, zoals differential of incremental back-ups. Een bedrijf in de financiële sector kan bijvoorbeeld ervoor kiezen om alle dagelijkse transacties lokaal op te slaan en de volledige back-ups wekelijks op een afgescheiden server te bewaren. Op deze manier kunnen zij hun data volledig beheren, met maatregelen die specifiek zijn afgestemd op hun eigen risico's en beleid. Toch komen on-premise back-ups met aanzienlijke nadelen. Een belangrijke uitdaging is de hoge initiële investering in hardware en onderhoud. Bedrijven moeten investeren in servers, harde schijven, netwerkinfrastructuur en mogelijk zelfs koeling- en beveiligingssystemen. Voor een middelgroot productiebedrijf dat bijvoorbeeld zijn back-ups op eigen servers wil opslaan, kan dit een aanzienlijke uitgave betekenen. Bovendien moeten deze systemen regelmatig worden geüpdatet en vervangen, wat extra kosten en logistieke planning met zich meebrengt. Een ander nadeel van on-premise back-ups is dat ze gevoelig zijn voor fysieke risico's zoals brand, diefstal of overstromingen. Aangezien de gegevens op locatie zijn opgeslagen, kunnen ze verloren gaan als de infrastructuur fysiek wordt beschadigd. Dit betekent dat bedrijven extra beveiligingsmaatregelen moeten nemen, zoals een secundaire back-up op een externe locatie. Stel dat een IT-bedrijf zijn servers in zijn hoofdkantoor opslaat en daar een brand uitbreekt; dan zijn zowel de primaire data als de back-up data in gevaar, tenzij er een tweede kopie offsite is opgeslagen. Dit vergroot de behoefte aan een goed doordachte noodherstelstrategie. Daarnaast vereisen on-premise back-ups specifieke IT-expertise om een goed beheerde en beveiligde omgeving te handhaven. Het interne IT-team moet in staat zijn om regelmatig back-ups uit te voeren, beveiligingsupdates bij te houden, en ervoor te zorgen dat de gegevens ten alle tijden toegankelijk en veilig zijn. Voor een kleine organisatie zonder een toegewijd IT-team kan dit een uitdaging zijn, aangezien deze taken continu onderhoud en aandacht vereisen.

Offline back-ups

Offline back-ups zijn back-ups die fysiek worden opgeslagen op opslagmedia zoals externe harde schijven, tape-drives of andere niet-aangesloten apparaten, zon-

der constante verbinding met het netwerk of internet. Het belangrijkste verschil met on-premise back-ups is dat offline back-ups na het maken ervan van het netwerk worden losgekoppeld, waardoor ze immuun worden voor online bedreigingen zoals ransomware of hacking. Bij on-premise back-ups blijven de gegevens meestal beschikbaar binnen de lokale netwerkomgeving van het bedrijf, terwijl offline back-ups juist fysiek worden verwijderd van elke vorm van netwerktoegang. Een van de grootste voordelen van offline back-ups is dat ze een extra laag bescherming bieden tegen cyberaanvallen. Doordat deze back-ups niet online toegankelijk zijn, kunnen kwaadwillenden er via het netwerk geen toegang toe krijgen. Dit kan een essentieel voordeel zijn voor bedrijven die met gevoelige gegevens werken, zoals een advocatenkantoor dat juridische documenten opslaat. Stel dat een ransomware-aanval het hele netwerk vergrendelt, dan blijven de offline back-ups onaangetast, omdat ze fysiek losgekoppeld zijn van het geïnfecteerde systeem. Op deze manier kunnen bedrijven hun gegevens nog steeds herstellen, zelfs in het geval van een grote cyberaanval. Offline back-ups bieden ook het voordeel van fysieke controle. Een bedrijf dat zijn offline back-ups in een kluis of beveiligde ruimte opslaat, heeft de zekerheid dat de gegevens veilig zijn tegen zowel digitale als sommige fysieke bedreigingen. Dit is bijvoorbeeld handig voor een onderzoeksorganisatie die vertrouwelijke onderzoeksgegevens heeft en ervoor wil zorgen dat alleen bevoegde personen toegang hebben. Door de back-ups fysiek op te slaan in een beveiligde ruimte kan worden bepaald wie wanneer bij de data kan. Echter, offline back-ups brengen ook enkele nadelen met zich mee. Een van de grootste uitdagingen is dat ze handmatig moeten worden bijgewerkt, wat arbeidsintensief kan zijn. Dit kan een probleem vormen voor bedrijven met zeer regelmatig veranderende gegevens. Neem een klein e-commercebedrijf dat elke dag nieuwe verkoopgegevens verzamelt en opslaat; om deze data te beschermen, zou dagelijks een offline back-up moeten worden gemaakt en fysiek worden opgeborgen. Dit proces kan tijdrovend zijn en vereist dat er een routine is om deze back-ups nauwgezet te beheren. Een ander nadeel van offline back-ups is dat ze kwetsbaar blijven voor fysieke schade, verlies of diefstal. Aangezien ze worden opgeslagen op fysieke media, zijn ze gevoelig voor gebeurtenissen zoals brand, waterschade of diefstal. Een mediabedrijf dat zijn videoprojecten op tapes opslaat, loopt bijvoorbeeld het risico dat al zijn gegevens verloren gaan als er brand uitbreekt in de opslagruimte. Het gebruik van een tweede offsite opslaglocatie kan hier een oplossing bieden, maar dat brengt extra kosten en logistiek met zich mee. Daarnaast is de toegang tot offline back-ups vaak minder flexibel en kan het herstelproces langer duren. Doordat de gegevens fysiek moeten worden aangesloten en overgezet naar een systeem, kan het tijd kosten om data te herstellen. Stel dat een productiebedrijf te maken krijgt met een systeemfout en de gegevens uit een offline back-up moet herstellen. Het proces kan langer duren dan bij een online back-up, omdat het opslagmedium fysiek moet worden aangesloten en de gegevens moeten worden overgezet naar het

netwerk. Dit betekent dat offline back-ups minder geschikt zijn voor bedrijven die minimale downtime nodig hebben.

Immutable storage

Immutable storage, of onveranderbare opslag, is een techniek waarbij opgeslagen gegevens na het opslaan niet kunnen worden gewijzigd of verwijderd gedurende een vooraf vastgelegde periode. Dit biedt een sterke bescherming tegen cyberaanvallen, zoals ransomware, en menselijke fouten, aangezien gegevens na het vastleggen immuun zijn voor wijzigingen. 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. Het belangrijkste voordeel van immutable storage is dat het data beschermt tegen kwaadwillende wijzigingen. Stel bijvoorbeeld dat een financiële instelling haar financiële rapporten opslaat met immutable storage. Als een ransomwareaanval probeert om de gegevens te versleutelen of te verwijderen, zal de immutable opslag de wijziging blokkeren, zodat de originele, ongewijzigde data beschikbaar blijft. Dit biedt organisaties die werken met onvervangbare gegevens een vrijwel onaantastbare zekerheid, aangezien geen enkele vorm van digitale aanval de opgeslagen gegevens kan wijzigen of verwijderen. Immutable storage is vooral effectief als back-upoplossing. Een onderneming die regelmatig back-ups maakt in een immutable storage-omgeving, kan erop rekenen dat deze back-ups intact blijven, zelfs als het hoofdnetwerk wordt aangevallen. Denk aan een ziekenhuis dat medische dossiers opslaat in een immutable omgeving. Bij een cyberaanval zou het ziekenhuis nog steeds toegang hebben tot de originele medische gegevens, omdat de back-ups in immutable storage onaangetast blijven. Dit kan van vitaal belang zijn in noodsituaties waarin de gegevens beschikbaar moeten blijven om de zorg voor patiënten te waarborgen. Naast bescherming tegen kwaadwillende aanvallen biedt immutable storage ook een betrouwbaarheidsvoordeel door menselijke fouten uit te sluiten. Als er bijvoorbeeld per ongeluk een bestand zou worden verwijderd uit de actieve opslag, dan blijft er altijd een onveranderbare kopie bestaan in de immutable storage. Dit kan een belangrijke geruststelling zijn voor een softwareontwikkelingsbedrijf dat regelmatig wijzigingen aanbrengt in de codebase en daardoor risico loopt op menselijke fouten. Immutable storage voorkomt dat deze onomkeerbare fouten de back-ups aantasten. Ondanks de voordelen zijn er echter ook nadelen verbonden aan immutable storage. Een groot nadeel is de kostenstructuur, omdat immutable opslag vaak gebruikmaakt van premium cloudopslag die speciaal is ontworpen om gegevens onveranderbaar te houden. Een mediabedrijf dat grote hoeveelheden videobestanden in immutable storage wil opslaan, kan te maken krijgen met hogere opslagkosten, omdat de cloudprovider voor deze beveiligingsfunctie extra kosten in rekening brengt. Het gebruik van immutable storage kan daarom duurder zijn dan conventionele cloudopslag, wat organisaties dwingt om zorgvuldig na te denken over welke gegevens hier worden

opgeslagen. Daarnaast kan immutable storage de flexibiliteit van gegevensbeheer beperken. Doordat de gegevens niet kunnen worden aangepast, moeten organisaties zorgvuldig bepalen welke data zij in deze omgeving opslaan en voor welke duur de data onveranderbaar moet blijven. Een IT-consultancybedrijf dat een projectdatabase opslaat in immutable storage, kan bijvoorbeeld problemen ondervinden als er fouten of verouderde data in deze database staan, aangezien het onmogelijk is om deze snel te corrigeren. Dit vereist dat bedrijven vooraf goed plannen hoe lang de onveranderbaarheid nodig is en of het gebruik van immutable storage past binnen hun datamanagementprocessen. Tot slot kan de hersteltijd bij immutable storage langer duren dan bij andere vormen van back-up. Omdat de data in immutable storage meestal in een afzonderlijke omgeving is opgeslagen en vaak niet direct toegankelijk is, kan het langer duren om deze gegevens te herstellen naar de actieve werkomgeving. Bijvoorbeeld, een productiebedrijf dat een belangrijke dataset in immutable storage heeft opgeslagen, zou mogelijk een extra stap moeten doorlopen om deze gegevens terug te halen en te gebruiken in hun primaire systeem. Dit maakt immutable storage minder geschikt voor bedrijven die onmiddellijke toegang tot back-ups nodig hebben bij downtime.

2.0.3. Ransomware

2.0.4. Ransomware-resistente back-upoplossingen

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

POCPOCPOC

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

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

Ghazi, K., & H. O. Nasereddin, H. (2013). Business Continuity Based on Backup. *American Academic Scholarly Research Journal*, *5*, 253–258.

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

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

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/

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