Controlware Security Day 2022

Identity & Access Management – Die neue Security Allzweckwaffe?

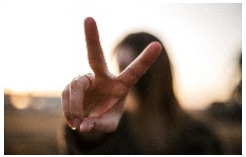
Warum Identity & Access Management eine Renaissance in der Bedeutung für die IT-Sicherheit erlebt

Benedikt Zumbrink, Controlware GmbH, Security Consultant

Controlware Security Day
22. - 23. September 2022
Congress Park Hanau

Der Fahrplan

Aufstehen – Fakten schaffen



Gehen – Status Quo

Joggen – Nach vorne sehen

Sprinten – Antworten geben

Aufstehen – Die Zeitung lesen – Fakten schaffen

Aufstehen – Die Zeitung lesen

Identität

- In der **Realität** ist eine Identität **eindeutig**
- **Attribute** oder **Eigenschaften** sind **Unterscheidungsmerkmale**
- Die Identität in der **digitalen Welt** entspricht eher einer **Rolle** in der Realität

Authentifizieren

- Sein oder nicht sein? – Das ist hier die Frage!

Aufstehen – Die Zeitung lesen

Digitale Identitäten

Attribute

- Name (**einmalig, eindeutig**)
- Stufe
- Klasse
- Vitalität, Stärke, Geschicklichkeit….
- ….

Authentifizieren

- Benutzername
- Passwort
- Chipkarten
- Authenticator Apps
- …

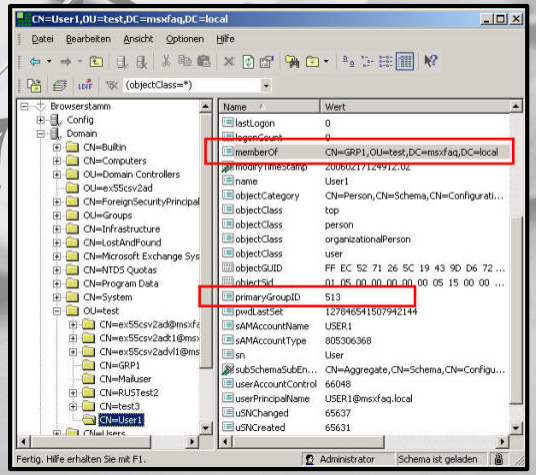
Aufstehen – Die Zeitung lesen

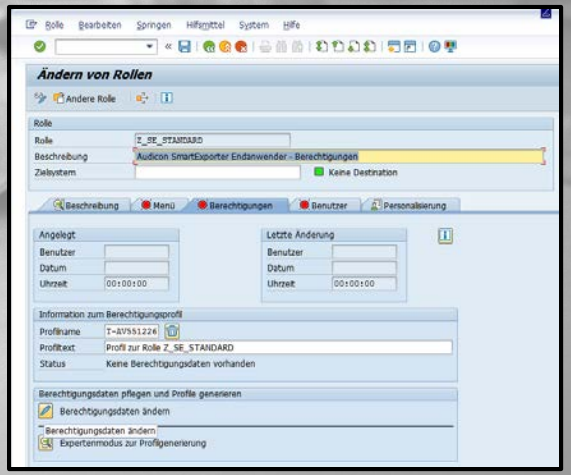
Access Management

- Beschreibt **im Alltagsleben** häufig die Möglichkeit etwas zu betreten
- Oder einen guten Platz zu ergattern…

Access Management – Digital

- **Zugriffserlaubnis**
- Häufig gruppen- oder rollenbasiert
- Was nicht explizit **erlaubt** ist, ist **verboten**





Aufstehen – Die Zeitung lesen

Access Management

- Was **darf** eine (authentifizierte) **Identität**?
  - ➢ **Autorisierung**
- **Entzug** von **Berechtigungen**

Aufstehen – Die Zeitung lesen

Ziel Identity & Access Management:

- Absicherung (von Ressourcen) vor **unerwünschtem Zugriff**

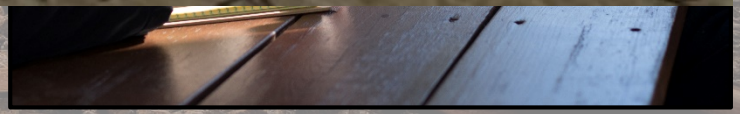
→ Das haben Tiere schon lange vor unserer Existenz durchgeführt…

→ Aber war es auch erfolgreich?

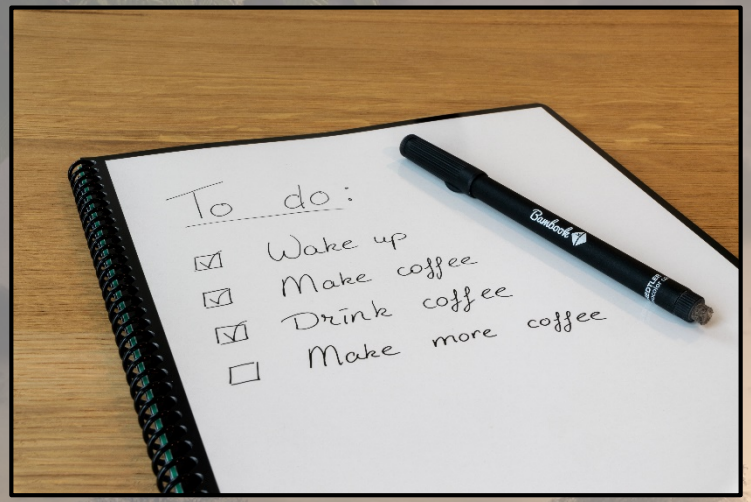
Gehen – Aller Anfang ist schwer

Gehen – Aller Anfang ist schwer

- One tool to rule them all!



Gehen – Aller Anfang ist schwer



Herausforderungen

- **Heterogenität** (HR Systeme, Zielsysteme)
- **Integration** in bestehende Arbeitsabläufe
- **Kosten**(-explosion)

Woran scheitern die aktuellen Lösungen?

- Grad der Automatisierung
- Flexibilität der Lösung
- Bedienung / Akzeptanz
- Anzahl an Aufrufen bzw. Skalierbarkeit

Joggen – Konstanz führt zum Erfolg

Joggen – Konstanz führt zum Erfolg

Erfolgsfaktoren

- Identifizierung **notwendiger** Use-Cases
- **Erleichterung** der Alltagsarbeit für Zielpersonen

→ **Automatisierung + Integration = Akzeptanz**

- **Frühzeitiges** Einbeziehen der Endanwender
- **Keine** Betrachtung des Vorhabens als **Projekt**

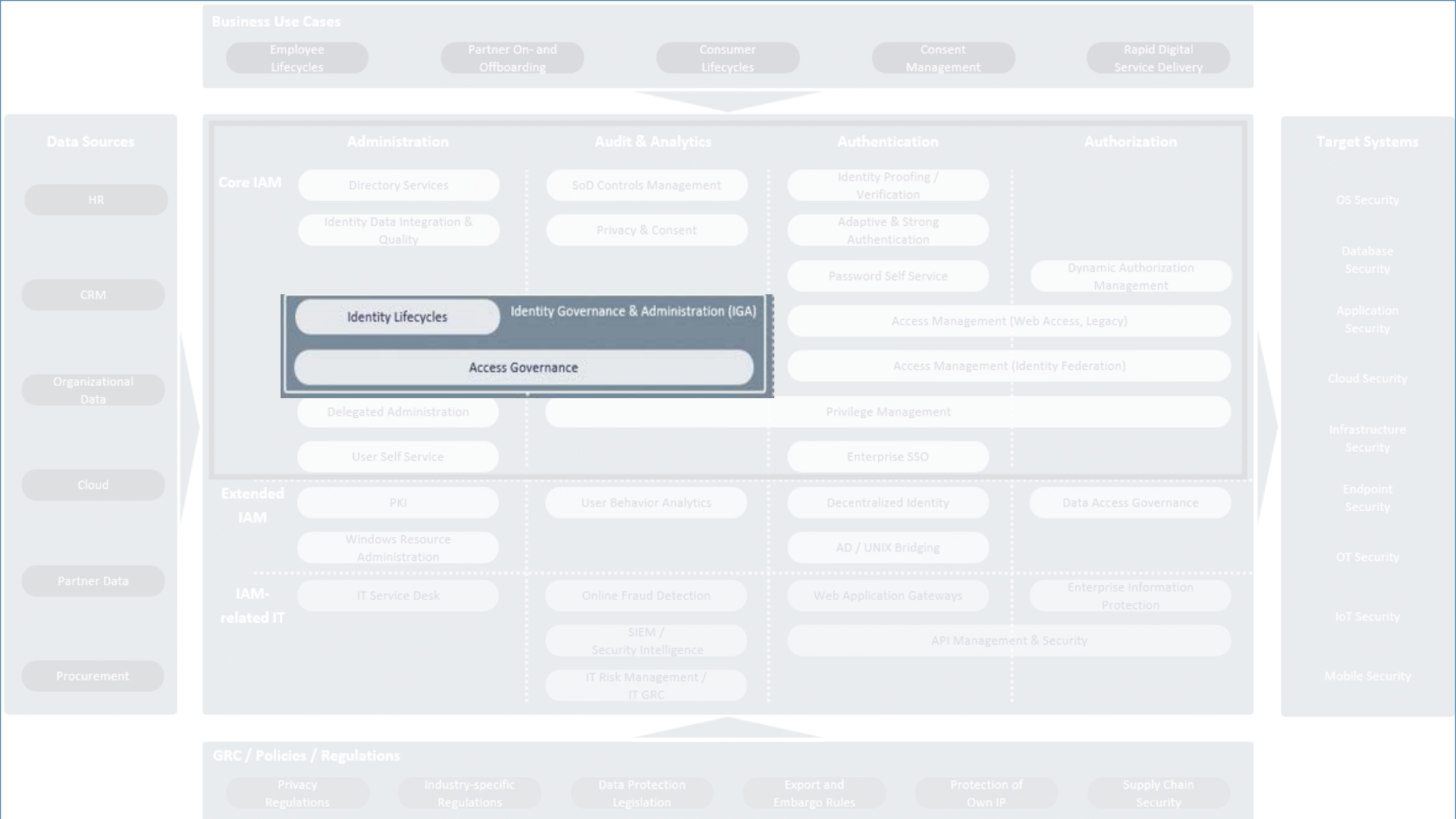
→ **Kontinuierliche** Weiterentwicklung!

- Identifizierung von **passenden** Lösungen für **notwendige** Use-Cases

Joggen – Konstanz führt zum Erfolg

Wo ist das **klassische IAM System** die **falsche Lösung?**

- Kundenmanagement
  → **C**ustomer **I**dentity & **A**ccess **M**anagement
- Management privilegierter Accounts
  → **P**rivileged **A**ccess **M**anagement
- **M**ulti-**F**aktor-**A**uthentifizierung
- Fernwartungsthemen – Partner- bzw. Supportermanagement


Business Use Cases
Employee Lifecycles
Partner On- and Offboarding
Consumer Lifecycles
Consent Management
Rapid Digital Service Delivery
Data Sources
HR
CRM
Organizational Data
Cloud
Partner Data
Procurement
Administration
Audit & Analytics
Authentication
Authorization
Core IAM
Directory Services
Identity Data Integration & Quality
SoD Controls Management
Privacy & Consent
Identity Proofing / Verification
Adaptive & Strong Authentication
Password Self Service
Dynamic Authorization Management
Identity Lifecycles
Identity Governance & Administration (IGA)
Access Governance
Access Management (Web Access, Legacy)
Access Management (Identity Federation)
Delegated Administration
Privilege Management
User Self Service
Enterprise SSO
Extended IAM
PKI
User Behavior Analytics
Decentralized Identity
Data Access Governance
Windows Resource Administration
AD / UNIX Bridging
IAM-related IT
IT Service Desk
Online Fraud Detection
Web Application Gateways
Enterprise Information Protection
SIEM / Security Intelligence
API Management & Security
IT Risk Management / IT GRC
Target Systems
OS Security
Database Security
Application Security
Cloud Security
Infrastructure Security
Endpoint Security
OT Security
IoT Security
Mobile Security
GRC / Policies / Regulations
Privacy Regulations
Industry-specific Regulations
Data Protection Legislation
Export and Embargo Rules
Protection of Own IP
Supply Chain Security

Sprinten – Das besondere Erreichen

Sprinten – Das Besondere erreichen

Warum ein neuer Security Perimeter?

- Cloud-/Hybride-Infrastrukturen
- Verschlüsselter Datenverkehr
- Work from Everywhere

Sprinten – Das Besondere erreichen

Warum Security im Umfeld von IAM?

„**Erhöhung von Berechtigungen**“ wurde als höchste Sicherheitsrisikokategorie eingestuft und betraf 2021 insgesamt **49 Prozent** aller gemeldeten Schwachstellen (Microsoft Vulnerabilities Report 2022 - BeyondTrust)

95% of privileged identities are **overprivileged** (Microsoft)

by 2023, **75% of security failures** will result from **inadequate management of identities, access, and privileges** (Gartner)

More than **90%** of identities are using less than **5% of permissions granted**, according to the report, which is based on 150 risk assessments. (CloudKnox)

61% of all breaches **involved credentials** (passwords, token, keys, and certificates) (SonicWall, Cyber Threat Report, 2022)

74% of breached organizations admitting the breach **involved** access to a **privileged account** (Verizon, Data Breach Investigations Report (2021))

42% Organisation **breached** as a result of a **user password compromise** (MobileIron)

Not only the big one suffer (Marriott, Target, Yahoo) from data-breaches; **43% of cyberattacks** aimed at SMBs (Accenture, Cost of Cybercrime Study, 2022)

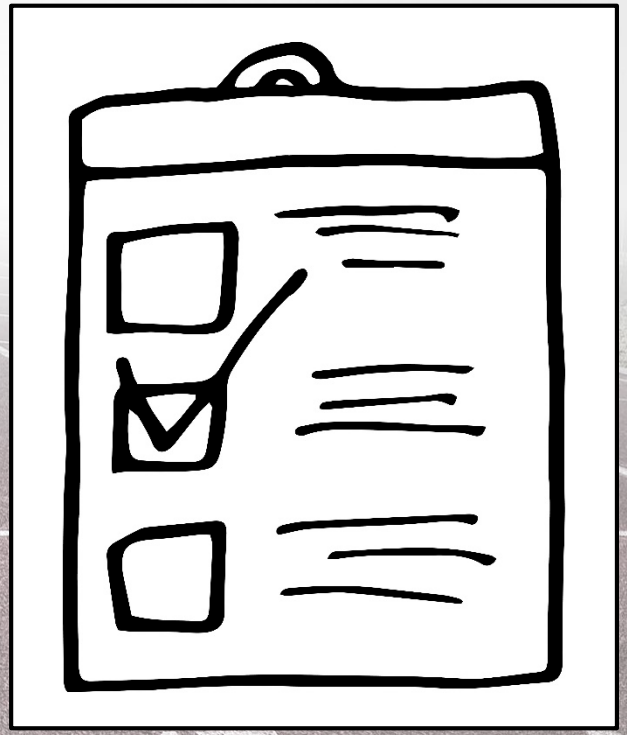
Cost of **1** data breach exceeding **4.25 million** (IBM Security, Cost of Data Breach, 2021)

Sprinten – Das Besondere erreichen

Was folgt daraus?

→ **Identitäten und Zugriffe** müssen besser gemanaged werden

- **Visibilität** und **regelmäßige** Kontrolle von **Identitäten** und **Berechtigungen**
- **Eliminierung** von **verwaisten** Accounts
- **Eliminierung** von **geteilten** Accounts
- Umsetzung des **N**eed-**t**o-**K**now bzw. **Least Privilege** Prinzips
- Etablierung von **Freigabeprozessen** für Berechtigungen
- Verwaltung **aller Identitäten** (OT, IoT, Service Accounts…)
- **Eindeutige Zuordnung** aller Identitäten



Sprinten – Das Besondere erreichen

- **Identität** als neuer **Security Perimeter**

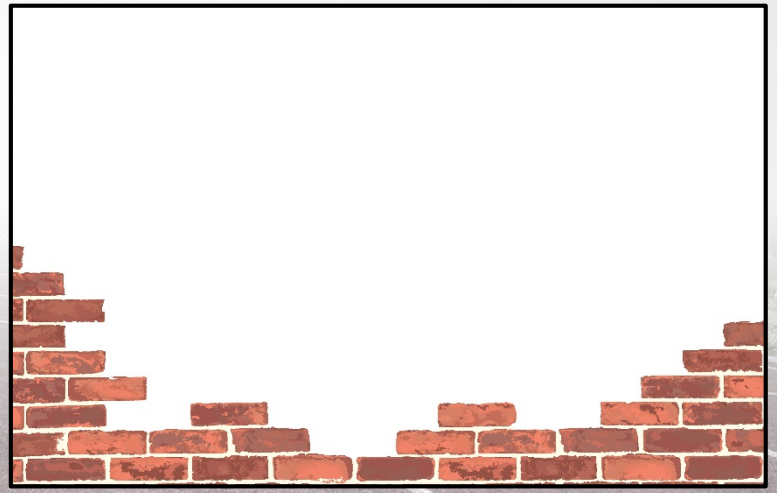
→ **Identitätsbasierendes** Access Management

- **Basis** für **Zero-Trust**

Sprinten – Das besondere Erreichen

Fazit

- Ist eine **Firewall überflüssig**?
- Ist die **Identität** der neue **Security Perimeter**?
- Stirbt der **VPN-Client** aus?
- Gibt es denn **eine** neue **Allzweckwaffe**?



Nicht

sein…

Gemeinsam
finden wir Wege,

um Ihre Ziellinie
zu durchlaufen!