DataNavigator

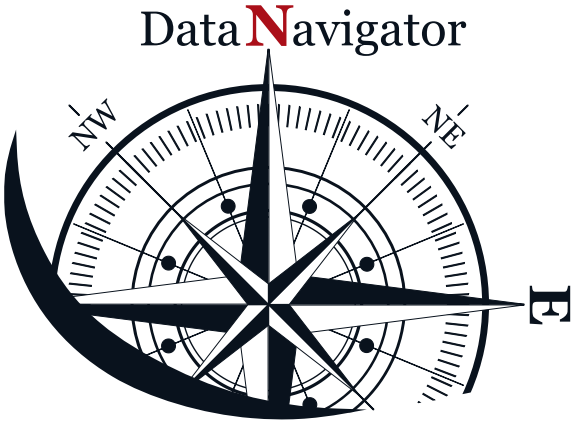
www.datanavigator.de | ISSN 2702-1904

CIEM – Cloud Infrastructure Entitlements Management

Luca Winters

#11 | Mai 2022

EUROGROUP CONSULTING



Das Thema ‚Berechtigungs- und Identitätsmanagement' hat im Finanzdienstleistungssektor insbesondere durch die Zunahme von Cybersecurity-Events an Bedeutung gewonnen. Im eigenen Sicherheitsinteresse, aber auch im Fokus der regulatorischen Rahmenbedingungen, haben Banken und Versicherungen hier mittlerweile entsprechende IAM-Lösungen im Einsatz, um ein Identity and Access Management (IAM) zu gewährleisten. Gleichzeitig sind Finanzdienstleister allerdings auch dabei zumindest einen Teil ihrer IT-Infrastruktur in die Cloud zu verlagern. Die etablierten IAM-Lösungen sind hiermit aber oftmals überfordert. Eine weitergehende Berechtigungssteuerung im Cloud-Kontext ist erforderlich. CIEM, also das Cloud Infrastructure Entitlements Management, spielt hier eine entscheidende Rolle, wenn es um die Berechtigungssteuerung bei Cloud-Dienstleistungen geht.

Da die Systemlandschaften von Finanzdienstleistern immer komplexer und schnelllebiger werden, steigen auch die Anforderungen an die IAM-Systeme. Als entsprechende System-klassifizierung wurden von Gartner CIEM-Systeme benannt, welche aber aktuell noch am Anfang des Hype Cycle Cloud-Security stehen. Ob der Themenbereich bis zur Produktionsreife gelangt, ist zum aktuellen Zeitpunkt fraglich.

Ziel dieses Artikels ist die Vorstellung von CIEM-Systemen sowie die kritische Diskussion, ob eine Erweiterung des IAM-Systems überhaupt notwendig ist. Zudem werden mögliche Vorteile, welche bei der Einführung von CIEM-Systemen genutzt werden können, beleuchtet.

Was verbirgt sich hinter CIEM?

Mit CIEM werden die Zugriffe und Rechte von Nutzer:innen insbesondere in verteilten, dynamischen und hybriden (Cloud-)Umgebungen transparent gemacht. Nutzer können dabei auch Applikationen oder einzelne Services sein, die auf Anwendungen oder Datenbanken in der Cloud zugreifen müssen. Das CIEM-System bietet vorgefertigte Schnittstellen zu allen relevanten Cloud-Anbietern und liefert in Echtzeit konsistente Berechtigungs- und Zugriffsinformationen hinsichtlich Anwendungen und Daten. CIEM-Systeme sind derzeit noch nicht flächendeckend im Einsatz, da sich die Anforderungslage an entsprechende komplexe Systeme aktuell erst herausbildet und schärft.

Wofür braucht man noch eine weitere Berechtigungssteuerung? Der Einsatz eines CIEM-Tools scheint bei der oftmals bereits voll ausgeprägten und im Einsatz befindlichen Identitäts- und Zugriffssteuerung (Identity and Access Management - IAM) überflüssig. Aktuell - für ein primär intern kontrollierbares „on premise"-Umfeld (die technischen Ressourcen sind direkt bei dem Unternehmen allokiert) - ist dies auch richtig. Die meisten Institute verfügen über ein für ihre Bedürfnisse optimiertes IAM-Tooling oder schaffen dies kurzfristig mittels geeigneter Projekte. Doch mit sich wandelnden Möglichkeiten und Anforderungen der Technologie sind auch diese Kontrollanwendungen entsprechend anzupassen.

Gründe für die Einführung eines CIEM

Folgende drei Gründe liegen dabei der künftig notwendigen CIEM-Einführung zugrunde:

Verlagerung der Bankaktivitäten in die Cloud

Als eine der letzten Branchen in der DACH-Region führen Finanzdienstleister breitflächig Cloud Computing ein. Dieser späte Einstieg liegt zum einen an den regulatorischen Herausforderungen, zum anderen an der (korrekten) datenprotektionistischen Haltung der Institute. Nach einigen Pilot-Anwendungen und kleineren Testaktivitäten hat ein Großteil der Institute nun Teile der eigenen IT in die Cloud ausgelagert. Meist wurde hierbei ein strategischer Anbieter für die Zusammenarbeit gewählt, mit einem weiteren Provider gemäß der jeweiligen Exit-Strategie. Zukünftig werden die Cloud-Anbieter noch stärker auf Zertifizierungen für die Finanzbranche setzen, was zu einem erleichterten Bezug der jeweiligen Cloud Services führen sollte. Durch Anwendungen wie „Red Hat Open Shift", ein System zur Erstellung und Lastverteilung von Linux-basierten Containern, ist es zudem möglich, Provider-unabhängig Anwendungen in der Cloud zu deployen. Dies hat zur Folge, dass Anwendungen aufgrund tagesaktueller Preise zwischen den Cloud-Anbietern hin- und hergeschoben werden können. In diesem Moment ist es aus IT-Security-Sicht essenziell, Anbieter- und Technologie-übergreifende, konsistente Rollen und Rechte zu vergeben.

Zunehmende Autonomie der Fachbereiche

Durch SaaS- und Low-Coding Anwendungen sind die Fachbereiche in der Lage, auch ohne Mitwirkung der IT neue Lösungen für ihre Anforderungen aufzubauen. Dies kann im schlimmsten Fall ohne Kenntnis des IT-Bereichs geschehen (sog. Schatten-IT), im besten Fall aufgrund der strategischen Ausrichtung. Besonders Cloud-Anwendungen sind dabei für die Fachbereiche attraktiv, da die Bereitstellung innerhalb weniger Minuten erfolgen kann und die Abrechnung im „Pay-per-Use"-Modell funktioniert. Um eine adäquate Umsetzung der IT-Security-Standards sicherstellen zu können, ist die (Teil-)Automatisierung der entsprechenden Anwendungen sinnvoll, zumal die meisten Fachbereiche nicht über die entsprechenden IT-Sicherheitskenntnisse verfügen. Die Anwendungen sollten dabei idealerweise direkt auf die firmenspezifischen Nutzerkonten bei den Cloud-Anbietern zugreifen können.

Multiplikation der Komplexität von Anwendungen und Daten

In der heutigen Zeit stehen Unternehmen potenziell eine größere Menge an zu verarbeitenden Daten zur Verfügung, unabhängig davon in welcher Form (unstrukturiert, semi-strukturiert oder strukturiert) diese vorliegen. Zusätzlich nimmt die Dynamik der eingesetzten Ressourcen zu, da die Cloud-Anbieter den flexiblen Einsatz der jeweiligen Server automatisiert bestimmen. Durch

die Kombination beider Faktoren potenziert sich die Menge und Variabilität der durch Rechte (für Personen, Applikationen oder technische Identitäten) zu verwaltenden Ressourcen in der Cloud (Server, Speicher, Datenbanken, Geschäftsanwendungen, Portale, Administrationskonsolen und Sicherheitseinrichtungen). Banken und Versicherungen müssen zwingend die Kontrolle über diese Zugriffe behalten. Dies kann in einer automatisierten Welt ebenfalls nur durch Automatismen erfolgen - durch die steigende Automatisierung im IT-Betrieb ist eine zeitgerechte Reaktion bezüglich des Rechtemanagements notwendig. Dies gilt insbesondere für die Anpassung von Rechten in dynamischen Multi-Cloud-Umgebungen. Mangelnde Sichtbarkeit und Transparenz von vergebenen Rechten in dynamischen, verteilten Cloud-Umgebungen sind hier ebenso gefährlich wie langwierige manuelle Prozeduren für Demand Management, Genehmigung, Umsetzung und Überprüfung.

Aus diesem Grund ist die Anpassung der IAM-Landschaft künftig zwingend notwendig. Hierbei kann ein CIEM-Tool bei entsprechender Cloud-Nutzung sinnvoll sein. Die Anwendung agiert dabei nach dem Prinzip der „minimalen Berechtigung“ (Least Privilege/Zero Trust Security Model). Mitarbeitende erhalten nur Zugriff auf Daten, welche Sie für die Tätigkeiten in ihrer aktuellen Rolle und Aufgabe benötigen. Dies sichert den Schutz gegen Datendiebstahl, bösartige Angriffe und weitere Risiken, die sich aus zu umfangreichen und nicht beherrschten Zugriffsrechten ergeben.

Weitere Vorteile beim Einsatz von CIEM-Lösungen und Sichtweise auf den Markt

Im Gegensatz zu traditionellen IAM-Anwendungen sind

- die Entwicklungszyklen von CIEM-Lösungen deutlich kürzer und
- die Anbindungsmöglichkeiten bestehender Services vielfältiger - beispielsweise ist eine AI-Unterstützung für die Analyse bestehender Rechte und der damit verbundenen Rezertifizierungen möglich - da die meisten AI-Anbieter ihre Services direkt auf entsprechenden Cloud Plattformen anbieten.

Da aktuell die oben geschilderten Prämissen (Verlagerung in die Cloud, Autonomie der Fachbereiche und Multiplikation von Komplexität) für den vollständigen Einsatz eines CIEM-Systems noch nicht gegeben sind, ist das Themenfeld auf dem Markt noch nicht so weit verbreitet. Dies liegt an der fehlenden Durchdringung eines Multi-Cloud-Ansatzes im FDL-Sektor. Es ist jedoch davon auszugehen, dass künftig Anbieter die entsprechenden Anwendungen, welche automatisiert Berechtigungen im Cloud-Umfeld managen, bereitstellen werden. Aller Wahrscheinlichkeit nach werden dies nicht die Cloud-Anbieter selbst sein, da diese kein Interesse an der Aufhebung eines Vendor-Lock-Ins auf der eigenen Plattform haben, sondern spezialisierte „Multi-Cloud-Broker“.

Die zunehmende Autonomie der Fachbereiche und Technologie erfordert zudem die Anpassung des organisatorischen Umgangs im Berechtigungsmanagement. Dies ist individuell in den Unternehmen zu prüfen und zukunftsgerichtet aufzubauen.

Als Fazit lässt sich somit festhalten, dass eine frühzeitige Beschäftigung mit der Berechtigungssteuerung in der Cloud-Infrastruktur sinnvoll ist. CIEM ist dabei nicht als

vorübergehender Hype einzustufen, sondern stellt eine notwendige Erweiterung des Berechtigungs- und Identitätsmanagements dar.

Luca Winters ist Experte für IT-Strategie und Cloud Computing. Mit über 5 Jahren Beratungserfahrung steht er Kunden aus dem Banken- und Versicherungsumfeld als Trusted Advisor zur Verfügung. Als Leiter des EGC Cloud Competence Center setzt sich Herr Winters kritisch mit neuen cloudbasierten Themenbereichen auseinander.

Bisher erschienen:

#1 Dr. Marco Weiß – *Welt und Wesen des Datenmanagements*; September 2020

#2 Mario Kubik – *„DLT" – Potenzial zur Zukunftstechnologie?*; November 2020

#3 Jonathan Misler – *Verwendung von Daten und Modellen in datengetriebenen Geschäftsmodellen*; Januar 2021

#4 Johannes Bänsch – *Data Analytics und die Cloud*; März 2021

#5 Kurt Tanneberger – *Ja, wo sind sie denn? – Daten im IT-Betrieb*; Mai 2021

#6 Thomas Tiebor – *Data Governance als Fundament guten Datenmanagements;* Juli 2021

#7 Dr. Marco Weiß – *Artificial Intelligence – Nature or Nurture?*; September 2021

#8 Binjamin Sancar, Hermann Sgardelli – *Vertriebschancen in einer Bank durch Nutzung ihrer Daten und ihres Ökosystems;* November 2021

#9 Abdalla El Kadi – *Datenvisualisierung – eine Geschichte in Bildern;* Januar 2022

#10 Carsten Kuhlmann – *Kundenfokussierung: Daten und Technik*; März 2022

#11 Luca Winters – *CIEM – Cloud Infrastructure Entitlements Management*; Mai 2022

#12 Kristian Buric – *Der Informationsverbund - Daten (nur) für die Aufsicht?*; Juli 2022

#13 Stefan Bauer – *Aufbau eines SOC (Security Operations Center) als Kommandozentrale zur Cyberabwehr*; September 2022

#14 Thomas Tiebor – *Der Charme von IT-Datenarchitekturmustern;* November 2022

#15 Dr. Marco Weiß – *Citius, Altius, Fortius – Daten im Sport*; Januar 2023

#16 Simon Wilmerding – *Daten statt (nur) Bauchgefühl – Mit Datenanalysen den War for Talent gewinnen*; März 2023

#17 Kay Helbig – *ESG-Berichterstattung bei Versicherungen*; Mai 2023

#18 Dr. Marco Weiß – *Daten und Modelle in der 7. MaRisk-Novelle*; Juli 2023

#19 Fabio Giacomo Müller – *Softwareeinführungsprojekte im internationalen Kontext*; September 2023

#20 Stefan Bauer – *Digital Operational Resilience Act (DORA): Wie hoch wird die nächste Welle der Regulierung?*; November 2023

#21 Prof. Dr. Hans-Gert Penzel – *Tokenisierung von Vermögenswerten: Wie die Zukunft des Eigentums aussehen wird*; Januar 2024

Über den DataNavigator

Unterschiedliche Autoren beleuchten in der Reihe DataNavigator die vielfältigen Facetten des Datenmanagements und zeigen Ihnen interessante Aspekte auf.

Der DataNavigator wird von Eurogroup Consulting regelmäßig zweimonatlich herausgegeben und möchte Ihnen interessante Denkanstöße liefern. Wir freuen uns, Ihnen mit dem DataNavigator unsere Erfahrungen weiterzugeben und stehen Ihnen für die Diskussion gerne zur Verfügung!

Sie erreichen Autoren und Herausgeber bei Anregungen und Feedback unter der E-Mail-Adresse datanavigator@eurogroupconsulting.de.