IHK Industrie- und Handelskammer zu Leipzig

Winterprüfung 2023

Ausbildungsberuf
Fachinformatiker/Fachinformatikerin (VO 2020) Fachrichtung: Systemintegration

Prüfungsbezirk
Leipzig FISY 1 (AP T2V1)

Melissa Futtig
Identnummer: 886355
Prüflingsnummer: 52065
E-Mail: mfuttig@deloitte.de, Telefon: +49 1575283 33896

Ausbildungsbetrieb: Deloitte GmbH Wirtschaftsprüfungsgesellschaft
Projektbetreuer: Edgar Kapler
E-Mail: ekapler@deloitte.de, Telefon: +49 1515448 4702

Thema der Projektarbeit
Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

1 Thema der Projektarbeit

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

2 Geplanter Bearbeitungszeitraum

Beginn: 30.10.2023
Ende: 10.11.2023

3 Ausgangssituation

In der Deloitte Wirtschaftsprüfungsgesellschaft GmbH wird die Sicherheit des Zugriffs auf verschiedene Dienste innerhalb einer Cloud-Infrastruktur verbessert, indem Multi-Faktor-Authentifizierung (MFA) eingeführt wird. Dies geschieht, um eine erhöhte Sicherheit für firmeninterne und kundenbezogene Daten zu gewährleisten.

Ist-Analyse

Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH verwendet die Cloud-Infrastruktur von OVHcloud, um einen Business Hosting Service bereitzustellen.
In dieser Konfiguration wird der Firewall eine öffentliche IP-Adresse zugewiesen. Das private Netzwerk enthält alle anderen Services und Instanzen und wird von der Firewall geschützt.
Eine Kontrollinstanz, namens „control_node“, ermöglicht den Zugriff auf alle anderen Instanzen, die sich im privaten Netzwerk befinden.

Die Cloud-Infrastruktur ist in vier Hauptbereiche unterteilt, in denen verschiedene Services/ Dienste bereitstellt werden:

A) Compliance and Security Stack
- Bereich für Compliance und Sicherheit
- Hierzu gehören eine OPNsense Firewall, ein Nginx Proxy Manager, der als reverse Proxy für das HTTP-Protokoll dient und andere Ports als Stream weiterleitet, der Guacamole Server und das Open-Source-Sicherheitstesttool Infection Monkey

B) Monitoring
- Überwachungsbereich aller vorhandenen Dienste der Cloud-Infrastruktur
- Beinhaltet die Open-Source-Software Grafana, Uptime Kuma als Webserver und Healthecks

C) DevOps
- Bereich für die Entwicklung und Bereitstellung von Anwendungen
- Enthält die kollaborative Entwicklungsplattform Gitlab, Nexus zur Verwaltung von Repositories, Sonarqube für die statische Analyse und Bewertung von Quelltextqualität, sowie

SFTPGo für die Authentifizierung mit öffentlichen Schlüsseln, SSH-Schlüsseln und Passwörtern

D) E-Mail
- E-Mail-Bereich
- Umfasst den Mail-Server Mailcow und SOGO für die E-Mail-Kommunikation

Der Zugriff auf die o.g. Dienste erfolgt durch die Eingabe eines Nutzernamens und eines Passworts. Dies erzeugt eine potenzielle Sicherheitslücke und macht die Dienste unserer Cloud-Infrastruktur anfälliger für Phishing-Angriffe und unbefugten Zugriff.

Soll-Konzept

Durch die Implementierung des MFA in der Cloud-Infrastruktur bei der Deloitte Wirtschaftsprüfungsgesellschaft GmbH soll durch das Hinzufügen einer weiteren Sicherheitsebene, Datenschutz und Integrität gewährleistet werden.

Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH kann in alle Cloud-Services MFA integrieren, sodass durch dieses eine zusätzliche Sicherheitsebene aktiviert wird.

Vorgang:

Zu Beginn erfolgt die Passworteingabe des Nutzers. Unter der Voraussetzung der Korrektheit, erhält dieser einen Sicherheitscode per SMS, E-Mail oder einer App, welcher eingegeben wird und zu einer erfolgreichen Anmeldung führt.
Mehrere fehlgeschlagene MFA-Versuche führen zu einer Sperrung des Kontos oder erfordern eine Rücksetzung durch den Administrator.

4 Projektziel

Das Hauptziel des Projekts besteht darin, die Sicherheit der Cloud-Infrastruktur der Deloitte Wirtschaftsprüfungsgesellschaft GmbH bei der Zugriffskontrolle auf die o.g. Services zu erhöhen, indem Multi-Faktor-Authentifizierung (MFA) eingeführt wird.

Dabei steht im Vordergrund das Ziel der Risikominimierung durch die Einführung einer zusätzlichen Authentifizierungsebene. Nur unter der Voraussetzung des zweiten Faktors kann eine erfolgreiche Anmeldung erfolgen.

Um die Arbeitsabläufe der Mitarbeiter nicht zu beeinträchtigen, wird darauf geachtet, die Benutzerfreundlichkeit aufrechtzuerhalten und die MFA-Lösung darauf zugeschnitten.

Die technische Umsetzung von Sitecars (Single Sign-On with Integrated Credential and Authentication System) für MFA ist eine effektive Methode, um die Sicherheit von Zugriffskontrollen auf verschiedene Services in unserer Cloud-Infrastruktur zu verbessern.

Diese Methode ermöglicht eine zentrale Verwaltung von Benutzeranmeldungen und -authentifizierung, wobei MFA eine zusätzliche Sicherheitsebene hinzufügt. Die Implementierung erfolgt in Docker-Container und ermöglicht eine einfache Bereitstellung und Portabilität zwischen verschiedenen Umgebungen.

Folgende Kriterien sollen erfüllt werden:

A) IT-Sicherheit
- Minimierung von Risiken, wie Passwort-Leaks und Phishing
- Anmeldung ist nur mit MFA möglich

B) Reibungsloser Benutzerzugriff
- Nutzerauthentifizierung, um Zugriff auf die o.g. Services zu erhalten
- Anmeldung/ Sperrung des Nutzers

C) Compliance
- Erfüllung von Sicherheits- und Datenschutzstandards

5 Zeitplanung

Planungsphase 5h
- Erstellen einer Ist-Analyse
- Erstellen einer Soll-Analyse
- Kostenplanung
- Projektumfeld
- Kosten- und Nutzanalyse
- Gantt-Diagramm
- Klärung der Projektziele

Implementierungsphase 14h
- Auswahl einer MFA-Lösung
- Installation und Konfiguration von Sitecars
- Konfiguration der MFA
- Integration mit Cloud-Diensten

Testphase 6h
- Überwachung der Laufzeit der Services
- Überprüfung/ Beseitigen von Fehlern
- Zugrifftests

Einführung und Übergabe 4h
- Ausführung und Ergebnisübergabe
- Schulung der zu Beteiligten für die Nutzung

Dokumentation 6h

- Erstellung einer Projektdokumentation der Ergebnisse
- Erstellung einer Entwicklerdokumentation

Gesamt: 35h

6 Anlagen

keine

7 Präsentationsmittel

- Laptop
- Beamer
- 5 Ausdrucke der Präsentation für den Notfall
- Ladekabel Laptop
- HDMI-Kabel
- USB-C Kabel
- PowerPoint

8 Hinweis!

Ich bestätige, dass der Projektantrag dem Ausbildungsbetrieb vorgelegt und vom Ausbildenden genehmigt wurde. Der Projektantrag enthält keine Betriebsgeheimnisse. Soweit diese für die Antragstellung notwendig sind, wurden nach Rücksprache mit dem Ausbildenden die entsprechenden Stellen unkenntlich gemacht.

Mit dem Absenden des Projektantrages bestätige ich weiterhin, dass der Antrag eigenständig von mir angefertigt wurde. Ferner sichere ich zu, dass im Projektantrag personenbezogene Daten (d. h. Daten über die eine Person identifizierbar oder bestimmbar ist) nur verwendet werden, wenn die betroffene Person hierin eingewilligt hat.

Bei meiner ersten Anmeldung im Online-Portal wurde ich darauf hingewiesen, dass meine Arbeit bei Täuschungshandlungen bzw. Ordnungsverstößen mit „null“ Punkten bewertet werden kann. Ich bin weiter darüber aufgeklärt worden, dass dies auch dann gilt, wenn festgestellt wird, dass meine Arbeit im Ganzen oder zu Teilen mit der eines anderen Prüfungsteilnehmers übereinstimmt. Es ist mir bewusst, dass Kontrollen durchgeführt werden.

9 Grund für „mit Auflage genehmigt“

Guten Tag Melissa Futtig,
bitte achten Sie darauf, dass Ihre ”Projektdokumentation der Ergebnisse” auch die Projektarbeit für den Prüfungsauschuss wiederspiegelt. In der Fachhrichtung Systemintegration wird keine Entwicklerdokumentation erwartet, aber eine Kunden- und/oder Benutzerdokumentation (siehe

Handreichung der IHK https://www.leipzig.ihk.de/mb-04-112/). Unglücklich ist die ”Klärung der Projektziele” am Ende der Planung. Berücksichtigen Sie gegebenenfalls, dass Ihnen nach neuer Verordnung 40 Stunden für die Projektarbeit zur Verfügung stehen.