SAP Security Group Deutschland

Innovation gemeinsam erleben

3./4. Juni 2025

SAP Security @ S/4 Transformationen – Mehr als nur Berechtigungen?

Bastian Becelewski (IBM), Julianna Loginova (IBM)

1. Was sich mit S/4HANA ändert
2. Warum SAP Security neu denken?
3. Rollen & Berechtigungen: Gutes Fundament, aber nicht alles
4. Cloud-basierte Security-Komponenten
5. Best Practices & Empfehlungen
6. Fazit
7. Wie kann IBM Sie unterstützen?

1. Kapitel

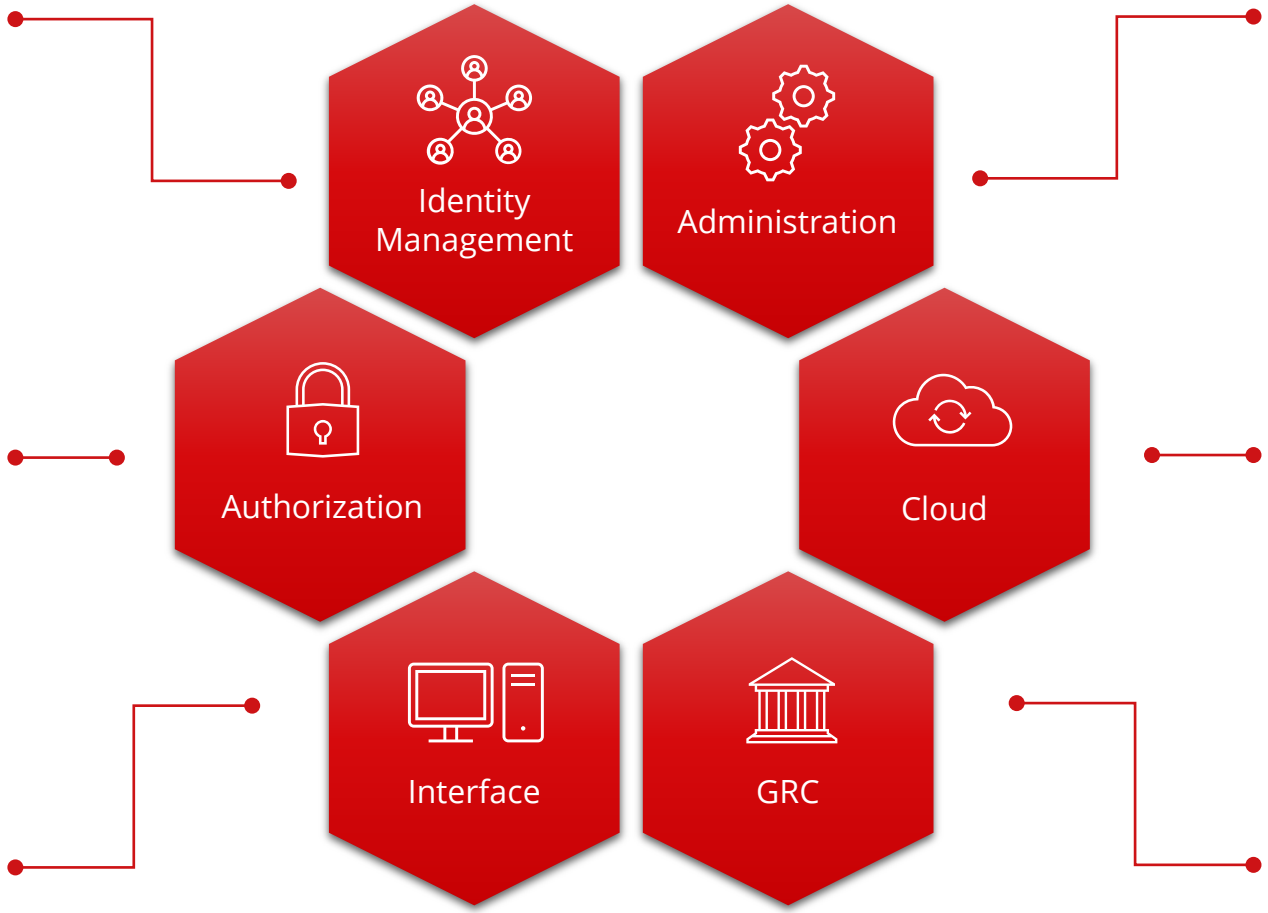
Was sich mit S/4HANA ändert

Änderungen im S/4HANA Security Management

- **Zentrale Cloud-Basierte IAM-Services** (IAS/IPS) statt dezentraler On-Premise-Lösungen
- **Modernes Authentifizierungs-Framework (**SAML, MFA, ...)

- **OData Services als Berechtigungselement** für SAP Fiori Apps
- **Fiori-Kataloge** als weitere Berechtigungsebene
- Berücksichtigung von **Front- und Backend-Berechtigungen**
- **S/4HANA Public Cloud**: Begrenzte Anpassungsmöglichkeiten, mehr Standardisierung

- **Fiori Spaces & Pages** als steuernde Elemente der User Experience
- **S/4HANA Cloud & Fiori First**: Fiori Launchpad als einziger Einstiegspunkt



- **Verteilte Systemarchitektur**: On-Premise, Cloud, Hybrid (z. B. RISE mit SAP)
- **Integration neuer Tools & Anwendungen**: SAP BTP, SAP Fiori, Cloud Connector, Identity Services
- **Neue Lizenzmodelle:** Nutzungs- und rollenbasiert

- Unterstützung **hybrider Security-Modelle** mit Cloud Connector, IAS/IPS
- **Sicherstellung konsistenter Sicherheitsrichtlinien** zwischen On-Premise und Cloud

- **GRC 12.0-Integration** mit neuen Regeln und Prozessen in S/4HANA
- **Neue SoD-Regeln** aufgrund geänderter Rollen- und Prozesslandschaft
- **Echtzeitkontrollen und Compliance-Monitoring**

Was sich mit S/4HANA ändert – Vergleich mit ECC

Bereich	Früher (SAP ECC / On-Prem)	Was ist neu ? (S/4HANA / Cloud-ready)
Benutzeroberfläche	**SAP GUI** mit Transaktionscodes	**SAP Fiori** – moderne Web-Apps mit Kacheln
Zugriffssteuerung	Transaktionen über Rollen erlaubt	Apps + Daten + Services müssen **getrennt berechtigt werden**
Datenzugriff	Tabellen und Reports	Core Data Services (CDS)-Views – **Zugriff muss separat geregelt werden**
Schnittstellen	RFC, BAPI, **selten API**	Mehr **API, REST, ODATA** – oft öffentlich zugänglich
Integration	In sich geschlossen, **selten externe Tools**	**Starke Cloud-Integration** (Entra, BTP, 3rd-Party-Systeme)
Identitätsverwaltung	Benutzer **direkt im SAP** (IdM) gepflegt, lokale Verwaltung	**Zentrale Verwaltung** in der Cloud (z. B. Entra ID, SAP IAS/IPS)
Sicherheitsmodell	**Netzwerktrennung**, klassische Firewalls	**Zero Trust Prinzipien**, API Security, Web-basierte Authentifizierung **(SSO, OAuth, MFA)**
Security-Fokus	„Wer darf rein?“ (Login & Rolle); **Manuelle Reports**, **begrenzte Transparenz**	„Wer darf was, wie, von wo, über welchen Kanal?“ – **Echtzeit Reports**
Risiken	**Begrenzte Angriffsfläche** (internes System)	**Offenere Systeme** = mehr Einfallstore = mehr Absicherung nötig

Ein umfassendes Sicherheitskonzept ist mehr als gefragt!

2. Kapitel

Warum SAP Security neu denken?

Security muss mit der Transformation mitwachsen

Warum SAP Security neu denken?

1. Weil die Systemwelt sich grundlegend verändert	Sicherheit muss heute **überall** greifen – nicht nur im internen Netzwerk
2. Weil Risiken heute dynamischer und verteilter sind.	**Alte Sicherheitsmodelle** wie „eine Rolle, ein Nutzer“ reichen nicht mehr
3. Weil Compliance und Audit Unternehmen Druck machen.	Security wird prüfbar und die **Prüfungen werden strenger**
4. Weil Identitäten der neue „Schlüssel“ sind	Wer die Identitäten nicht im Griff hat, **verliert die Kontrolle** über den Zugriff.

S/4HANA bedeutet nicht nur neue Technik – es bedeutet, dass **Security ein neues Denken** braucht: cloudfähig, ganzheitlich, identitätszentriert und auditfest.

3. Kapitel

Rollen & Berechtigungen – Fundament, aber nicht ausreichend

Security Layers – S/4HANA

SAP Security

- Identitäts- & Zugriffskontrolle
- Security Logging und Monitoring
- Systemhärtung und Secure Configuration
- Custom Code Security

- Schnittstellen- und API-Sicherheit
- Schwachstellen- und Patchmanagement
- Cloud Integration und Hybrid Security
- Awareness und Prozesssicherheit

Rollen & Berechtigungen

4. Kapitel

Cloud-basierte Security-Komponten

Effektive Sicherheit braucht cloud-native Tools & Prinzipien

	User Access & Permission	Communication & Encryption	Auditing & Monitoring	Secure Connectivity	Secure Development & Operations
	Restriktion verhindert Missbrauch & Risiken	Datenschutz & Compliance durch Verschlüsselung	Schnelle Reaktion auf Bedrohungen	Schutz vor Angriffen & Datenlecks	Sichere Apps reduzieren Schwachstellen
SAP-eigene Tools	**SAP Cloud Identity Services** • Identity Authentication (IAS) • Identity Provisioning (IPS) • Identity Directory • Authorization Management	**SAP Credential Store**	**SAP Audit Log Service**	**SAP BTP Connectivity Services**	**SAP Code Vulnerability Analyzer**
		SAP Custom Domain Service	**SAP Governance, Risk, and Compliance (GRC)**	**SAP Cloud Connector**	**SAP Cloud ALM**
		SAP Cryptographic Library	**SAP Enterprise Threat Detection (ETD)**	**SAP Web Dispatcher**	
	SAP Access Control	**SAP Secure Login Server**	**SAP Solution Manager**	**SAP API Management**	**SAP Business Application Studio**
Drittanbieter (Beispiel)	Microsoft Entra ID, Saviynt, ONE IDENTITY, SailPoint	Vormetric Data Security, ENTRUST, Symantec, HashiCorp Vault	splunk>, ONAPSIS Security Bridge, Microsoft Sentinel	PRISMA, f5, CISCO AnyConnect Secure Mobility, zscaler	Checkmarx, aqua, ONAPSIS Security Bridge, GitHub

5. Kapitel

Best Practices

Best Practises in S/4HANA Security

- **Security by Design**
  - Security als integraler Bestandteil, d.h. von Anfang an in die Transformationsplanung integrieren
  - Klare Definition von Schutzbedarf, Systemklassifizierung und Bedrohungsszenarien

- **Rollen & Berechtigungen neu denken**
  - Altdaten und -rollen nicht unreflektiert übernehmen (Nutzung & Pflege der SU24 bei Redesign)
  - Modellierung risiko- und joborientierter Rollen (z. B. nach SoD-Prinzip)
  - Nutzung moderner Tools (GRC, XAMS, IDM) zur Automatisierung und Qualitätssicherung

- **Ganzheitlicher Sicherheitsansatz (Beyond Authorization)**
  - Absicherung von End-to-End-Prozessen (z. B. Bestellprozesse, Benutzerpflege)

- **Cloud Security und Hybrid-Architekturen absichern**
  - BTP-Subaccounts, Cloud Connector, APIs und Integrationen konsequent absichern (TLS, OAuth, IP-Whitelisting)
  - Harmonisierung des Rollenmodells in Cloud-Diensten
  - Klare Trennung von Sicherheitszonen

Best Practises in S/4HANA Security

- **Standardisierung & Automatisierung der Security Prozesse**
  - Automatisierte Joiner/Mover/Leaver-Prozesse für Benutzerverwaltung
  - Genehmigungsworkflows für Berechtigungsanträge mit integrierter Risikoprüfung
- **Aktive Nutzung des Monitorings & Auditing**
  - Regelmäßige Auswertung sicherheitsrelevanter Logs (Audit Log, STAD, ETD, SIEM)
  - Implementierung von Alarmen bei kritischen Aktionen
- **Kontinuierliche Pflege der technischen Sicherheit**
  - Systemhärtung nach SAP Security Baseline umsetzen (Services, Protokolle, TLS)
  - Schwachstellenmanagement etablieren (Monatliche Patchzyklen, CVE-Monitoring)
- **Schaffung von Awareness und Verankerung von Governance**
  - Klare Definition von Verantwortlichkeiten für SAP Security (CISO, SAP Security Officer etc.)
  - Regelmäßige Schulungen und Sensibilisierung für Admins, Key-User & Entwickler
  - Etablierung von SAP Security als fester Bestandteil der Unternehmens-IT-Governance

6. Kapitel

Fazit

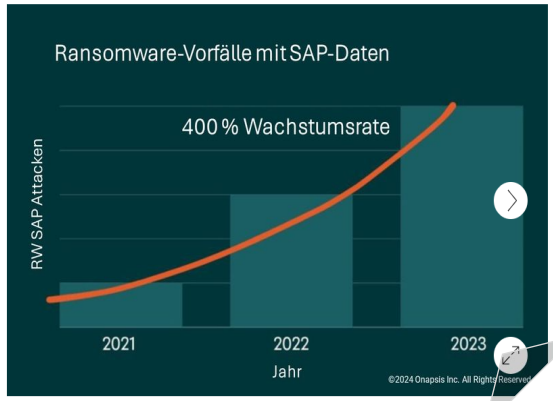
Fazit

> “Security is not a product, but a process.” – Bruce Schneier

Ausblick & zukünftige Herausforderungen:

- **Security als Business Enabler:** Sicherheit nicht als Bremse, sondern als Teil digitaler Resilienz verstehen
- **Shift Left in der Security:** Sicherheitsprüfungen früh im Entwicklungs- und Migrationsprozess verankern
- **Cloud & Hybrid werden Standard:** Komplexität durch hybride Landschaften
- **Zunehmende Automatisierung & Integration** = mehr Angriffsfläche
- **Steigende regulatorische Anforderungen & Prüfstandards:** Revisionssichere Rollenkonzepte & IAM-Prozesse sind Pflicht
- **Kritische Infrastrukturen:** SAP-Systeme geraten zunehmend in den Fokus gezielter Angriffe

Ransomware-Angriffe auf SAP-Systeme nehmen stark zu



Die Ransomware-Vorfälle, bei denen SAP-Systeme und -Daten kompromittiert wurden, sind seit 2021 um

Quelle: https://www.digitalbusiness-magazin.de/

S/4-Projekte brauchen einen ganzheitlichen Security-Ansatz, der Architektur, Prozesse, Benutzer und Schnittstellen gleichermaßen adressiert und als integraler Bestandteil eines Transformationsprojekts fungiert.

7. Kapitel

Wie kann IBM Sie unterstützen?

Beratung, Implementierung und Managed Services

Beratung & Implementierung → **Managed Services / Support & Operation**

Risiken & Regulatorische Vorgaben

- Identifikation im Compliance-Kontext des Kunden für die relevanten SAP-Systeme
- Risikobasierter Ansatz zur Einhaltung von Finanz- und IT-Sicherheitsvorgaben – zentral und einheitlich umgesetzt

Einsatz verschiedener Ansätze:

- **SAP Rapid Discovery**
- **SAP Data Privacy Discovery**
- **SAP Cybersecurity Assessment**
- **SAP ETD Discovery**
- **SAP DevSecOps Discovery**
- Architektonische Überlegungen

Lösungen & Kontrollen

- Umsetzung von SAP Security-Lösungen und –Kontrollen
- Umsetzung der als erforderlich identifizierten Risiken und Kontrollen gemäß den unterschiedlichen, für den Kunden relevanten Regulatorien

SAP Security Tools & Kontrollen:

- **Access Management & SoD**
- **Authentication**
- **Data Protection (Personal / Business)**
- **Other Regulatory Controls**
- **Security for Interfaces**
- **Secure Code (SDLC)**
- **Definition der SAP Security Baseline**

Security Hardening

- Erhöhung der Cybersicherheit von SAP-Systemen durch erweiterte Konfiguration
- Umsetzung von SAP-Cybersicherheitskontrollen zum Schutz von Daten
- Tests der Sicherheitsmaßnahmen vor dem Go-Live der SAP-Systeme

SAP Cybersecurity Mechanismen:

- **Implementierung der SAP Security Baseline**
- **Durchführung vom Vulnerability Assessment**
- Durchführung von Penetration Tests
- SAP patching process of key OSS
- Implementierung einer automatisierten Security Monitoring Plattform

Bedrohungen & Angriffe

- Laufende Sicherheitsunterstützung zur Prävention, Erkennung und Abwehr von Bedrohungen und Angriffen
- Identifikation von Mustern, die auf Angriffe auf die Systemlandschaft hinweisen könnten – auf Applikations-, Datenbank- und Netzwerkebene

Monatlicher lifecycle:

- **Update der SAP Security Baseline**
- **SAP Cybersecurity Managed Service:**
  - **SAP Vulnerability Management**
  - **SAP Threat Management**
  - **SAP DevSecOps / SDLC**
  - **Definition von Action Plans**
- **Remedial Actions follow-up**

Vielen Dank für Ihre Aufmerksamkeit!

Q&A