Industry Cloud Platform: Identitäts- und Zugriffsverwaltung in einer Cloud-Umgebung

Studiengang: MAS Cyber Security

Die Firma Deleproject AG entwickelt ein System zur erweiterten Datenerfassung und -analyse von Maschinen in der Prozessindustrie. Die verteilte Architektur, welche vom Maschinennetz bis zur Cloud-Umgebung reicht, erfordert eine solide Lösung zur Verwaltung von Identitäten und Zugriffsrechten.

Ausgangslage

Die Deleproject AG entwickelt ein System namens „Industry Cloud Platform“ zur erweiterten Erfassung und Auswertung von produktionsrelevanten Daten in der Prozessindustrie. Die Daten werden dabei mit Edge-Gateways auf der Maschinenebene erfasst und anschliessend in einer Cloud-Umgebung weiterverarbeitet, ausgewertet und dargestellt. Der Anspruch an eine moderne und modulare Architektur führt zur Nutzung von Software-as-a-Service (SaaS) und resultiert in einer umfangreichen Cloud-Architektur. Diese umfangreiche Architektur, kombiniert mit der Vielfalt von Ressourcen und Identitäten, stellt eine grosse Herausforderung für die Identitäts- und Zugriffsverwaltung dar.

Zielsetzung

Im Rahmen dieser Arbeit wird die Entwicklung eines zentralen Identity and Access Management System (IAM-System) mit Microsoft Entra als Identity Provider für die Industry Cloud Platform angestrebt, welches die Integration der verschiedenen Architekturkomponenten ermöglicht. Das Ergebnis soll aufzeigen, inwiefern die unterschiedlichen Elemente der Plattform effektiv in ein zentrales IAM-System integriert werden können und so eine solide Zugriffssteuerung und Identitätsverwaltung für die Industry Cloud Platform realisiert werden kann.

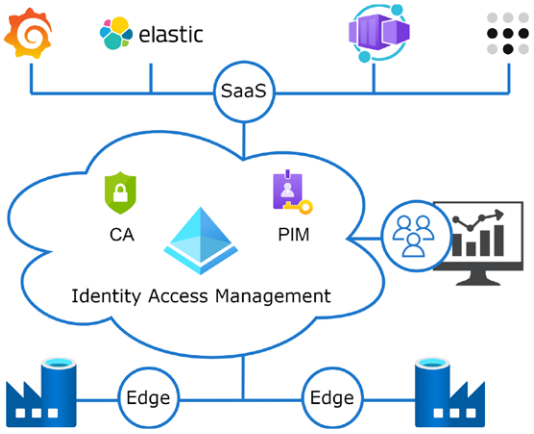
Vorgehen

Im Zuge einer Anforderungsanalyse wurden 37 spezifische Anforderungen erarbeitet, basierend auf einer internen Stakeholder Analyse sowie dem „IKT-Minimalstandard Assessment“ vom BWL und dem „eCH-0107 Standard“ für föderierte IAM-Systeme.
In der darauffolgenden Konzeptphase wurden die zentralen Architekturkomponenten Azure, Grafana, Elastic, Confluent, InfluxDB und Tailscale untersucht, um ein umfassendes Integrationskonzept und Berechtigungsmodell entwickeln zu können und die Einbindung externer Mandanten zu ermöglichen.
In der letzten Phase wurde das Konzept praktisch umgesetzt, fiktive Kundenunternehmen integriert und alle Funktionen sowie Anforderungen auf Erfüllung geprüft und dokumentiert.

Ergebnis

Während der Umsetzungsphase wurden verschiedene Limitationen zur Integrationsfähigkeit der einzubindenden SaaS-Dienste gefunden und aufgezeigt. Dank der flexiblen IAM-System Gestaltung konnten viele dieser Limitationen durch gezielte Anpassungen des ursprünglichen Konzeptes kompensiert werden. Insgesamt entstand ein solides IAM-System, welches die Zusammenarbeit mit externen Mandanten unter minimalem Konfigurationsaufwand ermöglicht. Alle geprüften SaaS-Dienste, mit Ausnahme von InfluxDB, konnten erfolgreich in das IAM-System integriert werden und sind so Teil der zentralen Berechtigungsverwaltung. Durch die Verwendung moderner Authentifizierungsmethoden und Sicherheitsmechanismen wie «Privileged Identity Management» (PIM) und «Conditional Access» (CA) konnte ein IAM-System entwickelt werden, welches alle obligatorischen Anforderungen erfüllt und relevante Sicherheitsprinzipien berücksichtigt.

Julian Friederich
MAS Cyber Security



Komponenten der Industry Cloud Platform