SAP Security Group Deutschland

Innovation gemeinsam erleben

3./4. Juni 2025

SAP Security: Last-Minute-Tipps, bevor die Prüfer kommen

Lucas Hoppe

Was Sie heute erwartet

01 **Wahrnehmung und Ziele eines IT-Audits**
Worum es eigentlich geht

02 **Die TOP 6 Prüfbereiche und typische Findings**
Worauf die Prüfer achten

03 **Das machen unsere Kunden**
Kundenbeispiel JOST-Werke Deutschland GmbH

04 **Last-Minute-Tipps, bevor die Prüfer kommen**
Darüber freuen sich die Prüfer

Wahrnehmung und Ziele eines IT-Audits

Audit oder Wirtschaftsprüfung wird oft als etwas Negatives empfunden

- Kontrolle (der eigenen Arbeit)
- Stress & mehr Arbeitsaufwand durch Zuarbeiten & für Behebung der Findings
- Erzeugt keinen Fortschritt im Tagesgeschäft
- Anforderungen (z. B. neue Prozesse oder Arbeitsschritte), die Prüfer verlangt, steigern Komplexität

Das Ziel eines Audits und eine andere Sichtweise

- Ziel: Buchführung und Jahresabschluss vollständig, richtig und zuverlässig?
- Sollte auch Eigeninteresse sein
- Besser proaktiv als reaktiv arbeiten
- Prüfungen orientieren sich an gesetzl. Standards und Branchenstandards
- Vermeidet Findings & Mehraufwand mit Prüfung und Stress

Was Sie heute erwartet

01 **Wahrnehmung und Ziele eines IT-Audits**
Worum es eigentlich geht

02 **Die TOP 6 Prüfbereiche und typische Findings**
Worauf die Prüfer achten

03 **Das machen unsere Kunden**
Kundenbeispiel JOST-Werke Deutschland GmbH

04 **Last-Minute-Tipps, bevor die Prüfer kommen**
Darüber freuen sich die Prüfer

Die Top 6 Prüfbereiche eines SAP Audits

- Berechtigungen
- Benutzer
- System-konfiguration
- Patching
- Prozesse & IKS
- Logging & Monitoring

Die Top 6 Prüfbereiche eines SAP Audits

Was wird geprüft?

- Kritische Berechtigungen
- Funktionstrennungskonflikte (SoD – Segregation of Duties)

Welche Risiken gibt es?

- Ungenehmigter Zugriff auf Daten oder Systemfunktionen
- Beeinträchtigung der Daten- und/oder Systemintegrität

→ Geld wird gestohlen

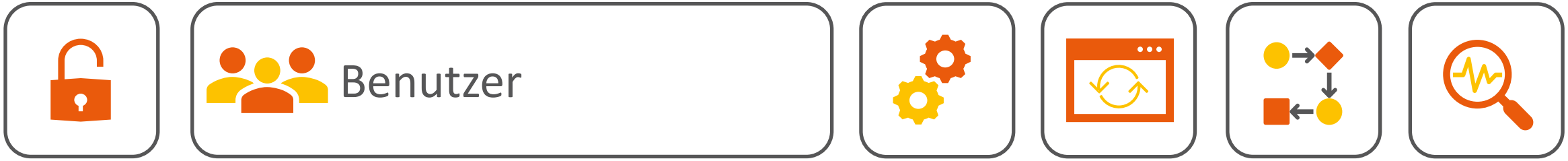
Typische Findings?

- SAP_ALL
- Tabellenpflege, Reportausführung, Entwicklung
- SoDs in Basis & FI-Bereich

Was können Sie tun?

- Rechtvergabe nach Minimal-/Funktionstrennungsprinzip
- Notfalluser bereitstellen
- Prüfung: Vergabe von kritischen Berechtigungen
  - SUIM: Benutzer nach kritischen Berechtigungen
  - Nutzung von Tools mit umfangreichen Regelwerken

Die Top 6 Prüfbereiche eines SAP Audits



Was wird geprüft?

- SAP Standard User (z. B. DDIC, SAP*)
  - Umfangreiche Berechtigungen, bekannte Initialpasswörter
- Zustand inaktive User

Welche Risiken gibt es?

- Unbefugter Systemzugriff gefährdet Integrität, Verfügbarkeit und Vertraulichkeit von Daten

Typische Findings?

- SAP Standarduser mit Initialpasswort & nicht gesperrt
- Nicht gesperrte/gelöschte inaktive User
  - Überprüfung des letztens Logins
  - Direkter Zugriff auf Cloud-Anwendungen ohne VPN oder zusätzliche Schritte aus dem Internet

Was können Sie tun?

- SAP Standard User sperren & Kennwortänderung (Report: RSUSR003) → auch nicht produktive Mandanten
- Festlegung klarer Offboarding-Prozesse für Mitarbeiter
- Report RSUSR_LOCK_USERS sperrt inaktive User nach X Tagen

Die Top 6 Prüfbereiche eines SAP Audits

Was wird geprüft?

- Einstellungen der SAP-Systemparameter (RZ10/RZ11)
- Verschlüsselung von RFC-Schnittstellen

Welche Risiken gibt es?

- Unbefugter Zugriff auf das System von außen
- Keine Nachvollziebarkeit kritischer Aktivitäten auf dem System
- Passwörter & Kommunikation können abgehört werden

Typische Findings?

- Parameter zur Authentifizierung (Passwörter, Login-Regeln)
- Schnittstellen sind unverschlüsselt

Was können Sie tun?

- Report RSPFRECOMMENDED prüft Parameter-Mindestkonfiguration der SAP
- Aufbau einer Baseline (Regelwerk zur Systemkonfiguration) nach z. B. DSAG-Prüfleitfaden
- Regelmäßige Überprüfung der Einstellungen

Die Top 6 Prüfbereiche eines SAP Audits

Was wird geprüft?

- Update Status des SAP-Systems
- aktuellste SAP Security Notes & Hinweise eingespielt?
  - SAP Security Patchday: jeden zweiten Dienstag im Monat

Welche Risiken gibt es?

- Bekannte & öffentliche Sicherheitslücken werden ausgenutzt
- Effizienzverlust, da neueste Systemfunktionen nicht genutzt werden

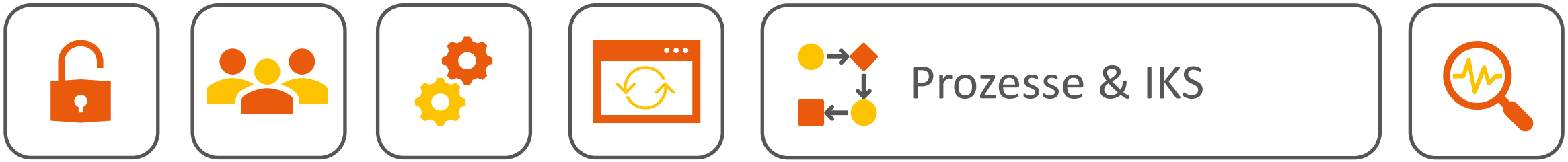
Typische Findings?

- Kein Patching-Prozess definiert
- Aktuellste Security Patches sind nicht eingespielt

Was können Sie tun?

- Etablierung eines klaren Prozesses zur regelmäßigen Überprüfung und Implementierung von Patches
- Mit Tools: Unterstützung bei Prüfung der Relevanz neuer Patches für das eigene System
- Möglichkeit zur automatisierten Überwachung

Die Top 6 Prüfbereiche eines SAP Audits



Was wird geprüft?

- Benutzer & Berechtigungsprozesse
- Notfalluserprozesse
- Transportprozesse
- Entwicklungsprozesse/-richtlinien

Welche Risiken gibt es?

- Verschlechterung der bestehenden Konzepte im System
- Keine Nachvollziebarkeit von Änderungen
- Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten

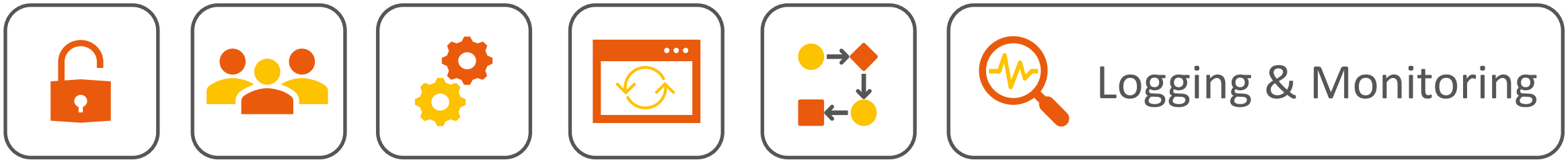
Typische Findings?

- Unterschied gelebter Prozess zu dokumentiertem Prozess
- Keine Verwendung von Standardformularen
- Freigaben erfolgen nicht oder durch falsche Personen

Was können Sie tun?

- Prozesse sauber definieren, dokumentieren und leben
- Standardformulare, Beantragungen, Freigaben durch Verantwortliche umsetzen

Die Top 6 Prüfbereiche eines SAP Audits



Was wird geprüft?

- Überwachung/Monitoring von kritischen Systemaktivitäten

Welche Risiken gibt es?

- Unvollständige Logs beeinträchtigen die Nachverfolgung von sicherheitskritischen Aktivitäten im System
- Verzögerte oder keine Erkennung von Systemangriffen durch keine/unregelmäßige Auswertung der Logs

Typische Findings?

- Logs (z. B. Security Audit Log SAL) ist nicht oder nicht vollständig/richtig eingerichtet
- Log wird nicht oder nicht regelmäßig ausgewertet (kein Auswertungsprozess)

Was können Sie tun?

- Konfiguration des SAL
- Aufbau eines Prozesses zur regelmäßigen Auswertung des SAL und der Nachverfolgung von kritischen Aktivitäten
- Auswertung über ein Tool oder als externer Managed Service

Was Sie heute erwartet

01 **Wahrnehmung und Ziele eines IT-Audits**
Worum es eigentlich geht

02 **Die TOP 6 Prüfbereiche und typische Findings**
Worauf die Prüfer achten

03 **Das machen unsere Kunden**
Kundenbeispiel JOST-Werke Deutschland GmbH

04 **Last-Minute-Tipps, bevor die Prüfer kommen**
Darüber freuen sich die Prüfer

Kundenbeispiel: SAP Einbruchserkennung – SAP Basis Abteilung

Unternehmenseckdaten

- **Kunde:** Jost-Werke GmbH
- **Branche:** Automobilzulieferer
- **Mitarbeiter:** ca. 3.600
- **Umsatz:** ca. 1,2 Mrd. €
- Hersteller von Systemen für Nutzfahrzeuge

Beratung zur SAP Security Logauswertung

1. Überprüfung der Logkonfiguration und gemeinsame Planung der Auswertung in einem SAP Security Check
2. Initiale Auswertung der Logdaten – manuell & mit Tool
3. Feststellung: Auswertung (auch mit Tool) erfordert viel Security-Wissen und ist aufwendig

Herausforderungen

- Keinen Überblick über sicherheitskritische Aktivitäten im SAP-System
- Prüfung fordert eine aktive Auswertung der SAP Security Logdaten
- Keine Kapazität & kein Knowhow in der SAP Basis, um die Daten selbst auszuwerten

Ablauf der SAP Security Logfile-Überwachung bei Jost

Protokollierung
Sicherheitsprotokolle Ihrer SAP-Systeme werden durch eine spezifische Software gescannt

Auswertung
Verdachtsfälle müssen mithilfe des Tools und Detailanalysen bewertet werden

Reporting & Empfehlungen
Regelmäßiges Reporting an das Management und Cybersecurity mit passenden Maßnahmen zur Behebung

Gezielte Maßnahmen
Entscheidung zur Durchführung von Ad-Hoc-Maßnahmen oder generellen Überarbeitung von Sicherheitseinstellungen

Kundenbeispiel: SAP Einbruchserkennung – SAP Basis Abteilung

LINKED EVENTS

System	Time	Severity	Listener	User & Terminal	Message
AED	**08.04.2024**	—	**1081**	**KHILVA** DESKTOP-IRF6F4F	The event no longer exists
SJ1	**08.04.2024**	—	**3000**	**SJ1LPUSER@1**	The event no longer exists
S4D 100	**02.07.2024** 16:31:18	Low (3)	**1011** Job scheduling	**DDIC** SRV03S4D1	Job SAP_ISLM_SCHEDULER is created and running with user (DDIC) on S[redacted] system. Technical jobs with user DDIC shall run on client 000. Instead of using user DDIC we recommend a different technical user. Password not trivial
SM1 001	**02.07.2024** 16:36:01	High (8)	**1011** Critical RFC/CPIC Logon	**SOLMAN_BTC** SRV01SM1.NCMI.CO	Critical user RFC login via internal call. Not Locked
SB-DEV	**02.07.2024** 16:42:18	Low (3)	**4000** Token issued event	**SB-NA-D4995179-AC8E-467A-BCAE-38D052140798!A189226**	Token issued event ('["xs_ user .write","uaa.resource","xs_authorization.read","xs_idp.write","xs_ user .read","xs_idp.read","xs_authorization.write"]'): principal=sb-na-d4995179-ac8e-467a-bcae-[redacted]
SM1 001	**02.07.2024** 18:35:06	High (8)	**1011** Critical RFC/CPIC Logon	**SOLMAN_BTC** SRV01SM1.NCMI.CO	Critical user RFC login via internal call. Not Locked

Kundenbeispiel: SAP Einbruchserkennung – SAP Basis Abteilung

Unternehmenseckdaten

Kunde: Jost-Werke GmbH
Branche: Automobilzulieferer
Mitarbeiter: ca. 3.600
Umsatz: ca. 1,2 Mrd. €
Hersteller von Systemen für Nutzfahrzeuge

Beratung zur SAP Security Logauswertung

1. Überprüfung der Logkonfiguration und gemeinsame Planung der Auswertung in einem SAP Security Check
2. Initiale Auswertung der Logdaten – manuell & mit Tool
3. Feststellung: Auswertung (auch mit Tool) erfordert viel Security-Wissen und ist aufwendig

Herausforderungen

- Keinen Überblick über sicherheitskritische Aktivitäten im SAP-System
- Prüfung fordert eine aktive Auswertung der SAP Security Logdaten
- Keine Kapazität & kein Knowhow in der SAP Basis, um die Daten selbst auszuwerten

Ergebnisse & Nutzen

- ✓ Service zur regelmäßigen Auswertung ist aktiv
- ✓ Sicherheitskritische Aktivitäten werden zeitnah erkannt
- ✓ Gewissheit, dass das System nicht kompromittiert ist
- ✓ Stress durch den Prüfer beseitigt
- ✓ Interne Mitarbeiter können sich weiter auf Projekte und Innovationen fokussieren

Was Sie heute erwartet

01 **Wahrnehmung und Ziele eines IT-Audits**
Worum es eigentlich geht

02 **Die TOP 6 Prüfbereiche und typische Findings**
Worauf die Prüfer achten

03 **Das machen unsere Kunden**
Kundenbeispiel JOST-Werke Deutschland GmbH

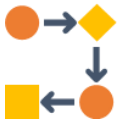
04 **Last-Minute-Tipps, bevor die Prüfer kommen**
Darüber freuen sich die Prüfer

Last-Minute-Tipps, bevor die Prüfer kommen

Identifizieren Sie vergebene kritische Berechtigungen und bereinigen Sie diese vor der Prüfung

Überprüfen Sie die SAP Standarduser in Ihrem System und sichern Sie die User ab

Sperren Sie inaktive User immer zeitnah und zuverlässig



Sorgen Sie für einen Prozess zur zeitnahen Implementierung von Sicherheitspatches

Aktivieren Sie das SAP Security Audit Log und sorgen Sie für eine regelmäßige Auswertung

Wie können Sie jetzt weitermachen?

Lucas Hoppe
Senior SAP Security Consultant
@mindsquare AG
0211 9462 8572 - 22
info@rz10.de

- Expertengespräch
- SAP Security Check
- SAP Security Monitoring

https://rz10.de/kostenloses-expertengespraech/