THM TECHNISCHE HOCHSCHULE MITTELHESSEN | CAMPUS FRIEDBERG | MND Mathematik, Naturwissenschaften und Datenverarbeitung

Proseminar 1
Dozent: Armin Wiechmann
Sommersemester 2024

Seminararbeit zum Thema:

Die Rolle von Identity und Authentication in Kontext IT Security

Student: Silas Lüdtke
E-Mail: silas.luedtke@mnd.thm.de
Matrikelnummer: 5332443

Abstract

Unternehmen stehen aufgrund der wachsenden Vernetzung und Digitalisierung von Geschäftsprozessen vor neuen Problemen im Zusammenhang mit der IT-Sicherheit. Es ist besonders wichtig, Identitäten zu verwalten und Nutzer zu authentifizieren, um den Zugriff auf sensible Daten und Systeme zu überwachen und vor unautorisiertem Zugriff zu schützen. Im Rahmen der IT-Sicherheit werden in dieser Studie die unterschiedlichen Verfahren und Vorgehensweisen zur Identitätsprüfung und Authentifizierung analysiert. Der Schwerpunkt liegt dabei auf der Untersuchung gegenwärtiger Entwicklungen wie der dezentralisierten Identität, der Authentifizierung ohne Passwörter und der Verwendung von künstlicher Intelligenz bei der Authentifizierung. Um den zunehmenden Gefahren im digitalen Zeitalter wirksam entgegenzuwirken, betont die Seminararbeit die Wichtigkeit einer umfassenden Sicherheitsstrategie, die Identitätsmanagement und Authentifizierung als zentrale Bestandteile einbezieht.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die Anforderungen an die IT-Sicherheit haben sich in den vergangenen Jahren deutlich erhöht, da sich die Informationstechnologie rasch weiterentwickelt und Systeme und Daten immer mehr miteinander verbunden haben. Es ist heutzutage dringender als je zuvor, sensible Daten vor unbefugtem Zugriff zu schützen. Authentication und Identität sind hierbei von entscheidender Bedeutung, da sie die Grundlage der IT-Sicherheit bilden. Es wäre fast unmöglich, die Vertraulichkeit und Integrität von Daten sicherzustellen, wenn es keine festen Mechanismen zur Identitätsverifizierung und Zugriffskontrolle gäbe.

Früher genügten einfache Passwortabfragen zur Sicherung des Zugangs zu IT-Systemen, doch heutzutage sind viel komplexere Verfahren notwendig. Die Weiterentwicklung ihrer Techniken durch Angreifer hat zu einer fortwährenden Bedrohung geführt. Daher ist es unverzichtbar, wirksame Strategien zur Identitäts- und Authentifizierung einzuführen, um den Schutz von Informationen und Systemen sicherzustellen.

1.1 Aufgabenstellung und Zielsetzung

Diese Seminararbeit untersucht die Rolle von Identity und Authentication im Kontext der IT-Sicherheit. Das Ziel besteht darin, die unterschiedlichen Verfahren zur Identitätsprüfung und Zugangskontrolle zu untersuchen und deren Relevanz für die Sicherheit der IT zu untersuchen. Darüber hinaus werden die gegenwärtigen Schwierigkeiten und Risiken im Zusammenhang mit Identität und Authentifizierung diskutiert und es werden potenzielle Lösungsansätze und bewährte Verfahren vorgestellt.

1.2 Vorgehensweise

Zuerst erfolgt eine Erläuterung grundlegender Konzepte und Definitionen im Kontext von Identität und Validierung. Anschließend werden die üblichen Authentifizierungsmethoden ausführlich analysiert und ihre Wirksamkeit in der Praxis getestet. Der Hauptteil der Arbeit beschäftigt sich mit den gegenwärtigen Herausforderungen und Gefahren auf diesem Gebiet sowie den Möglichkeiten, diese zu bewältigen. Zum Schluss erfolgt eine Zusammenfassung der gewonnenen Erkenntnisse und es wird ein Ausblick auf kommende Entwicklungen gegeben.

2 Grundlagen

2.1 Identity

Der Ausdruck Identity wird in der Informatik als eine eindeutige Identifikation einer Entität[1] verwendet, die als Benutzer, Gerät oder System funktionieren kann. Diese Identifizierung erlaubt es, unterschiedliche Entitäten zu identifizieren und ihnen bestimmte Zugriffs- oder Berechtigungen zuzuordnen. Dies erfolgt häufig anhand eindeutiger Merkmale wie Benutzername, E-Mail-Adresse oder einer Identifikationsnummer (ID). Es ist unverzichtbar für IT-Sicherheitsmaßnahmen, Entitäten korrekt zu identifizieren, da ohne diese keine bestimmten Zugriffsrechte vergeben oder überwacht werden können. Im Identity Management, welches sich mit der Verwaltung von Identitäten und deren Berechtigungen in einem System beschäftigt, ist Identität außerdem von entscheidender Bedeutung.

2.2 Authentication

Der Vorgang von Authentication dient dazu, die Identität einer Entität zu bestätigen, indem nachgewiesen wird, dass diese tatsächlich korrekt ist. Dieser Nachweis kann auf unterschiedliche Weise erfolgen, etwa mit einem Passwort, einem Fingerabdruck oder einer Zwei-Faktor-Authentifizierung (2FA). Ein wesentlicher Schritt zur Gewährleistung des Zugangs zu geschützten Ressourcen ist Authentication. Es bietet Schutz vor unbefugtem Zugriff und unterstützt die Einhaltung von Vertraulichkeit und Integrität sensibler Daten. Die Sicherheitsniveaus verschiedener Authentifizierungsmethoden variieren. Die Entscheidung für die passende Methode ist abhängig von den spezifischen Anforderungen und Bedrohungsmodellen eines Systems [ISO/IEC 27000:2018].

2.3 Grundlagen IT-Sicherheit

Es ist das Ziel der IT-Sicherheit, die Risiken, die sich aus Bedrohungen für IT-Systeme ergeben, angemessen zu verringern. Daher beschäftigt sich IT-Sicherheit mit IT-Sicherheitsmaßnahmen, die dafür sorgen, dass Informationen auf IT-Systemen sowie auf solchen selbst Vertraulichkeit, Authentifkation, Authentizität, Integrität, Verbindlichkeit, Verfügbarkeit und Anonymisierung/Pseudonymisierung nicht verloren gehen. Darüber hinaus umfasst IT-Sicherheit auch Softwaresicherheit und IT-Systemzuverlässigkeit. Das Ziel von IT-Sicherheit ist es, Schäden für Unternehmen, Behörden, Organisationen und Personen zu verhindern oder zumindest zu reduzieren.

Ziel der IT-Sicherheit

Die Hauptziele der IT-Sicherheit werde als "CIA-Triade"bezeichnet.

* Vertraulichkeit (Confidentiality): Sicherstellung, dass Informationen nur von autorisierten Personen eingesehen werden können.

[1] Ein Objekt oder ein Ding, das existiert und eindeutig identifizierbar ist.

* Integrität (Integrity): Gewährleistung, dass Daten während der Übertragung oder Speicherung nicht unbemerkt geändert oder manipuliert werden können.
* Verfügbarkeit (Availability): Sicherstellung, dass Systeme und Daten für autorisierte Benutzer bei Bedarf zugänglich sind.

Bedrohungen und Angriffe
Es existieren zahlreiche Risiken und Attacken, die die Sicherheit von IT gefährden können.

* Viren, Würmer, Trojaner und Ransomware gehören zu den Schadsoftwarekategorien.
* Phishing bezieht sich auf betrügerische Bemühungen, vertrauliche Daten wie Passwörter oder Kreditkartendaten auszurauben.
* Denial-of-Service (DoS)-Angriffe beziehen sich darauf, Systeme oder Netzwerke durch Überlastung zu blockieren.
* Man-in-the-Middle (MitM)-Angriffe beziehen sich darauf, dass die Kommunikation zwischen zwei Parteien ohne deren Wissen abgefangen und manipuliert wird.

Sicherheitsmaßnahmen
Zur Sicherstellung der IT-Sicherheit werden unterschiedliche Schritte und Technologien angewendet:

* Firewalls sind Systeme zur Überwachung und Steuerung des ein- und ausgehenden Netzwerkverkehrs.
* Antivirensoftware: Programme zur Erkennung und Beseitigung von schädlicher Software.
* Verschlüsselung: Verfahren zur Verschlüsselung von Daten, die nur befugte Personen lesen können.

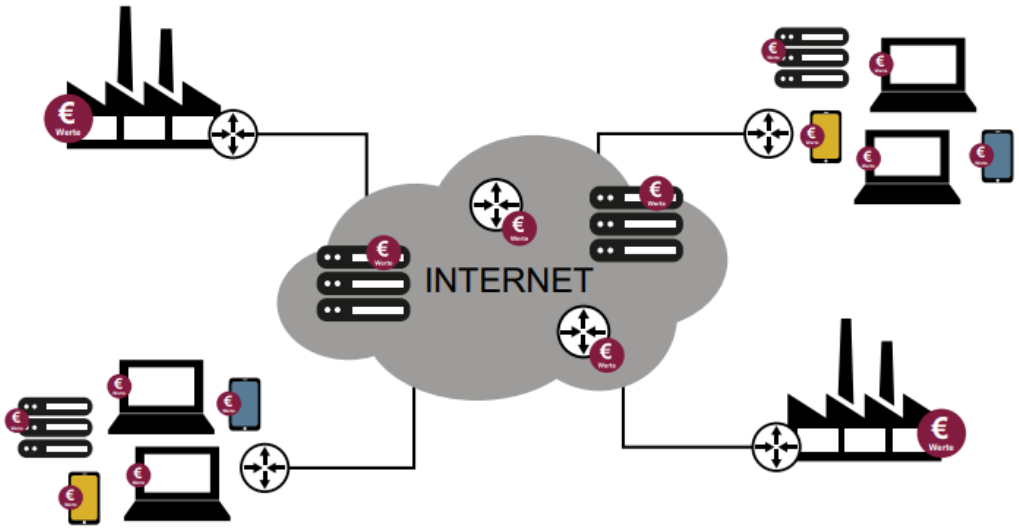

Abbildung 1: Cyber-Sicherheit © Prof. Norbert Pohlmann – Glossar Cyber-Sicherheit [Pohlmann 2019]

3 Identity Management

3.1 Begriffsdefinition

Identity Management (IdM) bezeichnet eine Sammlung von Funktionen und Kompetenzen, die zur Verwaltung und Sicherstellung von Identitätsinformationen (z.B. Identifikatoren, Anmeldeinformationen) und zur Gewährleistung der Identität einer Entität verwendet werden. Es umfasst außerdem die Unterstützung von Geschäfts- und Sicherheitsprozessen sowie die Durchsetzung von Richtlinien. Identität wird für das Identity Management als etwas verstanden, das je nach Kontext unterschiedlich sein kann, d.h., die Vielfalt der Attribute sind durch Rahmenbedingungen begrenzt, in dem die Entität existiert und interagiert. Authentifizierung im Identity Management bedeutet hingegen, sicherzustellen, dass eine Entität wirklich diejenige ist, die sie vorgibt zu sein [ITU-T X.1252 2021].

3.2 Komponenten eines Identity Management Systems

Das Konzept des Identity Managements (IdM) umfasst die organisatorischen Abläufe und Technologien, die genutzt werden, um Identitäten zu verwalten und Ressourcen zu nutzen. Es beinhaltet das Erstellen, Verwalten und Überwachen digitaler Identitäten, damit nur befugte Nutzer und Geräte auf bestimmte Informationen und Systeme zugreifen können. Die Komponenten dafür sind:

* Identitätsanbieter (IdP): Diese Komponente ist verantwortlich für die Erstellung, Verwaltung und Bereitstellung von Identitäten für Benutzer und Systeme.

* Verzeichnisdienste: Sie speichern und verwalten Identitätsdaten wie Benutzerprofile, Anmeldeinformationen und Attributinformationen. Diese Datenbanken sind zentral für die Organisation und den Zugriff auf Identitätsinformationen.

* Authentifizierungsdienste: Diese Dienste überprüfen die Identität der Benutzer oder Systeme durch verschiedene Authentifizierungsmethoden, wie Passwörter, biometrische Daten oder Zwei-Faktor-Authentifizierung.
* Autoritätsdienste: Sie verwalten die Zugriffsrechte und -privilegien basierend auf der verifizierten Identität und den zugewiesenen Rollen und Verantwortlichkeiten. Dies stellt sicher, dass Benutzer nur auf die Ressourcen zugreifen können, für die sie berechtigt sind.
* Audit- und Berichtssysteme: Diese Systeme protokollieren und überwachen Identitäts- und Zugriffsereignisse, um Sicherheitsvorfälle zu identifizieren und zu analysieren. Sie sind entscheidend für die Einhaltung von Sicherheitsrichtlinien und die Nachverfolgbarkeit von Zugriffen. [ITU-T X.1252 2021].

3.3 Prozesse im Identity Management

Die Prozesse im Identity Management beinhalten dynamische Aktivitäten, die darauf abzielen, Identitäten zu verwalten und zu schützen. Die dynamischen Prozesse sind:

* Registrierung und Einschreibung: Dieser Prozess beinhaltet die Erfassung und Verifizierung der Identitätsinformationen neuer Benutzer oder Systeme. Ziel ist es, diesen neuen Entitäten den Zugang zu den benötigten Ressourcen zu ermöglichen.
* Authentifizierung: Hierbei wird überprüft, ob eine Entität tatsächlich diejenige ist, die sie vorgibt zu sein. Dies kann durch Methoden wie Passwörter, biometrische Daten oder Tokens erfolgen.
* Autorisierung: Dieser Prozess bestimmt, welche Ressourcen und Daten eine authentifizierte Entität basierend auf ihren Rollen und Berechtigungen zugreifen darf. Autorisierung stellt sicher, dass nur berechtigte Entitäten auf bestimmte Ressourcen zugreifen können.
* Verwaltung und Wartung: Diese kontinuierlichen Aktivitäten beinhalten die Aktualisierung und Verwaltung von Identitätsdaten, wie die Änderung von Berechtigungen, das Zurücksetzen von Passwörtern und die Aktualisierung von Benutzerinformationen.
* Überwachung und Auditierung: Diese Prozesse umfassen die kontinuierliche Überwachung und Aufzeichnung von Identitäts- und Zugriffsaktivitäten. Sie sind wichtig, um die Einhaltung von Sicherheitsrichtlinien zu gewährleisten und verdächtige Aktivitäten zu erkennen.
* Identitätsbindung und -korrelation: Diese Prozesse verknüpfen Identitätsinformationen über verschiedene Systeme und Anwendungen hinweg, um eine konsistente und einheitliche Identität zu gewährleisten. Dies ist besonders wichtig in komplexen IT-Umgebungen, in denen verschiedene Systeme integriert sind [ITU-T X.1252 2021].

3.4 Herausforderungen im Identity Management

Die Integration neuer Technologien, die Verwaltung von Benutzeridentitäten über verschiedene Systeme hinweg und die Einhaltung gesetzlicher Anforderungen sind einige der Schwierigkeiten, mit denen das Identity Management konfrontiert ist. Des Weiteren ist es notwendig, Sicherheitslücken zu beheben und einen hohen Schutz der Identitätsdaten sicherzustellen.

3.5 Rechtliche und Compliance-Aspekte

Identity Management muss sich auch mit rechtlichen und Compliance[2]-Aspekten auseinandersetzen. Datenschutzgesetze und -verordnungen wie die DSGVO in Europa legen strenge Regeln für die Verarbeitung personenbezogener Daten fest. Unternehmen müssen sicherstellen, dass sie diese Vorschriften einhalten, um rechtliche Konsequenzen zu vermeiden.

4 Authentication Methods

Authentifizierungsmechanismen spielen eine entscheidende Rolle bei der Sicherung von Systemen und der Gewährleistung, dass nur autorisierte Benutzer Zugang erhalten. Es gibt verschiedene Authentifizierungsmethoden, jede mit ihren eigenen Vor- und Nachteilen. Im Folgenden wird ein Überblick über einige der gängigsten Methoden gegeben:

4.1 Statische Authentifizierung

Die statische Authentifizierung verwendet ein gemeinsames Geheimnis, wie ein Passwort, eine Passphrase oder eine PIN. Diese Methode ist aufgrund ihrer Einfachheit und leichten Implementierung weit verbreitet. Der Benutzer gibt ein bekanntes Geheimnis in das System ein, das dieses dann mit den gespeicherten Daten vergleicht. Diese Methode hat jedoch mehrere Schwächen, darunter die Anfälligkeit für Replay[3]-Angriffe, physische Angriffe (z.B. Keylogger[4]) und Brute-Force-Angriffe [Syed Zulkarnain Syed Idrus u. a. 2013].

4.2 Einmalpasswort

Einmalpasswort-Tokens (OTPs) generieren für jede Authentifizierungssitzung ein einzigartiges Passwort. Diese Methode verbessert die Sicherheit, da Passwörter nicht wiederverwendet werden können. OTPs können auf verschiedene Weise bereitgestellt werden, z.B. durch Hardware-Token, SMS oder E-Mail. Der Hauptvorteil von OTPs ist ihre Widerstandsfähigkeit gegen Replay-Angriffe, allerdings erfordern sie zusätzliche Infrastruktur und Benutzermanagement, was die Kosten und Komplexität erhöhen kann [Imlach 15.09.2023].

[2] Compliance bezieht sich auf die Einhaltung von Gesetzen, Vorschriften und ethischen Standards

[3] Kryptoanalytische Angriffsform auf die Authentizität von Daten in einem Kommunikationsprotokoll

[4] Gerät oder Programm, das die über die Computertastatur getätigte Eingabe aufzeichnet und dadurch alles Getippte rekonstruieren kann

Abbildung 2: One-Time Password [Imlach 15.09.2023]

4.3 Hardwarebasiert

Authentifizierungsgeräte wie YubiKeys[5] oder Sicherheitsschlüssel ermöglichen eine leistungsstarke, auf der Hardware basierende Authentifizierung. Um die Authentifizierung abzuschließen, ist eine physische Anwesenheit dieser Geräte erforderlich, was die Sicherheit deutlich erhöht [dos Santos, Uelison Jean Lopes u. a. 2022].

4.4 Magic Links

Bei dieser Vorgehensweise bekommt der Nutzer einen einmalig gültigen Link per E-Mail, der ihn ohne die Notwendigkeit eines Passworts direkt authentifiziert.

4.5 Push-Benachrichtigungen

Eine Push-Benachrichtigung wird an das mobile Gerät des Benutzers gesendet, die der Benutzer dann bestätigen muss, um sich zu authentifizieren.

4.6 Challenge-Response-Verfahren

Das Challenge-Response-Verfahren schreibt vor, dass ein Benutzer eine kryptografische Beweise gegenüber dem IT-System vorlegen muss. Dieser Prozess erfordert vom Benutzer ein Geheimnis, etwa einen geheimen Schlüssel, mit dem er spontan eine kryptografische Operation durchführen muss, um zu beweisen, dass er diesen besitzt. Normalerweise schickt das IT-System dem Benutzer eine zufällige Nummer, die Challenge. Diese wird dann automatisch kryptografisch verarbeitet und als Antwort an das IT-System geschickt. Das IT-System prüft die korrekte Durchführung der kryptografischen Operation durch den Benutzer. Wenn ja, ist die Authentisierung gelungen. Andernfalls wird die Echtheit als nicht bewiesen angesehen und es wird keine Kommunikation über das IT-System gestattet.

Es ist nicht möglich, aufgezeichnete Daten erneut zu nutzen, da ständig neue Zufallszahlen als Challenge gesendet werden. Um Abhören und damit verbundene missbräuchliche Nutzung zu vermeiden, müssen Challenge-Response-Verfahren bei der Authentifizierung über unsichere Netze verwendet werden. Beide Parteien nutzen Hardware-Sicherheitsmodule, um die geheimen Schlüssel zu speichern und kryptografische Verfahren zu berechnen. SM-C stellt das Hardware-

[5] YubiKey von Yubico ermöglicht sichere, passwortlose Authentifizierung

Sicherheitsmodul des Benutzers dar, während SM-S das IT-System darstellt [Pohlmann und Devnpo 2020].

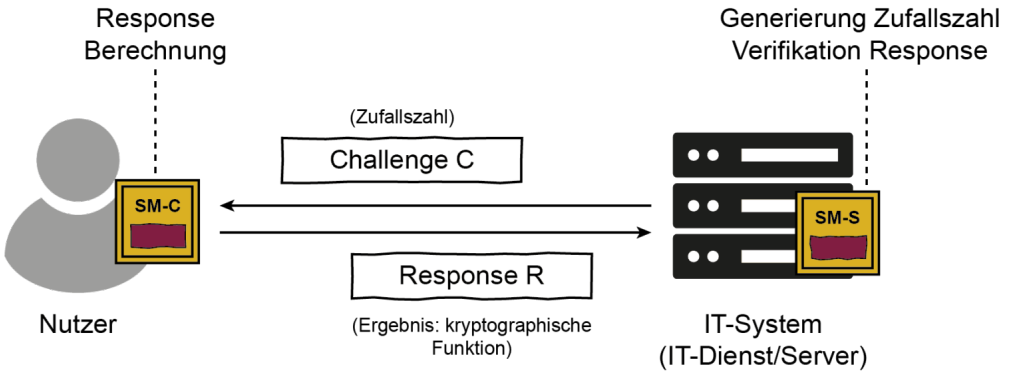

Abbildung 3: Challenge-Response-Verfahren © Prof. Norbert Pohlmann – Glossar Cyber-Sicherheit [Pohlmann und Devnpo 2020]

4.7 RFID-basierte Authentifizierung

Die auf RFID basierende Authentifizierung verwendet RFID-Tags[6] und -Lesegeräte zur Identitätsüberprüfung. Diese Methode wird häufig für die physische Zugangskontrolle, wie in gesicherten Gebäuden oder eingeschränkten Bereichen, verwendet. RFID-Tags können eindeutige Identifikatoren speichern, die von RFID-Lesegeräten gelesen werden, um Zugang zu gewähren oder zu verweigern. Die Vorteile von RFID umfassen Benutzerfreundlichkeit und schnelle Authentifizierung, allerdings können die Tags anfällig für Klonen und unbefugtes Auslesen sein [Syed Zulkarnain Syed Idrus u. a. 2013].

4.8 Biometrische Authentifizierung

Bei Biometrie handelt es sich um die Identifizierung und Authentifizierung durch biologische Eigenschaften. Die biometrische Authentisierung nutzt physiologische oder verhaltenstypische Eigenschaften, die also mit dem Individuum in Verbindung stehen. Der grundlegende Nutzen von biometrischen Methoden zur Identifikation und Authentifizierung besteht darin, dass biometrische Eigenschaften nicht direkt gestohlen werden können und in der Regel nur schwer nachahmen lassen. Biometrische Merkmale lassen sich auf zahlreiche Weisen messen. Das Tippverhalten an einer Tastatur, Fingergeometrie, Fingerlängenverhältnis und Handgeometrie werden durch verschiedene Methoden gemessen. Stimmanalyse, Gesichtserkennung, Unterschriftendynamik, Netzhautmuster, Irismuster, genetischer Code (DNA-Analyse) und Gesichtserkennung sind weitere Optionen. Auch diese Methoden können in verschiedenen Kombinationen angewendet werden [Pohlmann und Devnpo 2020].

[6] Senden und Empfangen von Informationen über eine Antenne und einen Mikrochip

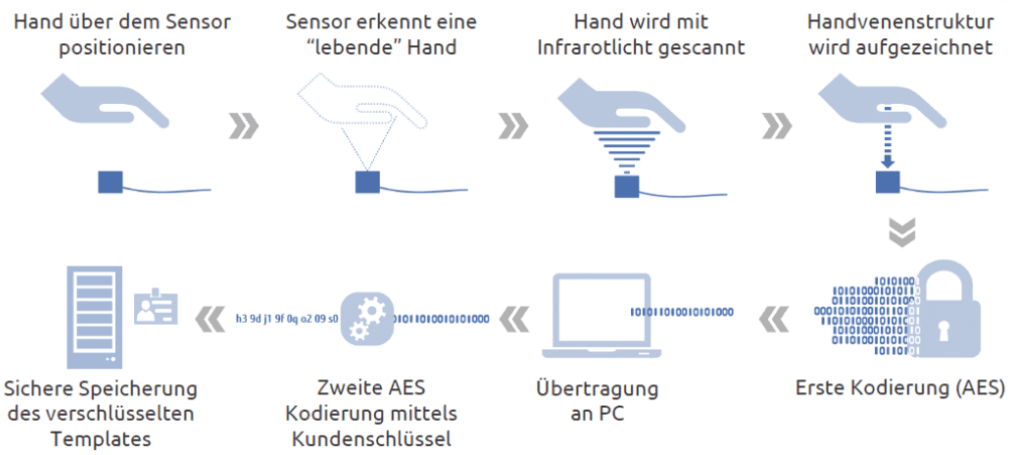

Abbildung 4: Biometrische Verfahren mit Handvenentechnologie [Secobit Website 13.03.2020]

4.9 Mulit-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) kombiniert mehrere Authentifizierungsmethoden, um die Sicherheit zu erhöhen. Beispielsweise kann ein Benutzer ein Passwort eingeben und zusätzlich einen Fingerabdruck scannen. Diese Methode erschwert es Angreifern, Zugang zu Systemen zu erhalten, da sie mehrere Authentifizierungsfaktoren überwinden müssen.

4.10 Moderne Ansätze und Technologien

Zu den modernen Ansätzen und Technologien in der Authentifizierung gehören unter anderem die Verwendung von Künstlicher Intelligenz (KI), um Anomalien im Benutzerverhalten zu erkennen, sowie Blockchain-Technologien zur sicheren Verwaltung von Identitäten und Authentifizierungsprozessen [Liu u. a. 2020].

5 Integration von Identity und Authentication in IT-Sicherheitsstrategien

5.1 Bedeutung für die IT-Sicherheitsarchitektur

Die IT-Sicherheitsarchitektur ist in der modernen digitalen Welt von entscheidender Bedeutung für jede Organisation, in der der Schutz sensibler Daten unverzichtbar ist. Die IT-Sicherheitsarchitektur beinhaltet die strategische Ausarbeitung und Realisierung von Sicherheitsvorkehrungen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Eine zuverlässige Sicherheitsarchitektur vereint Identitätsmanagement und Authentifizierungstechniken, um sicherzustellen, dass ausschließlich befugte Nutzer auf vertrauliche Informationen zugreifen können.

Eine stabile Basis für die IT-Sicherheitsarchitektur ist das Identitäts- und Zugriffsmanagement (IAM). Dies beinhaltet das Verwalten der Identitäten der Nut-

zer und die Steuerung des Zugangs zu Ressourcen. Indem ein wirksames IAM-System eingeführt wird, kann gewährleistet werden, dass die passenden Nutzer zum richtigen Zeitpunkt auf die passenden Ressourcen zugreifen können. Dadurch wird das Risiko von Sicherheitsvorfällen deutlich verringert [Deverajan Ganesh Gopal und Udhayakumar Hari Haran 2020].

5.2 Identity und Access Management (IAM) in der IT-Sicherheit

IAM ist ein wichtiger Bestandteil von IT-Sicherheitsstrategien und ist für den Schutz von Unternehmensdaten von entscheidender Bedeutung. IAM beinhaltet verschiedene Technologien und Abläufe, die gewährleisten, dass die Benutzeridentitäten überprüft und deren Zugriffsrechte verwaltet werden. Ein IAM-System hat die folgenden Hauptaufgaben zu erfüllen:

- Identitätsmanagement: Es umfasst das Erstellen, Verwalten und Deaktivieren von Benutzeridentitäten. Dies beinhaltet das Einloggen neuer Benutzer, das Aktualisieren von Benutzerinformationen und die Gewährleistung des Entfernens veralteter oder unberechtigter Identitäten.
- Authentifizierung: Die Überprüfung der Identität eines Benutzers durch verschiedene Methoden wie Passwörter, biometrische Daten oder Tokens. Eine starke Authentifizierung stellt sicher, dass nur autorisierte Benutzer auf Systeme und Daten zugreifen können.
- Autorisierung: Das Management der Zugriffsrechte und -privilegien, die auf der überprüften Identität sowie den zugewiesenen Rollen und Verantwortlichkeiten der Nutzer beruhen. Dadurch wird sichergestellt, dass Nutzer nur auf die für ihre Tätigkeiten erforderlichen Ressourcen zugreifen können.

Ein wirksames IAM-System trägt zur Minimierung von Sicherheitsrisiken bei, indem es gewährleistet, dass ausschließlich befugte Nutzer auf sensible Daten und Systeme zugreifen [Deverajan Ganesh Gopal und Udhayakumar Hari Haran 2020].

5.3 Zero Trust Security Modelle

Beim Zero Trust-Sicherheitsmodell handelt es sich um eine Methode zur IT-Sicherheit, bei der weder Benutzer noch Geräte im Netzwerk automatisch als vertrauenswürdig gelten. Stattdessen werden sämtliche Zugänge zu Ressourcen fortlaufend geprüft. Zu Zero Trust gehören die folgenden Grundsätze:

- Least Privilege Access: Nutzer bekommen lediglich die erforderlichen Zugriffsrechte, um ihre Aufgaben zu erfüllen. Dadurch wird das Risiko verringert, dass Nutzer unbefugten Zugang zu sensiblen Daten bekommen.
- Überwachung und Validierung: Es findet eine fortlaufende Überprüfung aller Benutzer und Geräte statt, um sicherzustellen, dass sie genehmigt und sicher sind. Dazu gehören die Überwachung von Benutzeraktivitäten in Echtzeit und das Aufspüren von Abweichungen.

- Mikrosegmentierung und Segmentierung: Zur Kontrolle und Isolierung des Zugriffs auf Ressourcen wird das Netzwerk in kleinere Abschnitte aufgeteilt. Dadurch wird verhindert, dass sich Angreifer, die einen Bereich kompromittiert haben, im Netzwerk verbreiten.

Das Zero Trust Modell betont die Notwendigkeit, jede Zugriffsanfrage zu verifizieren, unabhängig davon, woher sie kommt, um die Sicherheit der IT-Infrastruktur zu gewährleisten [Deverajan Ganesh Gopal und Udhayakumar Hari Haran 2020].

5.4 Sicherheitsrichtlinien und -verfahren

Es ist unerlässlich, Sicherheitsrichtlinien und -verfahren zu haben, um sensible Daten zu schützen und die Sicherheit der IT sicherzustellen. Zu den deutlichen Richtlinien und Verfahren gehören:

- Zugriffsrichtlinien: Festlegung der Zugriffsrechte und -privilegien für Nutzer auf der Grundlage ihrer Aufgaben und Aufgaben. Diese Leitlinien bestimmen, welche Personen Zugang zu welchen Ressourcen haben und zu welchen Konditionen.
- Passwortrichtlinien: Bewährte Verfahren zur Erstellung und Verwaltung von Passwörtern, darunter die Anforderungen an die Komplexität des Passworts, die Häufigkeit von Änderungen des Passworts und die Anwendung von Mehrfaktorauthentifizierung.
- Incident-Response-Verfahren: Pläne und Prozesse zur Reaktion auf Sicherheitsvorfälle. Dies umfasst die Erkennung, Eindämmung und Behebung von Sicherheitsvorfällen sowie die Durchführung von forensischen Untersuchungen und die Berichterstattung an die entsprechenden Behörden.

Die Befolgung dieser Vorschriften und Verfahren gewährleistet, dass Unternehmen auf Gefahren im Zusammenhang mit der Sicherheit vorbereitet sind und rasch und wirksam reagieren können [Deverajan Ganesh Gopal und Udhayakumar Hari Haran 2020].

5.5 Bedrohungsanalyse und Risikomanagement

Für die Sicherheit der IT sind umfassende Methoden der Bedrohungsanalyse und des Risikomanagements von entscheidender Bedeutung. Zu diesen Methoden gehören:

- Modellierung von Bedrohungen: Das Erkennen und Bewerten möglicher Risiken für die IT-Infrastruktur. Dazu gehören die Auswertung der Bedrohungslandschaft, die Einschätzung der Folgen möglicher Bedrohungen und die Ausarbeitung von Maßnahmen zur Risikominderung.

- Risikobewertung: Die Einschätzung der Gefahren, denen eine Organisation gegenübersteht, sowie die Festlegung der Wahrscheinlichkeit und der möglichen Folgen dieser Gefahren. Dies trägt zur Festlegung von Prioritäten und zur Konzentration von Ressourcen auf die kritischsten Gefahren bei.
- Risikoverringerung: Die Umsetzung von Maßnahmen, um die identifizierten Risiken zu verringern. Dazu gehören technische Vorkehrungen wie Firewalls und Intrusion-Detection-Systeme, aber auch organisatorische Maßnahmen wie Schulungen und Sensibilisierungsmaßnahmen.

Ein wirksames Programm zur Bedrohungsanalyse und zum Risikomanagement gewährleistet, dass man auf Bedrohungen im Bereich der Sicherheit vorbereitet ist und proaktive Maßnahmen zum Schutz der IT-Infrastruktur ergreift.

6 Identity und Authentication in Cloud-Umgebungen

6.1 Herausforderungen in der Cloud

Cloud-Computing bringt unterschiedliche Schwierigkeiten mit sich, vor allem in Bezug auf die Sicherheit und Identitätsverwaltung. Eine der größten Herausforderungen liegt darin, sicherzustellen, dass ausschließlich befugte Nutzer auf vertrauliche Daten und Dienste zugreifen. Dafür sind stabile Sicherheitsvorkehrungen und die Fähigkeit erforderlich, Identitäten in verschiedenen Cloud-Services einheitlich zu verwalten. Darüber hinaus müssen Firmen gewährleisten, dass ihre Sicherheitsprotokolle mit den Service Level Agreements (SLAs) übereinstimmen und dass die Daten inaktiver Prozesse sicher verwaltet werden [Temidayo und Isaac 2019].

6.2 Cloud Identity Management

Cloud Identity Management (IDM) spielt eine entscheidende Rolle bei der Verwaltung von Benutzeridentitäten und Zugriffskontrollen in Cloud-Umgebungen.Es existieren unterschiedliche Formen von Identitätsmanagement-Systemen, wie zum Beispiel isolierte, zentrale, föderale und anonyme Identitätsmanagementsysteme. Ein zentrales IDM-System erleichtert die Verwaltung und Umsetzung von Sicherheitsrichtlinien, indem es Identitätsdaten an einem Ort konsolidiert. Durch die Verwaltung von Identitäten über Vertrauensgrenzen hinweg ermöglichen föderale IDM-Systeme die Kooperation verschiedener Organisationen. Anonyme IDM-Systeme gewährleisten den Schutz der Privatsphäre der Nutzer durch die Speicherung von persönlich identifizierbaren Daten [Temidayo und Isaac 2019].

6.3 Authentifizierung in Cloud-Diensten

Um sicherzustellen, dass Benutzer tatsächlich die sind, für die sie sich ausgeben, ist die Authentifizierung in Cloud-Services von entscheidender Bedeutung. Einfache Sign-On (SSO), Zwei-Faktor-Authentifizierung (2FA) und Multi-Faktor-Authentifizierung (MFA) sind die üblichen Authentifizierungstechniken. SSO erlaubt es Nutzern, sich ohne erneute Authentifizierung auf mehrere Anwendungen

zuzugreifen, nachdem sie sich einmal angemeldet haben. Die Sicherheit wird durch 2FA und MFA gesteigert, da sie zusätzlich zum Passwort eine weitere Verifizierungsebene wie einen Code auf dem Handy oder biometrische Daten verlangen. Diese Verfahren gewährleisten, dass nur befugte Nutzer auf Cloud-Dienste zugreifen können [Temidayo und Isaac 2019].

6.4 Technische Implementierungen

OAuth:
Um sicheren Zugriff auf Ressourcen von Drittanbieteranwendungen im Namen eines Nutzers zu ermöglichen, ohne die eigentlichen Zugangsdaten des Nutzers weiterzugeben, ist OAuth (Open Authorization) ein häufig verwendetes Autorisierungsprotokoll. OAuth nutzt stattdessen Tokens mit bestimmten Berechtigungen und beschränkter Gültigkeit. Diese Tokens stammen von einem Autorisierungsserver und erlauben Anwendungen den Zugang zu geschützten Ressourcen, wie etwa Benutzerkonten in sozialen Medien, ohne dass das Passwort des Nutzers unmittelbar an die Anwendung gesendet wird. Dadurch wird das Risiko von Diebstahl und Missbrauch von Passwörtern deutlich reduziert [J.Vijaya Chandra 2019].

OpenID Connect:
OpenID Connect nutzt OAuth 2.0 als Grundlage und integriert eine Authentifizierungsschicht. Obwohl OAuth vor allem für die Autorisierung genutzt wird, erlaubt OpenID Connect die Authentifizierung, d. h. die Identitätsprüfung eines Benutzers. ID-Tokens, die vom Autorisierungsserver ausgegeben werden und über den authentifizierten Benutzer informieren, werden von OpenID Connect genutzt. Auf diese Weise können Nutzer sich mit nur einer Identität bei verschiedenen Diensten anmelden. Dadurch wird die Notwendigkeit mehrerer Benutzernamen und Passwörter beseitigt. Ein übliches Beispiel dafür ist die Option, sich über ein Google- oder ein Facebook-Konto auf unterschiedlichen Websites und Dienstleistungen anzumelden [J.Vijaya Chandra 2019].

Microsoft Azure Active Directory:
Der umfassende Cloud-basierte Verzeichnisdienst Microsoft Azure Active Directory (Azure AD) zentralisiert das Identitäts- und Zugriffsmanagement von Cloud- und On-Premises-Anwendungen. Azure AD verfügt über Features wie Single Sign-On (SSO), mit denen Benutzer auf unterschiedliche Anwendungen und Dienste mit nur einer Anzahl von Anmeldeinformationen zugreifen können, sowie Multi-Faktor-Authentifizierung (MFA), die eine zusätzliche Sicherheitsstufe bereitstellt. Darüber hinaus kann Azure AD mit anderen Cloud-Services und lokalen Verzeichnisdiensten integriert werden, wie zum Beispiel dem herkömmlichen Active Directory. Dadurch wird die Verwaltung von Zugriffsrechten und Identitäten in hybriden IT-Umgebungen vereinfacht und die Sicherheit und Wirksamkeit des Identitätsmanagements werden gesteigert [J.Vijaya Chandra 2019].

6.5 Sicherheitsaspekte

Um Identitäten und Authentifizierungsprozesse in der Cloud zu sichern, müssen bewährte Methoden eingeführt und moderne Technologien eingesetzt werden. Identity Access Management as a Service (IDaaS) ist eine anpassungsfähige und anpassungsfähige Methode, um Identitäten und Zugriffsrechte zu verwalten. IDaaS erlaubt es, maschinelles Lernen und andere Sicherheitsdaten zu integrieren, um die Sicherheitssituation zu optimieren. Die Verwendung von Multifaktor-Authentifizierung, die regelmäßige Überprüfung und Aktualisierung von Sicherheitsrichtlinien sowie die Schulung der Benutzer in Sicherheitsfragen sind Beispiele für bewährte Verfahren. Diese Schritte ermöglichen es Firmen, ihre Cloud-Umgebungen effektiver zu schützen und die Gefahren von Sicherheitsverletzungen zu verringern [Temidayo und Isaac 2019].

Schutzmaßnahmen

- **Sichere Kommunikationsprotokolle:** Die Verwendung von Verschlüsselungsprotokollen wie Transport Layer Security (TLS) gewährleistet einen Schutz der Daten bei der Übermittlung. Die Kommunikation zwischen Client und Server wird durch TLS verschlüsselt. Unbefugte Dritte können die Daten daher fast nicht entschlüsseln oder manipulieren [J.Vijaya Chandra 2019].
- **Sichere Kommunikationsprotokolle:** Eine fortlaufende Kontrolle von Netzwerkaktivitäten und Anmeldeversuchen trägt dazu bei, frühzeitig ungewöhnliche oder verdächtige Aktivitäten zu identifizieren. Tools, die dazu dienen, Bedrohungen zu überwachen und zu erkennen (Threat Detection), haben die Fähigkeit, automatisch Alarm zu schlagen, wenn ungewöhnliches Verhalten festgestellt wird. Dadurch können schnelle Sicherheitsmaßnahmen getroffen werden [J.Vijaya Chandra 2019].
- **Sichere Kommunikationsprotokolle:** Um sicherzustellen, dass die Sicherheit der IT-Infrastruktur gewährleistet ist, sind strenge Sicherheitsrichtlinien unverzichtbar. Dies umfasst regelmäßige Änderungen des Passworts, den Einsatz von Multi-Faktor-Authentifizierung (MFA) und regelmäßige Schulungen, um die Mitarbeiter auf gegenwärtige Sicherheitsbedrohungen aufmerksam zu machen. Indem solche Richtlinien umgesetzt und befolgt werden, wird das Risiko von Sicherheitsvorfällen erheblich verringert [J.Vijaya Chandra 2019].

Um Identitäten und Zugänge in Cloud-Umgebungen wirksam zu schützen und mögliche Bedrohungen abzuwehren, sind diese Schutzmaßnahmen und Protokolle entscheidende Elemente eines ganzheitlichen Sicherheitskonzepts.

7 Trends bei Identität und Authentifizierung

7.1 Dezentralisierte Identität

Dezentrale Identität ist ein neuer Ansatz, der es Benutzern ermöglicht, ihre Identitätsinformationen selbst zu kontrollieren, anstatt diese zentralen Stellen zu überlassen. Diese Vorgehensweise verwendet Blockchain-Technologien, um die unveränderliche und sichere Speicherung von Identitätsdaten zu gewährleisten [dos Santos, Uelison Jean Lopes u. a. 2022].

Verwendete Methoden

- **Blockchain-Technologie:** Verwendung von verteilten Ledgern[7], um Identitätsdaten zu speichern und zu verifizieren.
- **Self-Sovereign Identity (SSI):** Nutzer können ihre Identitätsinformationen vollständig kontrollieren und selbst entscheiden, mit wem sie welche Daten teilen.

Vorteil

- **Erhöhte Datensicherheit und Datenschutz:** Indem Identitätsdaten dezentral gespeichert werden, steigt die Datensicherheit und der Datenschutz.
- **Geringere Abhängigkeit von zentralen Identitätsanbietern:** Benutzer sind nicht länger auf zentrale Stellen angewiesen, um ihre Identität zu verwalten, was das Risiko von Datenmissbrauch reduziert.

7.2 KI und maschinelles Lernen in der Authentifizierung

Künstliche Intelligenz (KI) und maschinelles Lernen (ML) verändern die Authentifizierung grundlegend, da sie innovative und intelligente Sicherheitsmechanismen zur Verfügung stellen, die in der Lage sind, auf Abweichungen und Gefahren zu reagieren [dos Santos, Uelison Jean Lopes u. a. 2022].

KI-basierte Authentifizierungsmethoden

- **Verhaltensanalyse:** Die Verwendung von KI zur fortlaufenden Überwachung des Nutzerverhaltens und zur Erkennung ungewöhnlicher Aktivitäten, die auf mögliche Sicherheitsrisiken hinweisen.
- **Anomalieerkennung:** Die Anwendung von Modellen des maschinellen Lernens zur Identifizierung und Auswertung verdächtiger Verhaltensweisen und Aktivitäten, die sich von der üblichen Nutzung unterscheiden.

Vorteile und Ziele

[7] Hardware-Wallet zur sicheren Speicherung und Verwaltung von Kryptowährungen, das private Schlüssel offline hält

- **Proaktive Erkennung und Abwehr:** KI kann verwendet werden, um Sicherheitsbedrohungen frühzeitig zu erkennen und abzuwehren, bevor sie einen Schaden verursachen.
- **Anpassungsfähigkeit:** Die langfristige Sicherheit wird durch KI-gestützte Systeme sichergestellt, da sie sich fortlaufend auf neue und sich verändernde Bedrohungen einstellen können.

7.3 Blockchain-basierte Identitätslösungen

Die Blockchain-Technologie speichert Transaktionen in Blöcken, die als dezentral und unveränderlich gelten. Diese Blöcke werden in einer Kette verknüpft. Diese Technologie zeichnet sich durch ihre Sicherheitsmerkmale aus, darunter Transparenz und Unveränderlichkeit, wodurch sie sich besonders gut für das Management von Identitätsinformationen eignet.
Diese Merkmale werden von Blockchain-gestützten Identitätslösungen verwendet, um Identitäten sicher zu speichern und zu handhaben. Die Methode, mit der Identitätsdaten verifiziert und verwaltet werden, ist dezentralisiert und erschwert Manipulation und Missbrauch. Der wesentliche Nutzen solcher Lösungen ist [Liu u. a. 2020]:

- **Dezentralisierung:** ermeidung eines einzelnen Fehlers oder Missbrauchs durch zentrale Autoritäten.
- **Transparenz:** Jeder Benutzer hat Zugang zu den Transaktionsdaten, was dazu beiträgt, die Identität zu verifizieren.
- **Sicherheit:** Die Blockchain ist unveränderlich und bietet Schutz vor unautorisierten Veränderungen der Identitätsdaten.

Zukunftsperspektiven

- **Wachstum der dezentralen Identitätssysteme:** Die steigende Beliebtheit von Blockchain-Technologien könnte dazu führen, dass dezentrale Identitätslösungen, die den Nutzern eine größere Kontrolle über ihre persönlichen Daten ermöglichen, weit verbreiteter eingesetzt werden.
- **Innovation im Identitätsmanagement:** Es besteht die Möglichkeit, dass sich die Identitäts- und Authentifizierungsverwaltung durch Fortschritte in der Blockchain-Technologie und die Entwicklung neuer Anwendungen weiter verbessern.

8 Zusammenfassung

Im Bereich der IT-Sicherheit sind Identitäts- und Authentifizierungsmechanismen in der heutigen digitalen Welt von entscheidender Bedeutung. Die Grundlage für den Schutz vertraulicher Daten, den Zugang zu Netzwerken und die Sicherheit von Interaktionen mit Nutzern sind diese Ideen. Aufgrund der Komplexität der Bedrohungen und Angriffe müssen diese Sicherheitsmaßnahmen fortlaufend verbessert und angepasst werden.

Die Seminararbeit weist darauf hin, dass Identitätsmanagement nicht allein die Verwaltung von Benutzeridentitäten beinhaltet, sondern auch die Sicherstellung der Vertraulichkeit und Integrität von Informationen, die mit diesen Identitäten in Verbindung stehen. Im Laufe der Zeit haben sich Authentifizierungsmethoden weiterentwickelt, von simplen Systemen auf der Grundlage von Kennwörtern bis hin zu multifaktoriellen Methoden, die verschiedene Sicherheitsstufen berücksichtigen, um die Identität eines Nutzers zu verifizieren.

Es wurde offensichtlich, dass der Schutz von IT-Systemen und den enthaltenen Daten wesentlich von der Gewährleistung der Identität eines Benutzers und der Verhinderung unbefugten Zugriffs abhängt. Für die Einführung dieser Systeme ist es notwendig, die möglichen Schwachstellen und Angriffspunkte, die von Angreifern ausgenutzt werden könnten, eingehend zu verstehen.

In der Arbeit wurde außerdem hervorgehoben, dass die Auswahl der passenden Authentifizierungsmethoden und -technologien für die Wirksamkeit der Sicherheitsvorkehrungen von entscheidender Bedeutung ist. Sowohl technische als auch organisatorische Gesichtspunkte sind dabei von Bedeutung. Die Anpassungsfähigkeit dieser Technologien an sich verändernde Bedrohungslandschaften und die Bereitstellung einer benutzerfreundlichen und sicheren Umgebung für die Benutzer sind entscheidend für die zukünftige Entwicklung.

Zusammenfassend kann festgehalten werden, dass das Management von Identitäten und Authentifizierungen nicht nur technisch, sondern auch strategisch wichtig ist und einen wesentlichen Beitrag zur Sicherheit von IT-Infrastrukturen leistet. Es ist unverzichtbar, in diesem Bereich fortlaufend Forschung und Entwicklung durchzuführen, um den zunehmenden Herausforderungen der IT-Sicherheit gerecht zu werden.

Literaturverzeichnis

Deverajan Ganesh Gopal und Udhayakumar Hari Haran (2020). „Safety measures for EHR systems“. In: *Security and Privacy of Electronic Healthcare Records*. Hrsg. von Sudeep Tanwar. Healthcare Technologies Ser. Stevenage: Institution of Engineering & Technology, S. 249–266. ISBN: 978-1-78561-898-7. DOI: 10.1049/pbhe020e{\textunderscore}ch10. URL: https://www.researchgate.net/profile/u-hariharan/publication/342215946_safety_measures_for_ehr_systems.

dos Santos, Uelison Jean Lopes u. a. (2022). „Trends in User Identity and Continuous Authentication“. In: *Computer* 55.11, S. 52–61. ISSN: 0018-9162. DOI: 10.1109/mc.2022.3187274.

Imlach, Jeremy (15.09.2023). „What is a One Time Password OTP“. In: *FEITIAN Technologies US*. URL: https://ftsafe.us/what-is-a-one-time-password-otp/.

ISO/IEC (27000:2018). „ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary“. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (besucht am 25. 07. 2024).

ITU-T (X.1252 2021). „X.1252 : Baseline identity management terms and definitions“. URL: https://www.itu.int/rec/T-REC-X.1252-202104-I/en.

J.Vijaya Chandra (2019). „Authentication and Authorization Mechanism for Cloud Security“. In: *International Journal of Engineering and Advanced Technology* 8.6, S. 2072–2078. ISSN: 2249-8958. DOI: 10.35940/ijeat.F8473.088619. URL: https://www.researchgate.net/profile/dr-chandra-jadala/publication/335842661_authentication_and_authorization_mechanism_for_cloud_security.

Liu, Yang u. a. (2020). „Blockchain-based identity management systems: A review“. In: *Journal of Network and Computer Applications* 166, S. 102731. ISSN: 1084-8045. DOI: 10.1016/j.jnca.2020.102731.

Pohlmann, Norbert (2019). „Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“. Wiesbaden: Springer Vieweg. ISBN: 9783658253974. DOI: 10.1007/978-3-658-25398-1.

Pohlmann, Norbert und Devnpo (2020). „Authentifikation - Glossar - Prof. Dr. Norbert Pohlmann“. URL: https://norbert-pohlmann.com/glossar-cyber-sicherheit/authentifikation/.

Secobit Website (13.03.2020). „Biometrische Lösungen - Secobit Website“. URL: https://secobit.de/leistungen/biometrische-loesungen/.

Syed Zulkarnain Syed Idrus u. a. (2013). „A Review on Authentication Methods“. In: *Australian Journal of Basic and Applied Sciences* 7.5, S. 95–107. URL: https://hal.science/hal-00912435/.

Temidayo, Abayomi-Zannu und Odun-Ayo Isaac (2019). „Cloud identity management-A critical analysis“. IAENG. URL: https://www.iaeng.org/publication/imecs2019/imecs2019_pp170-175.pdf.