Gegevensbescherming in cloud-omgevingen: encryptie- en sleutelbeheer

8 oktober 2021 Gülnur Orpak

(Publicatie: 8 oktober 2021)

De revolutionaire ontwikkeling van cloud computing zou een enorme mislukking worden zonder voldoende activiteiten in de sfeer van beveiliging en privacybescherming, zoals encryptie- en sleutelbeheer. [SHAH 14] *Cloud service users* (hierna 'users') en IT-auditors besteden daar niet altijd genoeg aandacht aan. Er is dan ook een grotere rol voor de IT-auditors weggelegd dan we vaak zien. Dit artikel wil hen daar een aantal handvatten voor aanreiken.

Cloud computing is on demand-levering van IT-middelen via internet met *pay as yougo-prijzen*. In plaats van fysieke datacenters en servers te kopen, bezitten en onderhouden, heeft men toegang tot technologische diensten zoals rekenkracht, opslag en databases, op *as needed* basis. [AWS20] Ondanks dat een user een aantal diensten van de provider afneemt, is hij ook zelf verantwoordelijk voor een aantal activiteiten in de sfeer van beveiliging en privacybescherming, zoals encryptie- en sleutelbeheer. In hoeverre, is afhankelijk van het gekozen servicemodel.

Cloudbeveiliging en gegevensbescherming

Het aangaan van een zakelijke overeenkomst met derden betekent het aangaan van een relatie met hun governance, beheersmaatregelen en risicobeheer. De manier waarop zij hun organisatie beheersen en hun organisatiestructuur opzetten zou van significant belang moeten zijn voor een user. [ISACA19] Cloud services en de diensten die cloud serviceproviders (hierna 'providers') bieden, hebben grote impact op het IT-landschap van een user, zoals algemene veiligheid, infrastructuur en efficiëntie van de controlsystemen. [SPAN17] Daarom moeten IT-auditors de impact daarvan evalueren en controleren wanneer ze een audit uitvoeren op cloudomgevingen.

Cloudbeveiliging hoort een cruciaal onderdeel te zijn bij het ontwerpen en implementeren van cloud computing. Vertrouwelijkheid van data is een van de kwaliteitsaspecten die noodzakelijk is voor cloudbeveiliging. Daarom hebben user en providers de taak hun data

te beschermen tegen verlies en diefstal. Het is sterk aan te raden de data te versleutelen. Sterke encryptie met voldoende sleutelbeheer is een van de basismechanismen om de gegevens in de cloud te beschermen. De versleuteling zelf voorkomt geen dataverlies, maar biedt wel bescherming tegen ongeautoriseerd benaderen van data. Sleutelbeheer reguleert de toegang tot de middelen waarmee versleutelde data ontcijferd kan worden.

Cloudomgevingen kunnen worden gedeeld met andere gebruikers, bijvoorbeeld in een public cloud. Bovendien hebben de providers als leverancier in veel gevallen geprivilegieerde toegang tot de gegevens van de user. Dit soort situaties brengt extra veiligheidsrisico's met zich mee. Daarom is het noodzakelijk om een stelsel voor gegevensbescherming te hebben met toegangscontrole, contractuele aansprakelijkheid en encryptie. Hierdoor wordt de afhankelijkheid van providers verminderd bij beveiligingsincidenten zoals datalekken. [LEI10]

Encryptie en Sleutelbeheer

Encryptie is het door een algoritme met een sleutel omzetten van leesbare data in onleesbare vorm, cijfertekst, die alleen met de juiste sleutel weer leesbaar te maken is. Doel is de vertrouwelijkheid en privacy van die data te vergroten. De sleutel is de basis om data te versleutelen en sleutelbeheer heeft als doel ongeoorloofde decodering te voorkomen. De gebruikte cryptografische technieken gebruiken de sleutels die worden beheerd door cryptografische sleutelbeheer systemen (CSS) en bieden een niveau van beveiliging dat niet zichtbaar is voor de aanvaller. Het beveiligingsniveau van een encryptie-algoritme is simpelweg het aantal bewerkingen dat nodig is om de sleutel en daarmee encryptie te kraken. In praktijksituaties is ook het beheer van de sleutels medebepalend voor het beveiligingsniveau. Wie over de sleutel beschikt, heeft immers toegang tot de versleutelde data. [NIST13] Sleutelbeheer is daarom een cruciaal onderdeel bij het ontwerpen en implementeren van encryptie-oplossingen.

Aandachtspunten voor encryptie- en sleutelbeheeroplossingen

Voor een adequaat encryptie en sleutelbeheer is het nodig dat bedrijven bij hun besluiten over encryptie- en sleutelbeheeroplossingen rekening houden met relevante risico's. De aandachtspunten zijn:

1. **Risicobeoordeling en analyse van veiligheids- en privacyvereisten.** Het is lastiger om een systeem te veranderen nadat het operationeel is ingezet dan vooraf. Het is dus efficiënter en effectiever om alle mogelijke risico's zo vroeg mogelijk aan te

pakken. Daarom moeten de users allereerst de gevoeligheid van de data bepalen door een risicobeoordeling en veiligheidsanalyse. Daarop volgen dienovereenkomstige classificatie en labeling. Op basis hiervan weten de users welke data in aanmerking komen om te versleutelen en welke niet. De volgende stap is deze analyse en classificatie tot uiting te laten komen in de data-architectuur. Gegevensbescherming en encryptieprocedures moeten toelichten hoe data wordt beschermd en versleuteld op basis van bijbehorende labels en classificatie.

2. **Vastgesteld moet worden wie de encryptie-procedures zal toepassen, de user of de provider.** De belangrijkste vragen over de rollen zijn: wie zal de data versleutelen (user, provider of een derde partij)? Wie zal toegang hebben tot de sleutels en de versleutelde data? en Wie zal de toegang tot encryptiesleutels beheren, user, provider of beide?. [BUCH14] Duidelijke rollen, verantwoordelijkheden, taken en vereisten moeten in de contracten en serviceniveau-overeenkomsten (SLA's) tussen de user en de provider vastgesteld zijn. *Wie* de encryptiesleutels beheren zal en hoe, dat zijn de belangrijkste vragen. Deze elementen moeten grondig worden besproken en uiteindelijk is het aan de user om te bepalen welke opties het beste passen bij de eigen risicobereidheid en veiligheidseisen.
3. **Wat de kenmerken zijn van de sleutelbeheeroplossing.** De belangrijkste kenmerken van een sleutelbeheeroplossing zijn transparantie en helderheid van de IT-architectuur, veilige cryptografische technieken, flexibiliteit, kostenefficiëntie, interoperabiliteit met andere systemen en naleving van wet- en regelgeving. De gewenste kenmerken moeten in de besprekingen tussen de user en de provider aan de orde komen.

Dit zijn noodzakelijke aandachtspunten in het auditwerkprogramma van IT-auditors die een audit uitvoeren op de databeveiliging, encryptie- en sleutelbeheer bij cloudomgevingen.

Encryptie- en Sleutelbeheeroplossingen in de markt

Providers bieden encryptie-sleuteloplossingen om data te beveiligen in cloudomgevingen, of ze laten alle maatregelen aan de user. [LEI10] Omdat de logica achter encryptie- en sleutelbeheer bij de verschillende providers vergelijkbaar is, zijn de functies van deze producten grotendeels dezelfde en is er alleen verschil in de bewoordingen van de productbeschrijvingen van diverse providers . Zie bijvoorbeeld de oplossingen van Microsoft in tabel 1.

Oplossingen van Microsoft	Beschrijving
Server-side encryptie die gebruikmaakt van door de provider beheerde sleutels	Encryptie wordt uitgevoerd door de provider. De provider heeft volledige toegang tot de sleutels en volledige controle over sleutel- en levenscyclusbeheer.
Server-side encryptie die gebruikmaakt van klant-beheerde sleutels in een kluis (*key vault*) bij de provider.	Encryptie wordt uitgevoerd door provider. Azure Key Vault is de oplossing die Microsoft biedt om toegang tot sleutels te beheren.
Server-side encryptie die gebruikmaakt van klant-beheerde sleutels in hardware die de user zelf beheert.	Encryptie wordt uitgevoerd door provider. De sleutels zijn opgeslagen in een system dat geconfigureerd en beheerd wordt door de user zelf.
Klant-encryptie-model	Encryptie wordt uitgevoerd door user. Provider heeft geen toegang tot ontcijferde data.

Tabel 1: Microsoft Encryptie- en Sleutelbeheeroplossingen [MS20]

In alle oplossingen die providers aanbieden, zijn er verschillende niveaus van complexiteit op verschillende lagen van de informatiesystemen. Het niveau van complexiteit voor de user hangt ook af van de technische competenties van de user. Daarom is het cruciaal om de competenties en capaciteit van de user en haar medewerkers mee te nemen in de beslissing over verschillende oplossingen. De user moet beoordelen of er voldoende kennis in huis is om aan zijn verantwoordelijkheden te kunnen voldoen. Ook helpt het analyseren van de bestaande oplossingen voor gegevensbescherming om de haalbaarheid en kostenefficiëntie van de voorkeursoplossing te bepalen. Naast het adresseren van de hiervoor genoemde specifieke aandachtspunten voor encryptie- en sleutelbeheer, dient de user ook aandacht te schenken aan risicomanagement en wijzigingsbeheer tijdens het implementeren van encryptie- en sleutelbeheeroplossingen. Kortom, de user zouden de risico- en wijzigingsbeheer processen moeten volgen tijdens het implementeren van encryptie- en sleutelbeheeroplossingen.

Het is aan de providers om voor hun oplossingen *proof of concept* te leveren. Daar hoort bij dat ze vermelden welke user nog zullen moeten nemen. Bovendien is het cruciaal voor de user om te analyseren of er bepaalde vereisten zijn neergelegd in de wet- en regelgeving.

Relevante wet- en regelgeving en frameworks

Huidige wet- en regelgeving verwijst niet naar specifieke vereisten over encryptie- en sleutelbeheer. Maar het belang van vertrouwelijkheid van data wordt in veel wet- en regelgeving opgenomen, zoals in richtsnoeren van de Europese Bankautoriteit (EBA) en in de Algemene Verordening Gegevensbescherming (AVG). De user is verantwoordelijk om ervoor te zorgen dat gegevensbescherming ook in de cloudomgeving voldoet aan de vereisten van wet- en regelgeving. De user is hier juridisch verantwoordelijk voor en draagt

de financiële schade en reputatieschade als gevolg van gegevenslekken of niet beschikbaar zijn van data.

Frameworks zoals ISO -standaarden en COBIT kunnen gebruikt worden om inzicht te krijgen in de informatiebeveiligingsprincipes. In de NIST Special Publication 800-130 2013 over CKMS (cryptographic key management systems) zijn specifieke eisen aan sleutelbeheer-oplossingen opgenomen. De users kunnen van deze publicatie gebruikmaken om de componenten van sleutelbeheersystemen te beheersen, zie figuur 2.

Figuur 2: Key management lifecycle

Conclusie en consequenties voor IT-auditing

Er zijn cruciale aandachtpunten voor encryptie- en sleutelbeheeroplossingen. Deze zijn resultaten van risicobeoordeling, analyse van veiligheids- en privacyvereisten zoals gegevensclassificatie en labeling, gegevensbescherming en encryptieprocedures, duidelijke rollen, verantwoordelijkheden en taken. *Wie* zal de encryptiesleutels beheren en *hoe*, dat zijn de belangrijkste vragen. De verwachtingen aan een sleutelbeheeroplossing moeten ook worden vastgelegd tussen de user en de provider. Dit betreft transparantie en helderheid van de IT-architectuur, veilige cryptografische technieken, flexibiliteit, kostenefficiëntie, interoperabiliteit met andere systemen en naleving van wet- en regelgeving.

Het belang van veilige cloud computing vraagt om een prominente rol voor zowel externe als interne IT-auditors. Zij hebben de expertise om de user zekerheid te verschaffen over de processen en technische implementatie van encryptie- en sleutelbeheer. Ook ligt het op hun weg om te controleren of de user de risico's die in dit artikel zijn geschetst goed worden beheerst.

Zie tot slot een aantal praktische aanbevelingen in het tekstkader 'Praktische aanbevelingen voor IT-auditors'.

Samenwerking NOREA en VCO

- Controleer of de user afspraken heeft gemaakt met de provider over het naleven van het informatiebeveiligingsbeleid en indien van toepassing de uitvoering van het informatiebeveiligingsplan van de user. [DNB19]
- Controleer of de user een risicobeoordeling heeft uitgevoerd voor de clouddiensten. De user moet bijsturen wanneer haar risicotoleranties worden overschreden. [DNB19]
- Controleer of de verantwoordelijkheden en aansprakelijkheden van de user en de provider zijn opgenomen in de processen en SLA's. De user moet serviceniveaurapportages (SLR's) en/of assurancerapportages ontvangen met de juiste scope en diepgang, aan de hand waarvan die afspraken kunnen worden gemonitord. [DNB19]
- Controleer of de kenmerken van de sleuteloplossing afgewogen worden door de user.
- Controleer of het encryptiemodel voorziet in de behoeften van de user.

Verder kunnen IT-auditors ook veilig cloudgebruik bevorderen door:

- Encryptie- en sleutelbeheerrisico's op te nemen in het audit universe.
- Het management te helpen om de kwetsbaarheden rond encryptie- en sleutelbeheer te identificeren door audit- en consultingopdrachten uit te voeren.
- De genomen technische maatregelen te evalueren in verschillende lagen van de infrastructuur.
- Bij het bestuur de belangrijkste blootstellingen aan encryptie- en sleutelbeheer en de noodzakelijke mitigerende maatregelen onder de aandacht te brengen.

Literatuur

[AWS20] Amazon Web Services. *The definition of Cloud Computing*, 2020. https://aws.amazon.com/what-is-cloud-computing/. Geraadpleegd op 16 september 2021.

[BUCH14] Buchade, Ingle. Key Management for Cloud Data Storage: Methods and Comparisons. *2014 Fourth International Conference on Advanced Computing & Communication Technologies (ACCT)*, 2014.

[DNB19] DNB. *Good Practice: Informatiebeveiliging 2019/2020*, 2019. https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf. Geraadpleegd op 16 september 2021.

[ISACA19] ISACA. *Cloud Computing: Business Benefits And Security, Governance and Assurance Perspectives. Emerging Technology White Paper*, 2009.

[LEI10] Lei, Zishan, Jindi. Research on Key Management Infrastructure in Cloud Computing Environment. *2010 Ninth International Conference on Grid and Cloud Computing*, 2010.

[MS20] Microsoft. *Gegevensversleutelingmodellen*, 2020. https://docs.microsoft.com/nl-nl/azure/security/fundamentals/encryption-models. Geraadpleegd op 16 september 2021.

[NIST13] NIST. *800-130 A Framework for Designing Cryptographic Key Management Systems*, 2013. NIST Special Publication 800-130. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf. Geraadpleegd op 16 september 2021.

[SHAH 14] Shahzad, F. State-of-the-art survey on cloud computing security challenges, approaches and solution, *Procedia Computer Science*, 2014. https://www.sciencedirect.com/science/article/pii/S1877050914010187, geraadpleegd op 8 september 2021.

[SPAN17] Konstantina Spanaki, Zeynep Gürgüç, Catherine Mulligan, Emil Lupu. 2017, *Organizational cloud security and control: a proactive approach*. Loughborough University, 2017.

Gülnur Orpak RE, CISA, CIA, ISO27001LA | Manager Technical IT Audit bij *ABN Amro*

Gülnur Orpak is Technical IT Audit Manager bij ABN Amro en heeft meer dan tien jaar ervaring in financiële markten. Ze heeft diverse auditwerkzaamheden uitgevoerd bij verschillende financiële instellingen, onder andere op het gebied van informatiebeveiliging, netwerkbeveiliging, encryptie, digitalisatie, DevOps, API-beveiliging en PSD2. Gülnur is lid van IIA Nederland en ISACA NL Chapter.