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

Met trots en voldoening presenteer ik deze bachelorproef, het sluitstuk van mijn opleiding Toegepaste Informatica aan de HoGent. In het begin toen ik begon met zoeken naar een onderwerp had ik geen idee waar ik moest beginnen en ik vond dit dus ook een grote uitdaging. Ik begon met het opzoeken naar bepaalde interessante onderwerpen en ik kwam uiteindelijk op dit onderwerp. Ik heb sterke interesses in cybersecurity dus ik wou dit implementeren in mijn bachelorproef. Daarbij ontwikkelde ik ook interesse in back-ups tijdens het opleidingsonderdeel Cybersecurity Advanced. Het schrijven van deze bachelorproef was niet alleen een uitdagend leerproces, maar ook een unieke kans om mijn interesse in systeembeheer en cybersecurity verder te verdiepen. Dit project heeft me niet alleen geholpen mijn technische kennis te versterken, maar ook om praktijkervaring op te doen binnen een professionele context.

Ik wil graag mijn dankbaarheid uitdrukken aan mijn co-promotor, Rémy Tetaert, voor zijn waardevolle begeleiding, expertise en tijd tijdens dit proces. Zijn inzichten, ondersteuning en begeleiding waren heel belangrijk voor mij. Daarnaast wil ik mijn promotor, Martijn Saelens, bedanken voor zijn constructieve feedback en kritische blik, die me steeds hebben geholpen om mijn werk te verbeteren.

Tot slot wil ik ook mijn familie en vrienden bedanken voor hun geduld, steun en motivatie gedurende deze periode. Zonder hen zou dit niet mogelijk zijn geweest.

Samenvatting

Dit onderzoek heeft als doel het analyseren en optimaliseren van de back-upstrategie van Forvis Mazars. Deze organisatie maakt gebruik van Azure om hun data te beheren. Momenteel heeft het bedrijf een back-upstrategie die enkel bestaat uit automatische full back-ups van de twee databases en een script dat een back-up neemt van een databank en dit opslaat naar een Azure storage account.

De data dat een bedrijf bezit is één van de belangrijkste bezittingen en het beschermen van deze data heeft een hoge prioriteit. Back-ups spelen hierbij een belangrijke rol omdat deze de bedrijfscontinuïteit bewaren in het geval van een incident. Het back-upplan van Forvis Mazars had geen immutable storage en was dus kwetsbaar tegen cyberdreigingen zoals ransomware-aanvallen.

Om de back-upstrategie van Forvis Mazars te verbeteren is er een Proof-of-Concept (PoC) ontwikkeld in een lokale testomgeving met VirtualBox. Deze PoC simuleert een ransomware-aanval waarbij de effectiviteit van ransomware-resistente technieken, zoals immutable storage, wordt getest. Immutable storage voorkomt dat back-ups kunnen worden gemanipuleerd of verwijderd, zelfs bij volledige controle door een aanvaller.

Daarbij is er een analyse gedaan op de huidige back-upstrategie van de organisatie en zijn daar verschillende aanbevelingen uit gekomen, zoals het implementeren van immutable storage in de Azure-omgeving, het uitbreiden van het retentiebeleid en het automatiseren van manuele back-ups. Dit zou ervoor zorgen dat de back-ups veiliger en betrouwbaarder zijn en daarnaast bieden deze oplossingen ook een snellere en effectievere herstelmogelijkheid.

Dit onderzoek kan als hulpmiddel gebruikt worden om ransomware-resistente back-upstrategieën binnen Azure-omgevingen op te zetten. De resultaten dragen niet alleen bij aan het verhogen van de dataveiligheid en het bewaren van de bedrijfscontinuïteit van Forvis Mazars, maar bieden ook waardevolle inzichten voor andere organisaties die hun back-upplan willen versterken.

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-up oplossingen 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?

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. 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 de proof-of-concept beschreven, waarin immutabele opslag wordt getest door een ransomware-aanval na te bootsen op een virtuele machine.

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 hardwarestoring 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 een ernstige storing. 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 or-

ganisatie 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 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

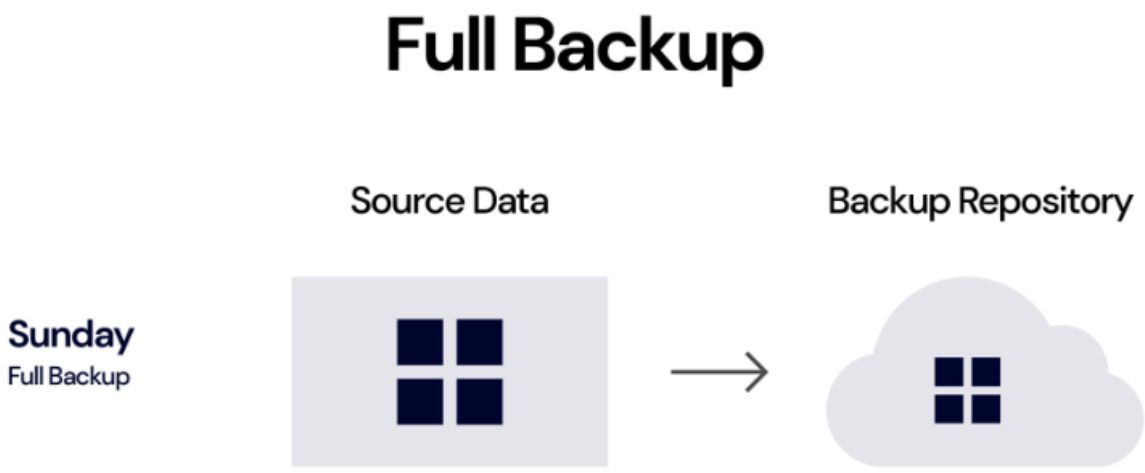
Back-ups zijn een belangrijk onderdeel voor het managen en beveiligen van data binnen organisaties. Back-ups zorgen voor de continuïteit van bedrijfssystemen in het geval van een incident zoals een cyberaanval. Back-ups zijn snapshots van gegevens die op een bepaald tijdstip zijn gemaakt, opgeslagen 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.



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

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 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.

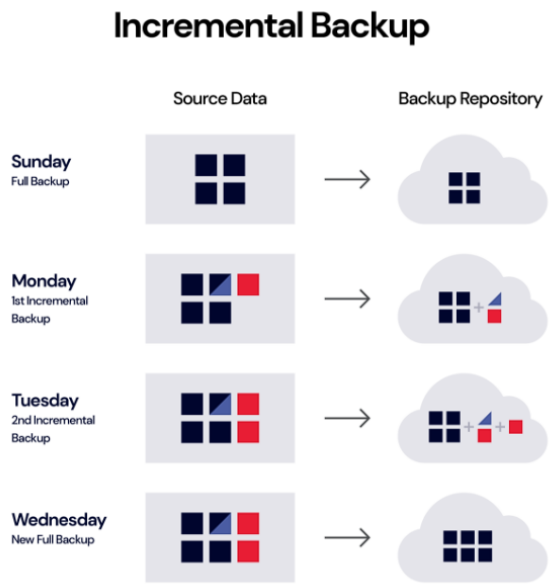
Aan de andere kant is er het probleem van opslagcapaciteit. Stel bijvoorbeeld dat een bedrijf elke nacht een full back-up maakt van zijn servers naar een opslagplaats in de cloud, waarbij per keer 500 GB aan data wordt opgeslagen. Na een week is er al 3,5 terabyte aan gegevens in de cloud opgeslagen. 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. 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 van de week zo verder, elke dag wordt enkel de nieuwe of gewijzigde data opgeslagen ten opzichte van de dag ervoor. De volgende week doet het bedrijf op maandag weer een full back-up en herhaalt het de stappen. Omdat bedrijven steeds meer data beheren, biedt deze methode een efficiënte manier om opslagkosten te beperken, vooral wanneer gebruik wordt gemaakt van een cloudservice.

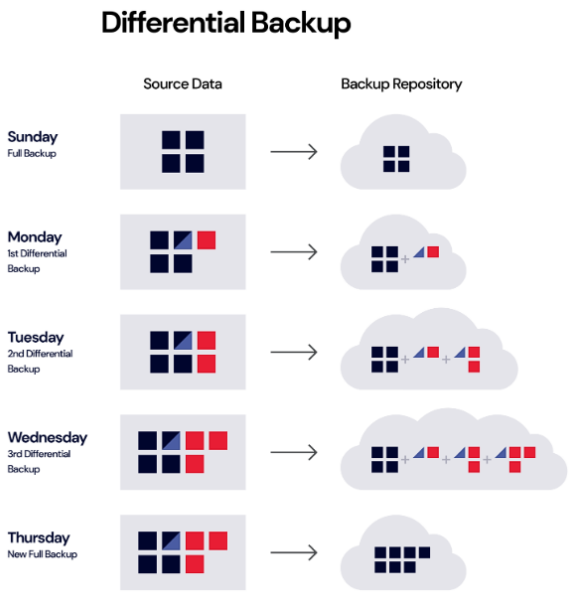
Stel dat een bedrijf dagelijks slechts 1% van zijn gegevens wijzigt; in plaats van elke dag een volledige kopie van bijvoorbeeld 1 TB te maken, slaat een incrementele back-up slechts de nieuwe 1% op, wat 990 GB aan opslagruimte per dag

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 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 back-ups 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 baseren hun prijs meestal op de hoeveelheid opslagruimte die gebruikt wordt, 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 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. Dit benadrukt het belang van goede service level agreements (SLA's) en mogelijk zelfs een hybride strategie die cloud-opslag 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 gegevens, wat vooral belangrijk is in sectoren waar veiligheid en privacy cruciaal zijn, zoals bijvoorbeeld 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.

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, totdat er losgeld wordt betaald, meestal in Bitcoin (Richardson & North, 2017). Malware is een software-programma 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.

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 constante groei zien sinds het einde van de jaren '80. In 1989 verscheen het eerste ransomwarevirus, de AIDS Trojan, die een-

voudige versleuteling gebruikte. In 2005 kwam de moderne ransomware met Trojan. 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, waaronder 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. 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.

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 controle 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 een betrouwbare ma-

nier 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).

Het verschil tussen air-gapped en offline back-ups ligt in de mate van isolatie van het netwerk. Air-gapped back-ups zijn volledig fysiek gescheiden van netwerken en kunnen niet op afstand worden benaderd, wat ze zeer veilig maakt tegen cyberaanvallen. Offline back-ups zijn ook niet constant verbonden, maar kunnen tijdelijk worden aangesloten voor het maken of herstellen van back-ups. Air-gapped back-ups bieden doorgaans een sterkere bescherming, omdat ze volledig geïsoleerd zijn van potentiële aanvallen.

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 configure-

ren 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 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.

BorgBackup

BorgBackup is een krachtige back-uptool die efficiëntie en beveiliging combineert door gebruik te maken van compressie en geverifieerde encryptie (BorgBackup, 2024).

Het maakt gebruik van deduplicatie, waarbij alleen nieuwe of gewijzigde data worden opgeslagen, dit zorgt ervoor dat er veel opslagruimte bespaart kan worden. Deze tool maakt gebruik van client-side encryptie met AES-256 en HMAC-SHA256.

Daarnaast heeft BorgBackup verschillende compressieopties zoals LZ4, Zstd en LZMA. Hierdoor kunnen gebruikers kiezen tussen snelheid en compressieniveau.

Als laatste is BorgBackup geschikt voor offsite back-ups via SSH, waardoor het ideaal is voor zowel lokale als externe back-upoplossingen.

MySQL

MySQL is een populair open-source relationeel databasesysteem gemaakt om data op te slaan en te beheren (Erickson, 2024). Het staat bekend om zijn snelheid, betrouwbaarheid en gebruiksvriendelijkheid.

MySQL wordt veel gebruikt voor het opslaan en beheren van gestructureerde data in zowel kleine toepassingen als grote, complexe systemen. MySQL ondersteunt SQL (Structured Query Language) voor het beheren van data en biedt functies zoals transacties, opslag op basis van verschillende engines en ondersteuning voor grote datasets.

Voor back-ups biedt MySQL tools zoals mysqldump, een command-line utility waarmee gebruikers eenvoudig een logische back-up (een logische back-up is een soort back-up die de tabelstructuur en gegevens reproduceert, zonder de daadwerkelijke gegevensbestanden te kopiëren (MySQL, z.d.)) kunnen maken van de structuur en data van een database naar een SQL-bestand. Dit bestand kan worden gebruikt om de database later te herstellen in geval van nood.

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. 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:

- **Regelmatige en betrouwbare automatische back-ups:** Er moet gezorgd worden voor de implementatie van een automatische back-upstrategie die dagelijks volledige back-ups van de databases uitvoert. Dit moet volledig geïntegreerd zijn in de bestaande Azure-omgeving van Forvis Mazars, zodat er altijd een up-to-date herstelpunt beschikbaar is bij systeemfouten of cyberaanvallen.
- **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.

- **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).
- **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:

- **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

De huidige back-upstrategie voor de databanken van Forvis Mazars bestaat uit twee componenten: automatische full back-ups en manuele back-ups d.m.v. een script. Hoewel dit een goede basis biedt, zijn er enkele verbeterpunten om de betrouwbaarheid, efficiëntie en veiligheid van hun back-upplan te verbeteren.

Automatisering van de manuele back-ups

De manuele back-ups worden op dit moment uitgevoerd met een script en vereisen handmatige interventie. Dit maakt het proces inefficiënt en foutgevoelig.

Aanbeveling: Automatiseer het proces met behulp van *Azure Automation* of *Logic Apps*. Met deze tools kunnen de manuele back-ups worden gepland op vaste tijdstippen, zonder menselijke tussenkomst. Dit verhoogt niet alleen de betrouwbaarheid van de back-ups, maar zorgt ook voor een consistente uitvoering.

Incrementele en Differentiële Back-ups

De huidige strategie gebruikt uitsluitend full back-ups, wat resulteert in hoge opslagkosten en langere tijden om gegevens te herstellen.

Aanbeveling: Introduceer *incrementele* of *differentiële back-ups*. Deze technieken maken alleen back-ups van gegevens die sinds de laatste back-up zijn gewijzigd, waardoor minder opslagruimte nodig is. Dit versnelt ook het herstelproces, wat cruciaal is voor het waarborgen van de bedrijfscontinuïteit.

Back-upretentie en Beheer

De huidige automatische full back-ups hebben een retentiebeleid van 7 dagen. Hoewel dit een basisbescherming biedt, kan een langere retentieperiode nodig zijn om te voldoen aan specifieke bedrijfs- of compliance-eisen.

Aanbeveling: Pas een uitgebreid retentiebeleid toe dat meer flexibiliteit biedt. Bijvoorbeeld:

- Dagelijkse back-ups: 7 dagen bewaren (zoals nu)
- Wekelijkse back-ups: 4 weken bewaren
- Maandelijkse back-ups: 1 jaar bewaren

Beveiliging van Back-ups

Hoewel de back-ups worden opgeslagen in een Azure Storage Account, zijn er momenteel geen specifieke maatregelen geïmplementeerd om deze te beschermen tegen aanvallen zoals ransomware.

Aanbeveling: Implementeer immutable storage om ervoor te zorgen dat back-ups gedurende een bepaalde periode niet kunnen worden gewijzigd of verwijderd.

Hersteltesten (Restore Testing)

Het is belangrijk dat de back-ups die gemaakt worden ook effectief werken. Momenteel ontbreekt een gestructureerd proces om te testen of de back-ups daadwerkelijk herstelbaar zijn.

Aanbeveling: Voer periodiek restore tests uit in een sandboxomgeving. Met behulp van *Azure Recovery Services Vault* kunnen deze tests worden geautomatiseerd, zodat de integriteit van de back-ups gegarandeerd blijft.

Monitoring en Rapportage

Zonder actieve monitoring en rapportage is het lastig om te bepalen of back-ups consistent worden uitgevoerd.

Aanbeveling: Maak gebruik van *Azure Monitor* of *Log Analytics Workspaces* om proactief meldingen te configureren voor mislukte back-ups. Daarnaast kan het genereren van rapportages helpen bij het volgen van de algehele status van de back-upstrategie.

Redundantie en Disaster Recovery

De huidige back-ups worden opgeslagen in één opslaglocatie. Dit vormt een risico in het geval van een storing of ramp in de primaire regio.

Aanbeveling: Gebruik *geo-redundante opslag (GRS)* om back-ups automatisch te repliceren naar een andere Azure-regio. Dit biedt een extra laag bescherming en verhoogt de beschikbaarheid van gegevens in noodsituaties.

Conclusie

De huidige back-upstrategie van Forvis Mazars biedt een basisbescherming, maar kan zeker op meerdere vlakken verbeterd worden. Door de voorgestelde verbeteringen uit te voeren, kan het bedrijf een veiligere en optimale back-upstrategie

hebben. Automatisering, beveiliging, redundantie en hersteltesten zorgen ervoor dat de back-ups niet alleen schaalbaar en kostenefficiënt zijn, maar ook dat de organisatie in noodsituaties operationeel blijft voor haar belangrijkste processen en bescherming tegen moderne aanvallen zoals een ransomware-aanval.

5

Proof-of-Concept

Voor het eerste 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.

5.0.1. Relevantie van de PoC voor de Azure-omgeving van Forvis Mazars

De Proof-of-Concept (PoC) in VirtualBox simuleert een ransomware-aanval in een lokale omgeving, gericht op het evalueren van beveiligingsmaatregelen zoals immutable storage. Deze aanpak sluit nauw aan bij de Azure-omgeving van Forvis Mazars, waar databases en back-ups worden beheerd.

De technieken uit de PoC, zoals immutable storage, kunnen direct worden toegepast in Azure via functies zoals immutable blobs in Azure Storage. Dit maakt het mogelijk om gegevens beter te beschermen tegen wijzigingen of verwijdering. Daarnaast biedt de PoC een veilig platform om de impact van een ransomware-aanval te begrijpen en te testen hoe snel en effectief back-ups kunnen worden hersteld, wat een cruciaal aspect is voor de bedrijfscontinuïteit.

Forvis Mazars kan de PoC gebruiken om risico's te analyseren en beveiligingsoplossingen eerst kleinschalig te testen, alvorens deze op grotere schaal binnen hun cloudinfrastructuur toe te passen. Hiermee helpt de PoC bij het verfijnen en optimaliseren van hun bestaande Azure-back-upstrategie.

5.0.2. Technische uitwerking

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: Back-up Server, Client, en Attacker

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

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

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

primary.vm.provider "virtualbox" do |vb|
vb.memory = "2048"
vb.cpus = 1
end
end

# Back-up VM
config.vm.define "backup" do |backup|
backup.vm.box = "ubuntu/jammy64"

backup.vm.network "private_network", ip: "192.168.0.20", virtualbox__intnet: "
    internal_network"

backup.vm.provider "virtualbox" do |vb|
vb.memory = "2048"
vb.cpus = 1
end
end

# Attacker VM
config.vm.define "attacker" do |attacker|
attacker.vm.box = "ubuntu/jammy64"

attacker.vm.network "private_network", ip: "192.168.0.30", virtualbox__intnet: "
    internal_network"

attacker.vm.provider "virtualbox" do |vb|
vb.memory = "1024"
vb.cpus = 1
end
end

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 het netwerk. 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	NAT + Internal
Back-up server	1 GB	1	192.168.0.20	Ubuntu 22.04.5 LTS	NAT + Internal
Attacker VM	2 GB	1	192.168.0.30	Ubuntu 22.04.5 LTS	NAT + Internal

Tabel 5.1: Beschrijving van de virtuele machines in de Proof of Concept

De Primary VM stelt een actieve databankserver voor binnen een bedrijfsomgeving. Deze server bevat de operationele data van het bedrijf en vertegenwoordigt de belangrijkste bron die beschermd moet worden tegen dataverlies of aanvallen.

De Back-up VM fungeert als een back-upserver waarop regelmatig de databankback-ups worden opgeslagen. Deze back-upserver is cruciaal voor bedrijfscontinuïteit en disaster recovery, omdat ze in geval van een aanval of fout de herstelmogelijkheden biedt.

De Attacker VM vertegenwoordigt een hacker met slechte intenties binnen de testomgeving. Deze machine wordt gebruikt om een ransomware-aanval te simuleren, waarbij de functionaliteit van zowel de Primary VM als de Back-up VM wordt bedreigd. Het doel van deze opstelling is om te demonstreren hoe een back-upstrategie, inclusief technieken zoals immutable storage, een bedrijf kan beschermen tegen de gevolgen van een dergelijke aanval.

Aanmaken van de database

Op de primary VM werd een eenvoudige SQL-database geïnstalleerd en de volgende tabel aangemaakt om als testdata te dienen:

Listing 5.2: MySQL-code voor het aanmaken van de testdatabank

```
CREATE TABLE employees (
    id INT AUTO_INCREMENT PRIMARY KEY,
    name VARCHAR(50),
    role VARCHAR(50)
);
INSERT INTO employees (name, role) VALUES
    ('Alice', 'Engineer'),
    ('Bob', 'Manager'),
```

```
9       ('Charlie', 'Analyst');
```

Back-up van de database

Nadien werd de database geëxporteerd naar een `.sql`-bestand met het volgende `mysqldump`-commando:

Listing 5.3: mysqldump commando om een databank te exporteren

```
1 mysqldump -u testuser -p testdb > /home/vagrant/backup.sql
```

Het resulterende bestand, `backup.sql`, werd vervolgens met BorgBackup opgeslagen in een back-uprepository op de back-up VM. De repository werd vooraf geïnitialiseerd met het volgende commando:

Listing 5.4: Borg commando om een map te initialiseren als Borg repository

```
1 borg init --encryption=repokey /home/vagrant/backups
```

Vervolgens werd de back-up gemaakt:

Listing 5.5: Borg commando om een back-up te nemen

```
1 borg create --progress
2 ssh://vagrant@192.168.0.20/home/vagrant/backups::backup-$(date +%Y-%m-%d)
3 /home/vagrant/backup.sql
```

Beveiliging van de back-updirectory

Om de back-updirectory ransomware-resistent te maken, werd het Linux-commando `chattr` gebruikt om het *immutable*-attribuut toe te passen op de back-updirectory. Dit attribuut zorgt ervoor dat er geen wijzigingen aan de bestanden in de directory gebeuren, zelfs door gebruikers met `root`-rechten. Het commando:

Listing 5.6: Linux commando om de map immutable te maken

```
1 sudo chattr +i /home/vagrant/backups/
```

Simulatie van de ransomware-aanval

Op de attacker VM werd een script gebruikt om de ransomware-aanval te simuleren. Het script probeert alle bestanden in de back-updirectory te hernoemen door `.malware` toe te voegen aan de bestandsnamen. Dit zou overeenkomen met een ransomware-aanval waarbij de back-up bestanden geëncrypteerd worden. Het script is hieronder weergegeven:

Listing 5.7: Bash script om een ransomware-aanval na te bootsen

```
1 #!/bin/bash
2
3 BACKUP_DIR="/home/vagrant/backups"
4
5 for file in "$BACKUP_DIR"/*; do
```

```
  if [ -f "$file" ]; then
    if mv "$file" "${file}.malware"; then
      echo "Renamed␣$file␣to␣${file}.malware"
    else
      echo "Error:␣Could␣not␣rename␣$file"
    fi
  fi
done
```

Voor het gemak heeft de Attacker VM volledige controle gekregen over de Back-up VM. Dit is gedaan omdat de scope van deze bachelorproef niet is om toegang te verkrijgen tot een server, maar eerder om een gecontroleerde omgeving te creëren waarin een Attacker VM een ransomware-aanval nabootst. Het doel is te demonstreren hoe de ransomware zich verspreidt naar de back-up directory, en niet om de daadwerkelijke methoden voor het verkrijgen van toegang tot een server in detail uit te werken.

Toen dit script werd uitgevoerd op de back-up VM, werd duidelijk dat het hernoemen van de bestanden niet lukte vanwege het immutable-attribuut. Dit toont aan dat de ransomware-aanval niet slaagde en de bestanden in de back-updirectory beschermd bleven.

Herstellen van de back-ups

Om te bewijzen dat de back-ups nog steeds bruikbaar waren, werd een herstelproces uitgevoerd op de primary VM vanuit de Borg-repository:

Listing 5.8: Borg commando om een back-up te herstellen

```
borg extract
ssh://vagrant@192.168.0.20/home/vagrant/backups::backup-2024-12-05
```

De databank werd opnieuw opgezet vanuit het bestand dat uit de Borg-repository werd gehaald met het volgende commando:

Listing 5.9: MySQL commando om een databank te herstellen vanuit een .sql-bestand

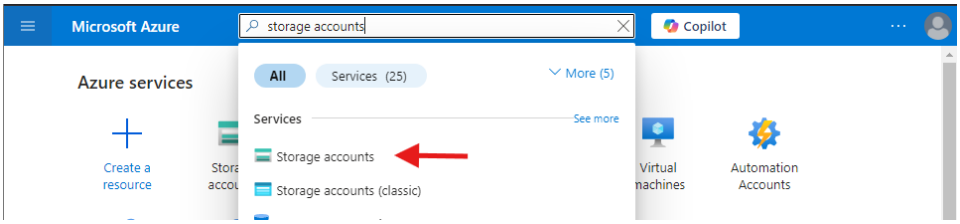
```
mysql -u root -p restored_db < /home/vagrant/backup.sql
```

De back-up werd gebruikt om de database te herstellen en te controleren. Het herstelproces verliep succesvol, wat bewijst dat de immutable storage de integriteit van de back-ups had behouden en dat de bestanden veilig waren gebleven ondanks de ransomware-aanval.

5.0.3. Implementatie van immutable storage in de Azure-omgeving

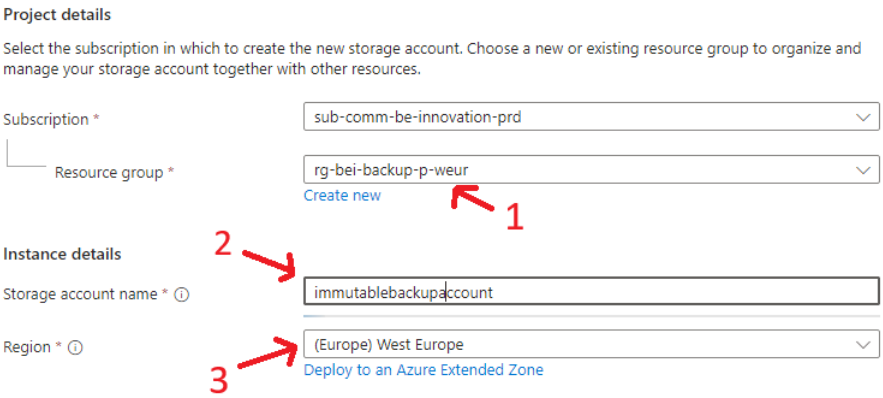
Aanmaken van een storage account

De eerste stap in het implementeren van Immutable Storage in Azure is het aanmaken van een `Storage Account` in de Azure Portal. Bij het aanmaken van het storage

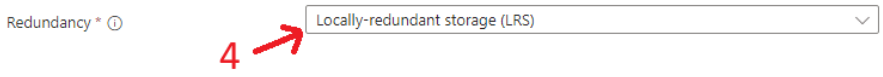


Figuur 5.1: Storage account zoekopdracht binnen de Azure Portal

account kiezen we de correcte resource group, naam die het account moet krijgen, regio en bij redundancy kiezen we voor `Locally-redundant storage (LRS)`. Bij de optie `Account kind` kiezen we voor `General-purpose v2`, omdat deze versie alle benodigde functionaliteit biedt, zoals het ondersteunen van de blob storage en het configureren van immutability policies.



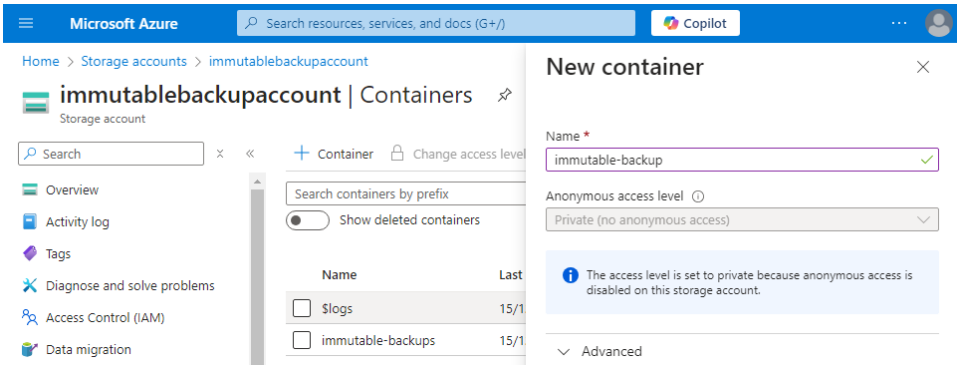
Figuur 5.2: Configuratie voor het nieuwe storage account



Figuur 5.3: Tweede deel van de configuratie voor het nieuwe storage account

Aanmaken van een container binnen het storage account

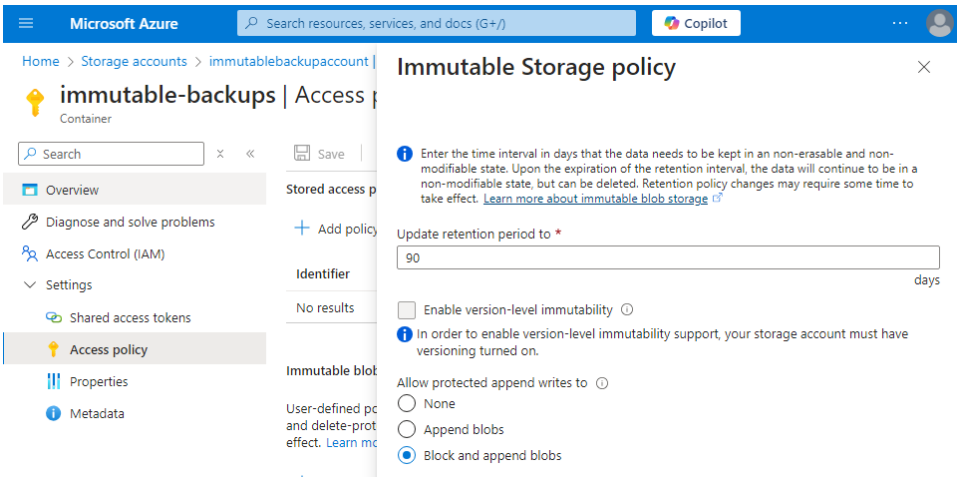
Na het aanmaken van het storage account moet er een container geconfigureerd worden binnen het nieuwe storage account om de gegevens op te slaan. Bij het aanmaken van de container moet de `public access level` op private staan voor de veiligheid. Containers in Azure werken als mappen waarin je blobs kunt opslaan zoals back-ups.



Figuur 5.4: Configuratie voor de container in het storage account

Opzetten van een time-based retention policy

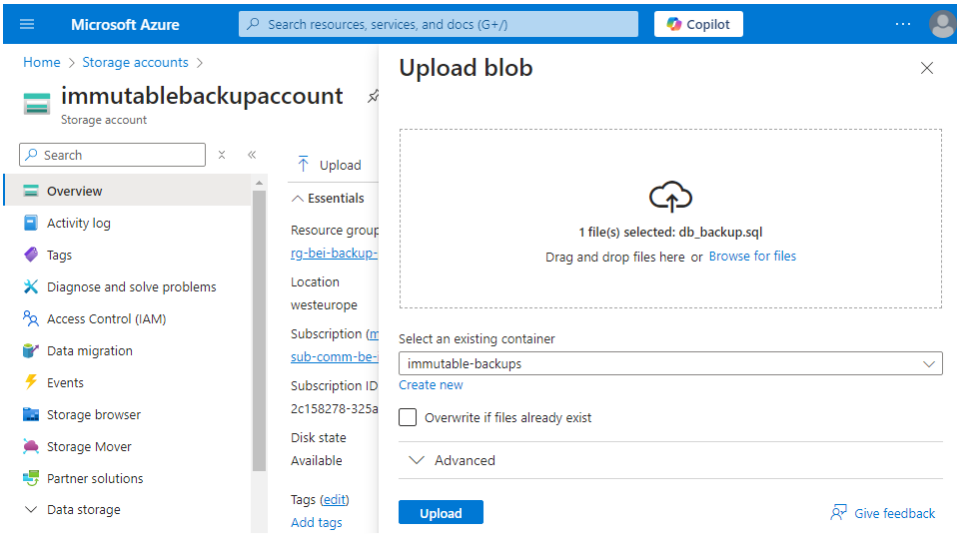
Nadien moet er een immutability policy opgezet worden. Hierbij werd gekozen voor een time-based retention policy van 90 dagen, de back-up is met andere woorden bescherm tegen verwijdering of wijziging voor deze periode. Dit is een veilige en praktische keuze voor back-ups. Daarnaast is er bij de optie `Allow protected append writes to` gekozen voor `Block and append blobs`, dit maakt het mogelijk om gegevens te blijven toevoegen aan de blob zonder de bestaande gegevens te wijzigen of te verwijderen, wat ideaal is voor scenario's zoals logbestanden of incrementele back-ups.



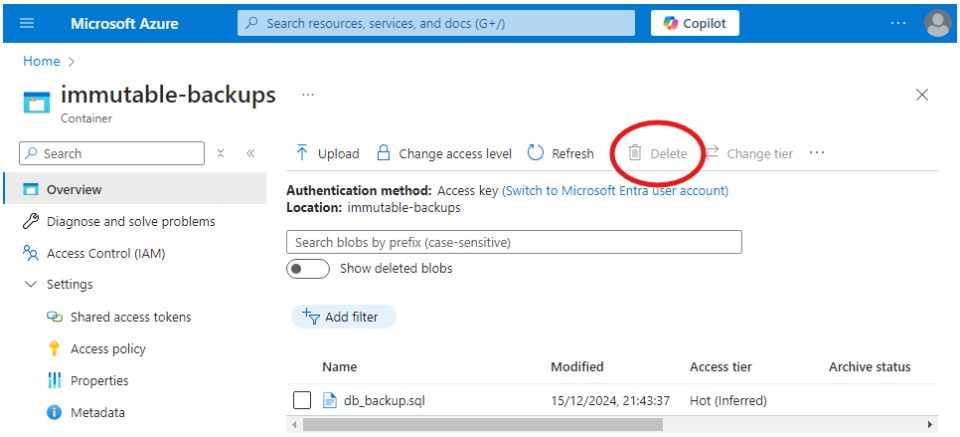
Figuur 5.5: Configuratie voor time-based retention policy

Testen van de immmutable storage

Om de immutable storage te testen is er gekozen om een back-up van een MySQL-database de uploaden naar de container. Na het uploaden van het bestand was er geen optie om dit bestand te verwijderen of te wijzigen. Met andere woorden is deze back-up dus beschermd tegen een ransomware-aanval.



Figuur 5.6: Uploaden van het back-up bestand van de MySQL-databank



Figuur 5.7: Screenshot van de poging om het bestand te verwijderen, waarbij de actie wordt geblokkeerd

Conclusie

De implementatie van immutable storage op het azure storage account is succesvol afgerond, waardoor de opgeslagen back-ups nu beschermd zijn tegen onverwachte wijzigingen of verwijderingen. Daarnaast worden er dagelijks automatische back-ups van de databanken genomen, welke een retentieperiode van 7 dagen hebben. Dit zorgt ervoor dat er altijd een versie van de back-up beschikbaar is, zelfs als de meest recente back-up beschadigd of onbruikbaar blijkt. Deze com-

binatie van immutable storage en versiebeheer versterkt de bescherming tegen dataverlies en maakt het mogelijk om eerdere, werkende back-ups snel te herstellen.

5.0.4. Automatiseren van de manuele back-ups met Docker en Python

5.0.5. Overzicht van de oplossing

Om een efficiënte en schaalbare oplossing te bieden voor het maken van databaseback-ups, werd een geautomatiseerd systeem ontwikkeld met behulp van een Python-script en een Docker-container. Dit systeem automatiseert zowel het maken van back-ups als het verwijderen van oude back-ups op basis van een ingestelde retentieperiode. De focus van deze implementatie is vooral herbruikbaarheid wat ervoor zorgt dat deze oplossing gemakkelijk geïmplementeerd kan worden in de productieomgeving van Forvis Mazars. Voor deze setup is er gebruik gemaakt van een databank die lokaal draait op een virtuele machine die als databank-server functioneert. Daarbij is er een Docker-container die, via het Python-script, back-ups neemt van de databank. Dit komt overeen met de actieve omgeving die Forvis Mazars gebruikt.

5.0.6. Python-script voor back-ups

Het Python-script vormt de kern van dit systeem en voert twee belangrijke taken uit. Enerzijds zorgt het voor het genereren van back-ups door gebruik te maken van `mysqldump` voor MySQL-databases en `pg_dump` voor PostgreSQL-databases. Deze tools bieden de mogelijkheid om volledige databaseback-ups te maken die in een gestandaardiseerd formaat worden opgeslagen. Anderzijds implementeert het script een retentiebeleid waarbij oude back-ups die ouder zijn dan een vooraf ingestelde periode automatisch worden verwijderd. Daarnaast is logging geïntegreerd in het script om eventuele fouten of waarschuwingen te registreren, wat helpt bij monitoring en foutopsporing.

Python-script: Backups en Retentie

Het volledige Python-script is hieronder weergegeven:

Listing 5.10: Python-script voor back-ups en retentie

```
1  import datetime
2  import os
3  import subprocess  # nosec
4  import getpass
5  import argparse
6  import logging
7
8  class Backup:
9
10 def __init__(self, database_name, database_user, type):
11 timestr = datetime.datetime.now().strftime('%Y-%m-%d')
```

```
self.filename = f'backup-{type}-{timestr}-{database_name}.dump'
self.database_name = database_name
self.database_user = database_user
self.type = type
self.password = None
self.hostname_mysql = os.environ.get("HOSTNAME_MYSQL", "192.168.1.62")
self.hostname_psql = os.environ.get("HOSTNAME_PSQL")
self.port_mysql = os.environ.get("PORT_MYSQL", "3306")
self.port_psql = os.environ.get("PORT_PSQL")

def set_password(self):
"""
Retrieve␣the␣database␣password␣from␣an␣environment␣variable.
"""
self.password = os.environ.get("DB_PASSWORD")
if not self.password:
logging.warning("Database␣password␣not␣set.␣Please␣provide␣the␣DB_PASSWORD␣
    environment␣variable.")
exit(1)

def create_backup(self, type):
"""
Create␣a␣backup␣of␣the␣database.
"""
if type == "MYSQL":
try:
cmd = [
'mysqldump',
'--single-transaction',
'-u', self.database_user,
f'-p{self.password}',
'-h', self.hostname_mysql,
'-P', str(self.port_mysql),
'--no-tablespaces',
'-B', self.database_name,
]

with open(self.filename, 'w') as backup_file:
result = subprocess.run(cmd, stdout=backup_file, check=True)  # nosec

if result.returncode != 0:
logging.warning(f'Command␣failed.␣Return␣code:␣{result.returncode}')
exit(1)

return self.filename

except Exception as e:
logging.warning(e)
exit(1)

elif type == "PSQL":
```

```
try:
cmd = [
'pg_dump',
f'--dbname=postgresql://{self.database_user}:{self.password}@{self.hostname_psql}:{self.port_psql}/{self.database_name}',
'-Fc',
'-f', self.filename
]

result = subprocess.run(cmd, check=True)  # nosec

if result.returncode != 0:
logging.warning(f'Command failed. Return code: {result.returncode}')
exit(1)

return self.filename

except Exception as e:
logging.warning(e)
exit(1)

@staticmethod
def delete_old_backups(directory, retention_days):
"""
Deletes backup files older than the specified retention period.
"""
now = datetime.datetime.now()
for file in os.listdir(directory):
if file.startswith("backup-") and file.endswith(".dump"):
file_path = os.path.join(directory, file)
file_mtime = datetime.datetime.fromtimestamp(os.path.getmtime(file_path))
age = (now - file_mtime).days
if age > retention_days:
try:
os.remove(file_path)
logging.info(f"Deleted old backup: {file_path}")
except Exception as e:
logging.warning(f"Failed to delete {file_path}: {e}")


def main():
parser = argparse.ArgumentParser(description="Execute a local backup of a database.")
parser.add_argument("-dn", "--database_name", required=True, help="Enter the name of the database for the backup.")
parser.add_argument("-du", "--database_user", required=True, help="Enter the username of the database for the backup.")
parser.add_argument("-b", "--backup", action="store_true", help="Backup the database.")
parser.add_argument("-t", "--type", choices=["MYSQL", "PSQL"], required=True, help="MYSQL or PSQL")
```

```
parser.add_argument("-bd", "--backup_directory", required=True, help="Directory where backups will be stored.")
parser.add_argument("-r", "--retention", type=int, help="Retention period in days for old backups.")
args = parser.parse_args()

db_name = args.database_name
db_user = args.database_user
backup = args.backup
type = args.type
backup_directory = args.backup_directory
retention = args.retention

if backup:
b = Backup(db_name, db_user, type)
try:
b.set_password()
backup_file = b.create_backup(type=type)
if backup_file:
backup_path = os.path.join(backup_directory, backup_file)
os.rename(backup_file, backup_path)
print(f"Backup successful: {backup_path}")
except Exception as e:
logging.warning(e)

if args.retention is not None:
backup = Backup("", "", "")  # Placeholder values, not needed for deletion
try:
backup.delete_old_backups(args.backup_directory, args.retention)
except Exception as e:
logging.warning(e)
else:
print(f"Old backups older than {args.retention} days deleted successfully.")
return

if __name__ == '__main__':
main()
```

5.0.7. Automatisering met Docker

De automatisering wordt verder versterkt door het gebruik van een Docker-container. Deze container biedt een reproduceerbare omgeving waarin het script kan worden uitgevoerd. Door een gestandaardiseerde Docker-image te gebruiken die gebaseerd is op Ubuntu, wordt een consistente setup gegarandeerd dat Forvis Mazars makkelijk kan implementeren. Binnen de container wordt een `setup.sh` script uitgevoerd om cronjobs te configureren die verantwoordelijk zijn voor het dagelijks maken van nieuwe back-ups om 2:00 uur 's nachts en het verwijderen van oude back-ups die ouder zijn dan 14 dagen. De retentieperiode is hier dus op 14 dagen gezet voor de dagelijkse back-ups. Daarnaast zorgt dit Bash-script ook voor

het opstarten van de cron-service. Dit is nodig om een cronjob uit te voeren. De back-ups worden opgeslagen in een aparte directory binnen de container, en de cron-service wordt gestart door het setup-script. Bij het opzetten van de container worden ook alle benodigde softwarepakketten geïnstalleerd zoals `mysql-client`, `cron`, en `python3`. Er worden 2 bestanden gekopieerd naar de container namelijk het Python-script en het Bash-script.

Dockerfile

Hieronder volgt de Dockerfile die gebruikt is voor het bouwen van de container:

Listing 5.11: Dockerfile voor de back-upcontainer

```
FROM ubuntu:latest

WORKDIR /src

USER root
RUN apt update -y \
&& apt -y install mysql-client cron nano \
&& apt install -y python3

COPY src/* /src/
COPY crontab.txt /etc/cron.d/my-cron-job
COPY src/setup.sh /src/setup.sh

RUN chmod 0644 /etc/cron.d/my-cron-job && \
chmod +x /src/backup_script.py
RUN chmod +x /src/setup.sh
ENTRYPOINT ["tail"]
CMD ["-f", "/dev/null"]
```

Setup-script

Het `setup.sh`-script dat wordt uitgevoerd in de container is hieronder weergegeven:

Listing 5.12: Setup-script voor het configureren van cronjobs

```
#!/bin/bash
service cron start

mkdir /src/backups

echo -e "0 2 * * * DB_PASSWORD='root' python3 /src/backup_script.py -dn testdb -du
     root -t MYSQL -b -bd /src/backups >> /var/log/cron.log 2>&1\n0 2 * * *
    DB_PASSWORD='root' python3 /src/backup_script.py -bd /src/backups -r 14 -dn
    testdb -du root -t MYSQL >> /var/log/cron.log 2>&1" | crontab -

exec "$@"
```

5.0.8. Relevantie voor Forvis Mazars

Deze oplossing kan eenvoudig worden geïntegreerd in de infrastructuur van Forvis Mazars, omdat het gebruik maakt van Docker-containers. Forvis Mazars beheert hun back-ups binnen een Kubernetes-cluster, en Docker-containers kunnen rechtstreeks als pods worden gedeployed in Kubernetes. Hierdoor kan de huidige oplossing zonder aanpassingen worden hergebruikt. De setup in deze implementatie, waarbij de databases op een virtuele machine draaien en de back-ups worden uitgevoerd via Docker-containers, komt overeen met de werkomgeving van Forvis Mazars. Dit zorgt ervoor dat de voorgestelde oplossing naadloos aansluit op hun huidige infrastructuur en gebruiksbehoeften.

6

Conclusie

In dit onderzoek werd onderzocht hoe de back-upstrategie voor Azure PostgreSQL en MySQL databases bij Forvis Mazars kan worden geoptimaliseerd met behulp van immutabele opslag en automatische back-ups. De implementatie van deze technologieën is essentieel om de betrouwbaarheid van back-ups te verhogen en om te beschermen tegen dataverlies, vooral in het geval van cyberaanvallen zoals ransomware. Door immutabele opslag toe te passen, kunnen de back-ups niet meer worden gewijzigd of verwijderd, zelfs niet door kwaadwillende actoren. Daarnaast zorgt de automatisering van de back-ups voor een consistente en betrouwbare back-upcyclus, waardoor het risico op menselijke fouten wordt verminderd en altijd een herstelpunt beschikbaar is.

Hieronder een beschrijving hoe de onderzoeksvraag en de deelvragen zijn beantwoord:

Hoofdvraag: 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?

De huidige back-upstrategie bij Forvis Mazars bestaat uit automatische dagelijkse full backups van hun databases en manuele back-ups die via een script naar een Azure Storage Account worden gepusht. De back-ups worden 7 dagen bewaard. De implementatie van immutabele opslag, in combinatie met een geautomatiseerde back-upstrategie, biedt aanzienlijke voordelen voor de bescherming van deze back-ups tegen dataverlies en cyberaanvallen, zoals ransomware. Door immutabele opslag in te schakelen, kunnen de back-ups gedurende de ingestelde retentieperiode (bijvoorbeeld 30 dagen) niet worden gewijzigd of verwijderd, wat het risico op verlies van back-upgegevens drastisch vermindert. De dagelijkse automatische back-ups zorgen ervoor dat er altijd een up-to-date herstelpunt beschikbaar is, zelfs als de meest recente back-up corrupt raakt.

Deelvraag 1: Hoe veilig en betrouwbaar zijn de huidige back-upoplossingen van Forvis Mazars voor Azure PostgreSQL en MySQL databases?

De huidige back-upoplossingen van Forvis Mazars omvatten automatische dagelijkse full backups via Azure en manuele back-ups opgeslagen in een Azure Storage Account. De automatische back-ups bieden basisbescherming, maar de manuele back-ups zijn minder frequent en afhankelijk van menselijke interventie, wat kan leiden tot inconsistenties of gemiste back-ups. Hoewel de back-ups worden opgeslagen in een beveiligd Azure Storage Account, is er een potentieel risico van dataverlies of corruptie, vooral als back-ups worden overschreven of verwijderd. Er wordt momenteel geen gebruik gemaakt van technieken zoals immutabele opslag, die een extra beveiligingslaag biedt door ervoor te zorgen dat back-ups niet gewijzigd of verwijderd kunnen worden, zelfs niet door kwaadwillende actoren of interne fouten. De betrouwbaarheid van de huidige oplossing is dus goed, maar kan sterk worden verbeterd met de implementatie van immutabele opslag.

Deelvraag 2: Welke rol speelt immutabele opslag in het beschermen van back-ups tegen ransomware en andere vormen van dataverlies?

Immutabele opslag speelt een cruciale rol in het beschermen van back-ups tegen ransomware en andere vormen van dataverlies door te garanderen dat de opgeslagen back-upgegevens niet kunnen worden gewijzigd of verwijderd tijdens de ingestelde retentieperiode. Bij een ransomware-aanval worden vaak gegevens in een netwerk versleuteld, inclusief back-ups. Immutabele opslag voorkomt dit door de integriteit van de back-updata te beschermen. Zelfs als een aanvaller toegang krijgt tot het systeem, kunnen de back-ups niet worden overschreven of verwijderd, waardoor het herstel na een aanval mogelijk blijft. Dit zorgt ervoor dat er altijd een veilige versie van de back-up beschikbaar is, wat essentieel is voor het herstel van systemen na een incident. Door immutabele opslag toe te passen, kunnen organisaties zoals Forvis Mazars er zeker van zijn dat hun back-ups intact blijven, zelfs in geval van ernstige bedreigingen zoals ransomware.

Deelvraag 3: Wat zijn de belangrijkste uitdagingen bij het integreren van immutabele opslag met Azure cloud back-upsystemen?

Er zijn verschillende uitdagingen bij het integreren van immutabele opslag met Azure cloud back-upsystemen:

- **Configuratie en integratie:** Het correct configureren van immutabele opslag in combinatie met de bestaande Azure back-ups kan complex zijn. Het vereist dat het juiste beleid voor de retentieperiode wordt ingesteld en dat het back-upproces goed wordt geconfigureerd om de back-ups naar een immutabele opslaglocatie te sturen. Dit kan technische expertise en zorgvuldige planning vereisen.
- **Compatibiliteit met bestaande systemen:** Niet alle systemen of applicaties

kunnen volledig profiteren van immutabele opslag. Er moet worden gezorgd dat de bestaande back-upprocedures en -tools die Forvis Mazars gebruikt, compatibel zijn met immutabele opslag. Dit kan extra stappen vereisen, zoals de integratie van specifieke Azure-functies.

- **Kosten:** Het gebruik van immutabele opslag kan kosten met zich meebrengen, zowel voor opslag als voor de implementatie van aanvullende beveiligingsmaatregelen. Er moeten afwegingen worden gemaakt tussen de kosten van het gebruik van immutabele opslag en de voordelen die het biedt in termen van bescherming tegen dataverlies en cyberaanvallen.

Ondanks deze uitdagingen biedt de integratie van immutabele opslag aanzienlijke voordelen voor de veiligheid en betrouwbaarheid van back-ups, en kan het helpen bij het verminderen van de risico's van gegevensverlies en aanval.

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.

A.0.1. abstract

In deze bachelorproef wordt een optimalisatie van de back-upstrategie voor de Azure PostgreSQL en MySQL databases bij Forvis Mazars onderzocht, de focus ligt voornamelijk op immutabele opslag en automatische back-ups. Het doel is om de back-upstrategie van Forvis Mazars te optimaliseren en het resistent te maken tegen ransomware-aanvallen. Daarnaast wordt er ook een Proof-of-Concept (PoC) uitgevoerd, waarin immutabele opslag wordt geïmplementeerd om ervoor te zorgen dat back-ups onveranderlijk zijn na opslag. Verder worden geautomatiseerde back-ups geïmplementeerd om de back-ups efficiënter te maken en de consistentie van de back-ups te verbeteren. In de state-of-the-art ligt de focus op bestaande back-upstrategieën, zoals cloud back-ups, on-premise back-ups, en offline back-ups. De methodologie omvat een literatuurstudie, een analyse van de huidige back-upstrategie bij Forvis Mazars, en de ontwikkeling van een PoC. De verwachte resultaten zullen de verbeterde beveiliging en efficiëntie van de back-upstrategie aantonen, met als doel het minimaliseren van de risico's op dataverlies en het waarborgen van bedrijfscontinuïteit.

Inhoudsopgave

A.0.2. Inleiding

Ransomware-aanvallen zijn één van de meest voorkomende aanvallen dat een organisatie kan treffen de dag van vandaag. Om gegevensverlies tegen te gaan in geval van een aanval moeten bedrijven altijd een back-upplan klaar hebben in geval van een incident. Het niet hebben van een back-upplan of het hebben van een suboptimaal plan kan leiden tot een groot verlies op financieel vlak. Daarnaast kan dit ook zorgen voor het verliezen van cruciale informatie en als laatste kan dit de reputatie van een organisatie sterk doen dalen, aangezien niemand in zee wilt gaan met een bedrijf dat niet goed beveiligd is of niet goed voorbereid is op uitzonderlijke incidenten. Om deze redenen is het van groot belang voor een bedrijf om een doordacht, robuust en veilig back-upplan te hebben.

Het doel van deze bachelorproef is het optimaliseren van het back-upplan van Forvis Mazars. Dit bedrijf maakt gebruik van 2 soorten databases in Azure, eenderzijds een PostgreSQL databank en anderzijds een MySQL databank. Van deze databanken worden er automatische alsook manuele back-ups gemaakt. De automatische back-ups gebeuren door Azure zelf en de manuele back-ups worden per database uitgevoerd. Stel dat applicatie A een nieuwe versie heeft, dan zal er eerst een back-up genomen worden van de database vooraleer de nieuwe versie uitgerold wordt. Echter zijn er nog bepaalde verbeteringen mogelijk, zoals het veiliger opslaan van deze back-ups met behulp van technieken als immutable storage en het instellen van geautomatiseerde dagelijkse, wekelijkse en maandelijkse back-ups. Daarbij is een belangrijk aandachtspunt dat de databanken beter beveiligd moeten worden tegen cyberaanvallen aangezien gegevens in zo'n situatie versleuteld of vernietigd kunnen worden.

De doelgroep van dit onderzoek bestaat uit de IT-professionals en vooral de systeembeheerders van Forvis Mazars, die verantwoordelijk zijn voor het beheer van de back-ups en de beveiliging van gegevens binnen de organisatie alsook het herstellen van alle gegevens na een incident.

De onderzoeksvraag die onderzocht zal worden is: "Hoe kan de back-upstrategie van de Azure PostgreSQL en MySQL databases bij Forvis Mazars worden geoptimaliseerd door het implementeren van automatische back-ups en het veilig opslaan van deze back-ups om gegevensverlies te minimaliseren?" In dit onderzoek wordt onderzocht hoe de bestaande back-upoplossingen kunnen worden verbeterd, zodat Forvis Mazars in geval van een incident goed voorbereid is en geen informatie

verliest. De onderzoeksvraag kan onderverdeeld worden in volgende kleinere 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?

Het uiteindelijke doel van dit onderzoek is om ervoor te zorgen dat de Azure databanken van Forvis Mazars een geoptimaliseerd back-upplan hebben dat veilig en efficient is. Het plan moet immuun zijn tegen ransomware-aanvallen en daarnaast moet het ook geautomatiseerd zijn. Daarbij zal de tijd bij een herstel vanuit een back-up ook onderzocht worden. Om het back-upplan te testen zal er een Proof-of-Concept (PoC) opgesteld worden om alles grondig te testen in een testomgeving.

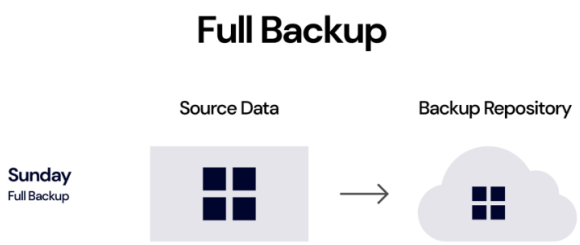
A.0.3. Literatuurstudie

Bedrijven moeten hun data goed beschermen om succesvol te zijn. Echter vormen back-ups van de databases vaak een zwakke schakel in de beveiligingsketen van gegevensbescherming. Hoewel veel organisaties zich richten op het beveiligen van hun actieve databases, worden de back-ups vaak over het hoofd gezien, wat een groot risico met zich meebrengt. Back-ups worden meestal offsite opgeslagen, bijvoorbeeld op tape, en zijn daardoor vatbaar voor verlies of diefstal (Cherry, 2015). Dit maakt het van essentieel belang om back-ups goed te beveiligen, bijvoorbeeld door encryptie. Echter, bij het kiezen van een encryptieoplossing is het belangrijk om een evenwicht te vinden tussen de sterkte van de encryptie en de impact op de prestaties van de server omdat sterke encryptie meer resources nodig heeft en het kan de beschikbaarheid van de back-ups veranderen. In de afgelopen jaren is er een scherpe toename van ransomware-aanvallen gericht op bedrijven, waarbij het aantal getroffen organisaties is gestegen van ruim 2.700 naar bijna 4.900 in slechts twaalf maanden. Deze toename laat zien hoe vastberaden en steeds slimmer ransomwaregroepen worden in hun aanvallen. Wat bijzonder zorgwekkend is voor de bedrijfswereld, is de trend van herhaalde aanvallen op bedrijven, waarbij sommige organisaties binnen korte tijd door meerdere ransomwaregroepen worden getroffen (Dikbiyik e.a., 2024). Dit wijst erop dat cybercriminelen actief profiteren van momenten van kwetsbaarheid om bedrijven in hun zwakste momenten

opnieuw aan te vallen, wat de noodzaak voor robuuste preventieve maatregelen benadrukt.

back-upstrategieën

Full back-up



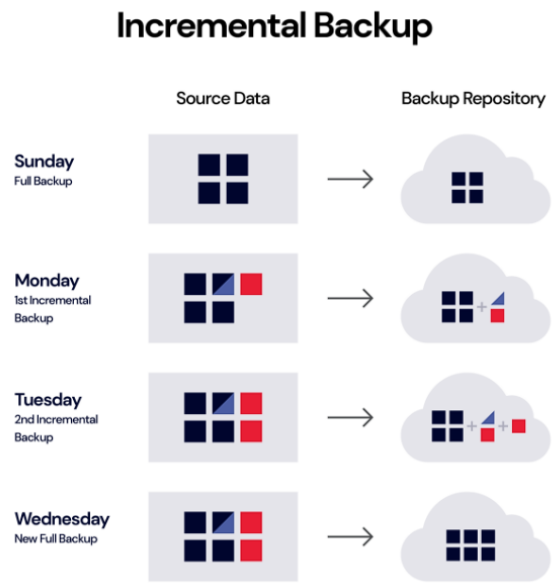
Figuur A.1: Representatie van een full back-up (Rivas, 2022)

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 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. Ten eerste is het proces van het lezen en schrijven van het volledige bestandssysteem tijdsintensief, vooral bij grote hoeveelheden data. Ten tweede gebruikt het opslaan van een volledige kopie van het bestandssysteem veel opslagruimte, wat inefficiënt kan zijn wanneer de back-ups regelmatig worden gemaakt (Chervenak e.a., 1998).

Incremental back-up

Incremental back-ups zijn een efficiënte methode om alleen gewijzigde data sinds de laatste back-up op te slaan, wat tijd en opslag bespaart. In tegenstelling tot een volledige back-up, die alle data kopieert, richten incrementele back-ups zich enkel op nieuwe of aangepaste bestanden. Dit maakt ze sneller, maar hersteltijden kunnen langer zijn omdat meerdere incrementele back-ups nodig zijn naast de laatste volledige back-up. Recente onderzoeken hebben zich gericht op het optimaliseren van back-upstrategieën, met name voor databasesystemen. Zo zijn er modellen ontwikkeld die bepalen hoe vaak volledige en incrementele back-ups moeten worden uitgevoerd op basis van factoren zoals systeem-betrouwbaarheid, de hoeveelheid dataveranderingen en back-up-kosten (Zhao e.a., 2024). Er zijn ook varianten zoals differentiële back-ups, die alle veranderingen sinds de laatste volledige back-up bevatten, waardoor de hersteltijd korter kan zijn dan bij traditionele incrementele back-ups. Daarnaast zorgen moderne geautomatiseerde oplos-

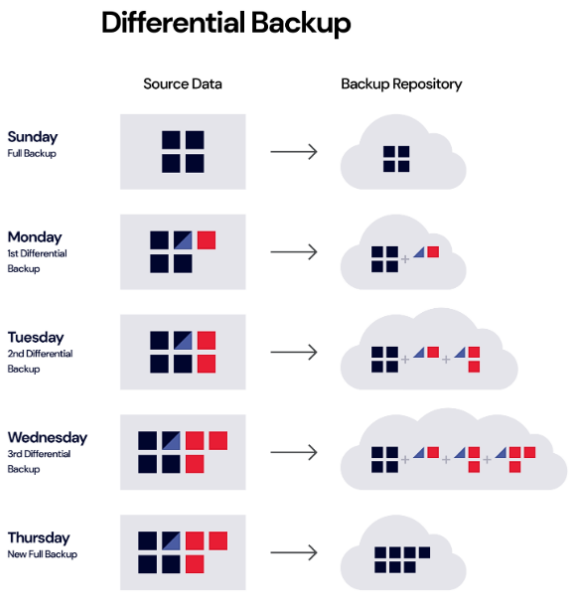
singen voor continue incrementele back-ups, wat realtime herstelmogelijkheden biedt zonder noemenswaardige belasting van de productieomgeving (Qian e.a., 2010).



Figuur A.2: Representatie van een incremental back-up (Rivas, 2022)

Differentiële back-up

Een differentiële back-up is een soort back-up waarbij alleen de data die sinds de laatste volledige 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. Dit komt doordat elke differentiële back-up alle wijzigingen sinds de meest recente volledige back-up bevat, waardoor de grootte van de back-up groter wordt naarmate er meer wijzigingen plaatsvinden. Een belangrijk voordeel van differentiële back-ups is de relatief snelle hersteltijd (Beard, 2018). Om data te herstellen, is alleen de laatste volledige back-up en de meest recente differentiële back-up nodig, wat het herstelproces eenvoudiger en sneller maakt dan bij incrementele back-ups. Differentiële back-ups zijn bijzonder nuttig in omgevingen waar een snel herstelproces cruciaal is, zoals bij bedrijven die minimale downtime vereisen. Het nadeel van differentiële back-ups is dat de back-ups groter worden naargelang de tijd tussen de volledige back-ups. Elke nieuwe differentiële back-up bevat namelijk alle wijzigingen sinds de laatste volledige back-up, wat betekent dat deze geleidelijk groter wordt totdat er een nieuwe volledige back-up wordt gemaakt. Daarom is het belangrijk om een goede balans te vinden tussen de frequentie van volledige back-ups en differentiële back-ups.



Figuur A.3: Representatie van een differentiële back-up (Rivas, 2022)

On-premise back-ups

Bedrijven staan vaak voor de uitdaging om te beslissen of ze hun data on-premise opslaan of de voorkeur geven aan een cloud-service (Ali e.a., 2024). On-premise back-ups slaan gegevens lokaal op, meestal op fysieke schijven binnen het bedrijf zelf. Deze methode biedt bedrijven volledige controle over hun back-up- en gegevensbeheer. Een belangrijk voordeel van on-premise back-ups is dat data altijd beschikbaar is, zelfs zonder toegang tot het internet, wat nuttig is bij netwerkproblemen (Trovato e.a., 2019). Daarnaast hebben bedrijven volledige eigendom over de beveiliging van hun gegevens, aangezien de opslag lokaal blijft binnen het bedrijf. Hoewel deze methode geen terugkerende kosten aan externe providers met zich meebrengt, brengt het wel risico's met zich mee, zoals schade door brand of overstromingen, en vraagt het om regelmatige onderhoud van de hardware. Het herstelproces is doorgaans sneller dan bij een cloudservice, wat van cruciaal belang kan zijn na een ransomware-aanval of een ander incident.

Cloud-gebaseerde back-ups

Cloud-gebaseerde back-ups zijn een populaire oplossing waarbij data extern wordt opgeslagen bij een bedrijf dat cloudservices aanbiedt. Dit biedt individuen en bedrijven de mogelijkheid om hun gegevens veilig op afstand te bewaren, zonder dat ze hoeven te investeren in fysieke opslagapparaten. Hoewel dit handig is om gegevensverlies te voorkomen bij hardware- of softwarestoringen, of onverwachte rampen, brengt het gebruik van cloud-opslag vaak aanzienlijke kosten met zich mee, vooral op de lange termijn (Obrutsky, 2016). Naarmate je meer opslag nodig hebt is er altijd een mogelijkheid om te opschalen, dit is een groot voordeel van het gebruiken van een cloudservice. Echter, het waarborgen van de veiligheid van

deze data is een cruciaal aandachtspunt, vooral omdat cloudproviders vaak niet open zijn over hoeveel kopieën van de data er zijn en waar deze precies worden opgeslagen. Om problemen zoals datalekken en foutieve verwijdering te voorkomen, zijn er nieuwe methoden zoals “assured deletion” ontwikkeld, waarmee klanten zeker weten dat hun gegevens permanent worden verwijderd op verzoek. Hierdoor kunnen bedrijven hun data met zekerheid beheren in de cloud terwijl gevoelige informatie veilig blijft (Rahumed e.a., 2011).

Offline back-ups

Offline back-ups zijn een traditionele methode waarbij data wordt opgeslagen op fysieke media, meestal externe harde schijven zonder tussenkomst van het internet. Het voornaamste voordeel is dat de data dan beveiligd is tegen online bedreigingen en er geen internettoegang nodig is om aan de data te geraken (Edwards, 2022). Een belangrijk voordeel is dat offline back-ups niet beïnvloed worden door stroomstoringen of internetuitval, waardoor ze een robuuste back-upoptie vormen voor gevoelige data. Echter, in tegenstelling tot on-premise back-ups, die vaak op dezelfde fysieke locatie als de IT-infrastructuur van een bedrijf worden opgeslagen, kunnen offline back-ups eenvoudig meegenomen en elders bewaard worden, waardoor ze extra bescherming bieden tegen fysieke rampen. Toch delen beide methoden het nadeel dat ze kwetsbaar zijn voor schade door ongelukken, diefstal of verlies, en moeten de fysieke apparaten op een veilige locatie opgeslagen worden (James, 2019).

Immutable storage

Immutable storage is een type opslag waarbij data niet meer kan worden gewijzigd of aangepast vanaf het geback-upt is. Dit concept is cruciaal voor het waarborgen van de integriteit van belangrijke gegevens. Het idee achter immutability is dat bepaalde bestanden, nadat ze zijn gemaakt, niet meer mogen worden gewijzigd zonder de juiste autorisatie. Dit biedt een sterke bescherming tegen ongewenste wijzigingen en hierdoor kunnen hackers de gegevens niet aanpassen. Immutable storage speelt dus een belangrijke rol in het beschermen van systemen tegen cyberaanvallen. Bij aanvallen, waarbij hackers volledige toegang verkrijgen, kunnen onbeveiligde systemen worden gemanipuleerd of misbruikt. Immutable storage voorkomt dit, omdat de opgeslagen gegevens niet kunnen worden gewijzigd, zelfs niet door iemand met volledige toegang. Hierdoor wordt de integriteit van de data behouden en is het risico op schade door hackers aanzienlijk kleiner (Hasan e.a., 2005).

A.0.4. Methodologie

In de eerste fase van het onderzoek zal er een grondige literatuurstudie worden uitgevoerd rond back-upstrategieën, ransomware-resistentie, en immutable storage met een overzicht van de state of the art van back-upstrategieën en immutabele

opslag als deliverable. Wetenschappelijke papers, bedrijfscasussen en technische artikels zullen gebruikt worden om een theoretische basis aan te leggen en om de best-practices te achterhalen. Dit zal ook helpen om de onderzoeksvragen te beantwoorden. Daarnaast zal er een Proof-Of-Concept ontworpen worden waarbij onderzocht zal worden hoe er immutable back-ups gemaakt kunnen worden voor de back-ups van Forvis Mazars. Daarnaast zal er een testomgeving opgezet worden om een ransomware-aanval na te bootsen en het systeem opnieuw op gang te krijgen. De deliverable voor de PoC is een werkende immutable back-upoplossing in Azure die tegen een ransomware-aanval bestendig is. Verder zal er een optimale back-upstrategie opgesteld worden met de state-of-the-art technieken. De literatuurstudie zal ongeveer 4 weken duren, de Proof-Of-Concept zal 4 weken duren en als laatst zal het rapport met de optimale verbeteringen 2 weken duren.

A.0.5. Verwacht resultaat, conclusie

Het verwachte resultaat is dat door de implementatie van immutable storage en automatische back-ups, de back-upstrategie van Forvis Mazars zal worden verbeterd. Vooral de bescherming tegen ransomware en andere bedreigingen zal beter zijn door het gebruik van immutable storage, waarbij back-ups onveranderlijk worden opgeslagen en niet kunnen worden gemanipuleerd. Daarnaast zorgt de automatisering van de back-ups voor een efficiënter beheer, waarbij de manuele taken van het IT-team verminderd worden. Dit kan in de praktijk leiden tot meer consistente back-ups en een verbeterde betrouwbaarheid van het systeem. De resultaten zullen waarschijnlijk aantonen dat de combinatie van deze twee oplossingen zorgen voor een sterkere, efficiëntere en beter back-upstrategie.

Bibliografie

Ali, A., Laghari, A. A., Kandhro, I. A., Kumar, K., & Younus, S. (2024). Systematic analysis of on-premise and cloud services. *International Journal of Cloud Computing*, *13*(3), 214–242. https://doi.org/https://doi.org/10.1504/IJCC.2024.139604

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

BorgBackup. (2024, november 18). *Borg Documentation*. Verkregen december 14, 2024, van https://borgbackup.readthedocs.io/en/latest/

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

Cherry, D. (2015). Database Backup Security, 293–311. https://doi.org/https://doi.org/10.1016/B978-0-12-801275-8.00010-5

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

Dikbiyik, F., Gul, F., Tapkan, G., Han, Y., Akdora, O., Budakoglu, G., Ciftci, B., Celik, E. S., Cengiz, S. E., Toprak, G., & Dogan, Y. (2024). State of Ransomware 2024:A Year of Surgesand Shuffling. *Black kite*. https://blackkite.com/wp-content/uploads/2024/05/BlackKite_Report_Ransomware-2024.05.14.pdf

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

Erickson, J. (2024). MySQL: Understanding What It Is and How It's Used. *Oracle*. https://www.oracle.com/be/mysql/what-is-mysql/

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

MySQL. (z.d.). *MySQL 8.4 Reference Manual: MySQL Glossary*. Verkregen december 15, 2024, van https://dev.mysql.com/doc/refman/8.4/en/glossary.html

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

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

Qian, C., Huang, Y., Zhao, X., & Nakagawa, T. (2010). Optimal Backup Interval for a Database System with Full and Periodic Incremental Backup. *Journal of Computers*, *5*(4), 557–564. https://doi.org/10.4304/jcp.5.4.557-564

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