Vertrauen und Sicherheit im Kontext von IAM


Die Burg ist längst gefallen

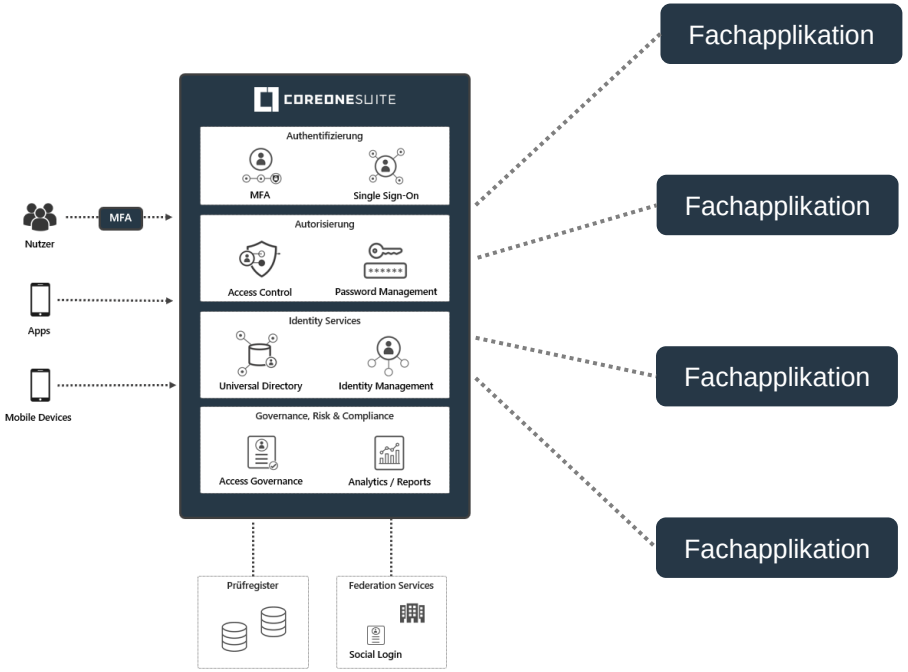
Quelle: Pixabay

Zero Trust – Die Burg ist längst gefallen

- **Zero-Trust** (traue keiner Gestalt - insbesondere denen ohne Nase ☺) - Organisationen sollten davon ausgehen, dass sowohl interne als auch externe Netzwerke unsicher sind und daher **jeder Zugriffsversuch sorgfältig überprüft** und validiert werden muss, unabhängig von der Quelle des Zugriffs.
- **Starke Authentifizierung** (ein unschuldiges Gesicht reicht nicht mehr aus) - kontinuierliche Überprüfung der Identität, unabhängig davon, ob ein Benutzer bereits authentifiziert wurde oder nicht (Re-Authentifizierung).
- **Least-Privilege-Prinzip** (wenn das Burgtor doch nicht so solide ist wie man meint) - selbst wenn ein Angreifer Zugriff auf ein System oder Netzwerk erhält, können die Schäden begrenzt werden, wenn fein granulare Zugriffsberechtigungen nach dem Least-Privilege-Prinzip implementiert sind.
- **Überwachung und Protokollierung** (auch die stärkste Burg hat Wachtürme) - Die Aktivitäten der Benutzer und Mitarbeiter sollten kontinuierlich überwacht und protokolliert werden. Dadurch können verdächtige Aktivitäten schnell erkannt und darauf reagiert werden.

Kernaufgaben von IAM

Kernaufgaben von IAM



- **Zentrale Verwaltung und sichere Speicherung** sämtlicher digitalen Identitäten
- Bereitstellung von Single Sign-On (Einmalanmeldung)
- Bereitstellung von **Identifikationsverfahren** für die eindeutige Identifikation der Nutzer
- Bereitstellung starker **Authentifizierungsverfahren** (Multi-Faktor-Authentifizierung)
- **Autorisierung** der Nutzer (wer darf wann was?)
- Bereitstellung von Selbstregistrations- und Aktivierungsprozessen
- Bereitstellung eines intuitiven Self-Service Portals für die Verwaltung der digitalen Identitäten
- Validierung von Daten gegenüber Prüfregistern (Bsp. AHV-Register)
- **Zentrale Verwaltung von Vertretern**
- **Zentrale Verwaltung von Unternehmen** (juristischen Personen)
- Integration von Föderationspartnern
- Einhaltung der Datensicherheit und des Datenschutzes
- Sicherstellung der Nachvollziehbarkeit und Berichtfähigkeit

ITSENSE

Vertrauen und Sicherheit

Vertrauen und Sicherheit

Identitätsvalidierung und Überprüfung - Das IAM-System stellt sicher, dass die Identität jedes Benutzers ordnungsgemäss überprüft wird, bevor Zugriffsrechte gewährt werden.

Multi-Faktor-Authentifizierung (MFA) - Die Implementierung von Multi-Faktor-Authentifizierung (MFA) erhöht die Sicherheit, indem mehrere Identitätsnachweise verlangt werden, wie beispielsweise ein Passwort, ein Einmalpasswort per SMS oder eine biometrische Bestätigung. Authentizität bezieht sich auf die Echtheit oder Glaubwürdigkeit einer Person oder Sache.

Least-Privilege-Zugriffsprinzip - Ein IAM-System ermöglicht es, Zugriffsrechte auf verschiedene Ressourcen basierend auf den Rollen und Verantwortlichkeiten der Benutzer zu definieren und zu verwalten. Dadurch wird sichergestellt, dass Benutzer nur auf die Ressourcen zugreifen können, die für ihre Arbeit unerlässlich sind.

Benutzer- und Berechtigungsmanagement - Ein IAM-System ermöglicht die zentrale Verwaltung von Benutzerkonten und Berechtigungen. Dadurch wird sichergestellt, dass die Zugriffsrechte von Benutzern entsprechend ihren aktuellen Rollen und Zuständigkeiten angepasst werden können.

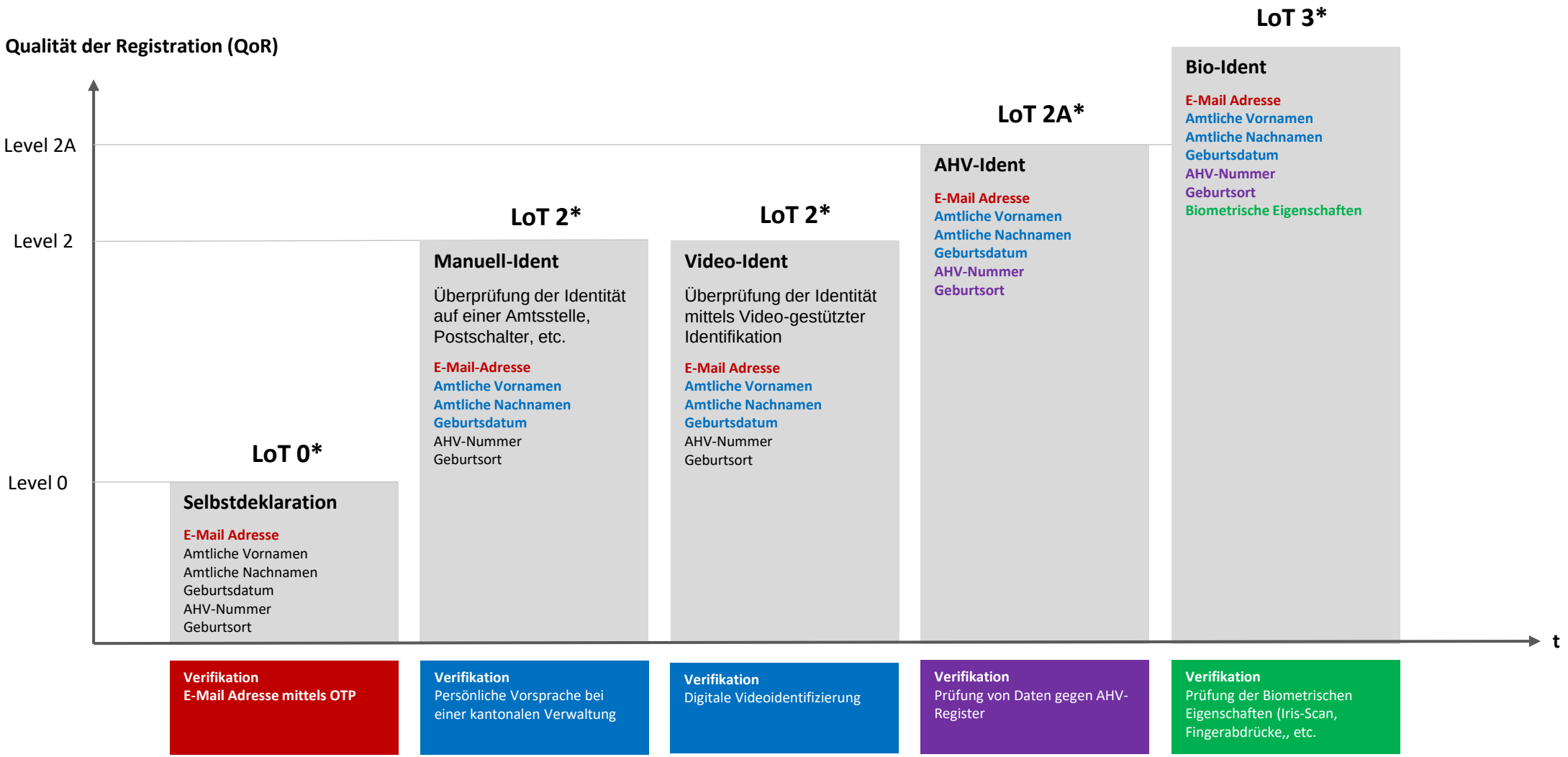
Überwachung und Protokollierung - Ein IAM-System überwacht kontinuierlich die Aktivitäten der Benutzer und protokolliert alle Zugriffsversuche sowie Änderungen an Berechtigungen. Dadurch können verdächtige Aktivitäten schnell erkannt und darauf reagiert werden.

Compliance und Richtlinienkonformität - Ein IAM-System unterstützt die Einhaltung gesetzlicher Vorschriften und branchenspezifischer Richtlinien, indem es sicherstellt, dass nur autorisierte Benutzer auf sensible Daten zugreifen können und dass die Zugriffsverwaltung den geltenden Standards entspricht.

Regelmässige Überprüfung - Ein IAM-System forciert regelmässige Attestierungen (Re-Zertifizierungen), um sicherzustellen, dass Benutzerkonten und Berechtigungen dem genehmigten Soll-Zustand entsprechen und um potenzielle Sicherheitslücken zu identifizieren und zu beheben.

ITSENSE

Level-of-Trust-Pfad im E-Government - von Zero zu 100 %



ITSENSE

* LoT: Der Level of Trust wird aufgrund der Qualität der Registration (QoR) und Quality of Authentication (QoA) bestimmt. Die Authentifizierungsstärke wird hier nicht dargestellt.

Managed Detection & Response unterstützen

IAM-Circle 3# I 14.03.2024 I öffentlich

Quelle: unsplash

Managed Detection & Responsive unterstützen

IAM kann dazu beitragen, die Effektivität von Managed Detection and Response zu verbessern. Durch die Integration von IAM-Daten in MDR-Plattformen können Sicherheitsteams verdächtige Aktivitäten schnell identifizieren und mögliche Sicherheitsverletzungen erkennen.

- **Identitätsbasierte Erkennung von Bedrohungen -** Überwachung und Protokollierung von Benutzeraktivitäten, einschliesslich Anmeldungen, Zugriffsversuchen und Änderungen an Berechtigungen.
- **Risikobasieret Zugriffskontrolle** - Anhand des "Level of Trust" einer Identität, Systems oder Netzwerkzone kann eine risikobasierte Zugriffskontrolle implementiert werden. Durch die Implementierung von feingranularen Zugriffsrichtlinien kann die Angriffsfläche verringert werden.
- **Periodische Überprüfung** - Durch regelmässige Attestierung (Rezertifizierung) von Zugriffsberechtigungen und Benutzerkonten (insbesondere externe Mitarbeiter, Guest-Accounts, etc.) können Überberechtigungen identifiziert und behoben werden, um die Sicherheit der Organisation kontinuierlich zu verbessern.
- **Sicherheitsüberprüfungen und Compliance** - Durchführung von Sicherheitsüberprüfungen und der Einhaltung von Compliance-Anforderungen, indem sie detaillierte Einblicke in die Zugriffskontrollen, Benutzerberechtigungen und Aktivitätsprotokolle bieten.

Vielen Dank.

abraxas

Delinea
Defining the boundaries of access

ti&m
big ideas. creative technology.

ARCTIC WOLF

white rabbit
Communications

TREND MICRO™

netzmedien