LU05b - Authentifizierung als Service

Bei der Authentifizierung als Service (AaaS) wird die Authentifizierungsfunktion von einem dedizierten Dienst bereitgestellt. Dieser Dienst wird von verschiedenen Anwendungen und Systemen innerhalb einer verteilten Umgebung genutzt.

Authentifizierung als Service (AaaS) zielt darauf ab, die Sicherheit und Zugriffskontrolle in einem verteilten System zu gewährleisten. Dazu stellt der Service die Dienste zur Überprüfung der Identität (Authentisierung, Authentifikation) bereit.

Wichtige Merkmale und Aspekte

Durch die Bereitstellung von Authentifizierung als Service können Organisationen die Komplexität der Authentifizierung in verteilten Umgebungen reduzieren, Sicherheitsrisiken minimieren und die Benutzererfahrung verbessern, indem sie einen zentralisierten und robusten Mechanismus für Identitätsüberprüfung bereitstellen.

Zentrale Verwaltung von Identitäten

Der Authentifizierungsdienst verwaltet Identitätsinformationen wie Benutzernamen, Kennwörter, Zertifikate oder biometrische Daten zentralisiert. Dadurch müssen Anwendungen diese Informationen nicht lokal speichern.

Standardisierte Protokolle und Schnittstellen

AaaS stellt standardisierte Schnittstellen und Protokolle bereit, die von verschiedenen Anwendungen und Systemen verwendet werden können, um sich gegenüber dem Authentifizierungsdienst zu authentifizieren und Identitätsinformationen abzurufen.

Sicherheitsmechanismen

Der Authentifizierungsdienst implementiert Sicherheitsmechanismen wie Verschlüsselung, sichere Kommunikationsprotokolle und Überprüfung von Zugriffsberechtigungen, um die Integrität und Vertraulichkeit der übertragenen Identitätsdaten zu gewährleisten.

Skalierbarkeit und Flexibilität

Da der Dienst zentralisiert ist, kann er leicht skaliert werden, um den Anforderungen von verteilten

Systemen gerecht zu werden. Er kann auch flexibel konfiguriert werden, um verschiedene Authentifizierungsverfahren und -richtlinien zu unterstützen.

Single Sign-On (SSO)

AaaS kann Single Sign-On-Funktionen bereitstellen, die es Benutzern ermöglichen, sich einmalig zu authentifizieren und dann nahtlos auf verschiedene Dienste und Anwendungen innerhalb des verteilten Systems zuzugreifen, ohne sich erneut anmelden zu müssen.

Protokollierung und Überwachung

Der Authentifizierungsdienst bietet Funktionen zur Protokollierung und Überwachung von Authentifizierungsaktivitäten, um Sicherheitsvorfälle zu erkennen, Compliance-Anforderungen zu erfüllen und die Systemintegrität zu überwachen.

Authentifizierung am BZZ

Als Lernende oder Lernender am BZZ nutzt du einige unterschiedliche Dienste:

- BZZ-Intranet
- Moodle
- Office 365
- OneDrive / Sharepoint
- Teams
- …

Alle diese Dienste verwenden einen gemeinsamen Authentifikationsservice von Azure AD. Dadurch brauchst du nicht für jeden Dienst ein eigenes Benutzerkonto mit Benutzername, Passwort und Authenticator. Zusätzlich entfällt das separate Anmelden bei jedem Dienst.

Für das BZZ entfällt der Aufwand pro Dienst ein eigenes Verzeichnis von Benutzern zu unterhalten.

Wieso muss ich mich trotzdem mehrmals anmelden?

Besonders wenn ich eine Weile keinen Dienst am BZZ genutzt habe, z.B. nach den Ferien, muss ich mich teilweise vier- oder fünfmal anmelden. Da frage ich mich schon, was es mit dem angeblichen Single Sign on zu tun hat.

Single Sign on gilt nur für eine bestimmte Umgebung. Melde ich mich im Brave-Browser bei einem Dienst erfolgreich an, so kann ich in Brave weitere Dienste ohne Login nutzen. Aus Sicherheitsgründen darf aber der Brave-Browser die Authentifizierung nicht mit anderen Browsern oder Applikationen austauschen.

M321-LU06

Marcel Suter

From:
https://wiki.bzz.ch/ - **BZZ - Modulwiki**

Permanent link:
https://wiki.bzz.ch/modul/m321/learningunits/lu05/authservice

Last update: **2024/03/28 14:07**