11.05.2023

Breakout Session 1 – SAP und IT Security

SAP und IT Security Packages für SAP-Systemlandschaften – Security Offerings und Services, die Ihre Daten und Ihr Unternehmen schützen

Scheer

Referenten

Heiko Bach

Unit Leader SAP Operations
Managed Services

Daniel Schillinger

Unit Leader Cloud / Datacenter Operations
Managed Services

Secure Operations Map

Organization	Awareness	Security Governance	Risk Management	
Process	Regulatory Process Compliance	Data Privacy & Protection	Audit & Fraud Management	
Application	User & Identity Management	Authentication & Single Sign-On	**Roles & Authorizations**	Custom Code Security
System	Security Hardening	**Secure SAP Code**	**Security Monitoring** & Forensics	
Environment	**Network Security**	Operating System & Database Security	Client Security	

Was sind die Herausforderungen bei SAP-Security?

- Security ist keine Eigenschaft, die man hat oder nicht hat. Sie ist eine Risikomaßnahme, bei der Sie ein höheres oder niedrigeres Maß an Sicherheit haben können.
- Maximale Sicherheit ist oft nicht das, was die Kunden wollen, da dies einen hohen Aufwand erfordert und die Funktionalität einschränken kann. Sie benötigen eine angemessene Sicherheit.
- Setzt man sich mit dem Thema Berechtigungskonzept detailliert auseinander, entdeckt man sehr schnell Schwachstellen in den Abläufen (wenn sie denn dokumentiert sind), z.B. Berechtigungsbeantragung und -erweiterungen. Deshalb muss das, was im Berechtigungskonzept beschrieben ist, auch umgesetzt und reviewt werden.

Was sind die Herausforderungen bei SAP-Security?

- Große Bandbreite an individuellen Unternehmenslösungen
- Verschiedenste Verantwortlichkeiten
- Unterschiedlichste Anforderungen ans SAP-System
- Unterschiedlichste Funktionen und Dienste welche sehr häufig das gesamte Unternehmen abbilden
- Verteilte Lösungen und Integration von Cloud Diensten
- SAP-Security ganzheitlich betrachten
  - Sicherheit der Infrastrukturkomponenten
  - Anwendungsebene
  - Systemhärtung
  - etabliertes Patch Management
  - Analyse der Systemkonfiguration
  - Erkennung von Angriffen
  - Analyse von Schwachstellen
- Events aus verschiedenen Systemen ganzheitlich Betrachten
- Evaluieren von Risiken durch einheitliche Übersicht über Infrastruktur, Applikation & Konfiguration
- Überblick im Dschungel der Informationen

Scheer Boxes

Wie unterstützt Scheer im Bereich Managed SAP Security

SEC-Basic

Managed SAP Security Service
- Security by default (für S4HANA)
- SAP-Security Checks (Monatliche Security Prüfungen; Security Audit Log; Scheer Security Policy)
- SAP Hana Patching
- Netzwerk IDS/IPS
- Betriebssystemhärtung/Patching
- Schwachstellenmanagement

SEC-NET

Erweiterte Netzwerksicherheit
- Microsegmentierung auf System-Ebene
- Web-Proxy
- Web Application Firewall (WAF)

SEC-Enhanced

Erweiterter SAP Security Service
- SAP Security Baseline Check
- Security Reporting

Scheer Boxes

Wie unterstützt Scheer im Bereich Managed SAP Security

SEC-R&A

SAP Security Service "Rollen & Berechtigungen mit Xiting (AddOn)"

- Berechtigungskonzept vereinfachen mit XITING AUTHORIZATIONS MANAGEMENT SUITE (XAMS) – „Anpassung des Berechtigungskonzeptes für S/4HANA“
  - Automatisierte Abarbeitung der Simplification List
  - Toolgestützte Rollenanpassungen
  - Fiori-App Tracker
- Scannen des SAP-Systems mit Hilfe von XAMS
  - Überprüfung der Berechtigungen auf Qualität und IKS-Konformität
  - Überprüfung der technischen Absicherung des Produktivsystems
  - Überprüfung der Aktualität und Korrektheit des SAP-Berechtigungskonzeptes
- Dauerhafte Compliance: Unterstützung Projektphase sowie nach dem Projekt zur Überwachung der Systeme

SEC-SIEM

Erweiterte SIEM-Integration

Standard

- Sammeln/Auswerten von Protokollen auf Anwendungsebene
- Incident-Response for SIEM

Advanced (XAMS)

- Standard SIEM Systeme kennen die SAP Anwendung nur bedingt
- Zugriff auf spezifische SAP Funktionen und Meldung an das SIEM System
- Verlagerung der Logik zur Erkennung der möglichen Angriffe ins SAP-System

Szenario in der Praxis

- **Security Operation** als ganzheitlicher Ansatz
  - Aufbau, Betrieb und Wartung dedizierter DMZ-Lösungen („Security Hub“)
    - Firewall Betrieb
    - Web-Proxy Betrieb
    - DNS-Betrieb
    - Betrieb eines SIEM-Systems
    - …
  - Security Incident Response
    - Monitoring von Services durch die im Security Hub eingesetzten Security Tools
    - Reaktion auf Alarme (Events) der im Security Hub eingesetzten Security Tools und entsprechende Priorisierung
  - Erstellung eines regelmäßigen Sicherheitsreports
  - Prüfung der Security-Regeln, Firewall Regelwerk etc. inklusive Report
  - Regelmäßiges Review des Security Hub Aufbaus

Was haben die SAP-Anwender davon?

- Vereinfachte und schnellere S/4-Transformation von Rollen und Berechtigungen
  - Schnelle Analyse der beteiligten Rollen zur Ermittlung der Auswirkungen einer Migration auf SAP S/4HANA
  - Effizientere Durchführung der Rollenmigration durch einen automatisierten Abgleich mit der SAP Simplification List
  - Kürzere Vorlaufzeiten bei der Anpassung von SAP-Rollen im Rahmen der Migration des Berechtigungskonzepts

- Vollständige Dokumentation
  - Aktuelles und gut dokumentiertes Berechtigungskonzept. Ein gutes Berechtigungskonzept lässt sich einfacher und schneller migrieren.
  - Reduzierung von Sicherheitsrisiken. Parametereinstellungen werden dabei auch gegen allgemeine Empfehlungen geprüft.
  - Sicherheit schützt nicht nur vor böswilligen Angriffen, sondern auch vor unbeabsichtigten Fehlern.

- Bestmögliche SIEM-Integration ins SAP-System und den Überblick im Dschungel der Informationen

Empfehlung

- Thema SAP-Security sollte ganzheitlich betrachtet werden
- Angefangen bei der Sicherheit der Infrastrukturkomponenten sowie die Betrachtung auf Anwendungsebene
- Eine sehr effektive Maßnahme verdächtigen Vorgängen zu erkennen und Risiken zu minimieren, ist die Implementierung eines SIEM-Systems mit entsprechender Integration ins SAP-System mit zusätzlicher XAMS-Integration.
- Unterschätzen Sie nicht den Wert eines gut dokumentierten und gelebten Berechtigungskonzeptes. Es hilft Ihnen dabei Ihre Systeme sicherer zu machen.