

SAP-Sicherheitsprüfung

In SAP-Systemen wird meist ein Großteil der Unternehmenswerte verwaltet. Hierbei geht es um Finanzdaten, Human Capital und/oder Know-how. Eine umfassende Systemprüfung deckt etwaige Schwächen im Schutz dieser Daten auf und ermöglicht Ihnen, die System-sicherheit effizient zu erhöhen.

Der SAP Security Check von Xiting ist ein Service, der es Ihnen ermöglicht, potenzielle Schwachstellen zu identifizieren und Ihre SAP-Systeme auf die Einhaltung von Best-Practice-Sicherheitsrichtlinien zu prüfen. Die Analyse erfolgt unter der Nutzung der von Xiting entwickelten Sicherheitslösung "Xiting Authorizations Management Suite (XAMS)" und deckt eine Vielzahl von sicherheitsrelevanten Bereichen Ihres SAP-Systems ab, darunter:

- Dokumente (Vergleich von Soll- und Istzustand der Einsatzkonzepte)
- Prüfung der Übereinstimmung mit einem bestehenden SAP-Sicherheitskonzept
- Rollen (technische und fachliche Compliance gemäß DSAG-Vorgaben)
- Berechtigungen (Administration von Jobs, Benutzern, Transporten, System)
- Benutzer (Profilvergabe, Benutzertypen, kritische Berechtigungen, Login-Aktivitäten)

XAMS WEBINARE

Get clean – stay clean!

Erfahren Sie von einem unserer SAP-Sicherheitsexperten mehr über die XAMS sowie zu Best Practices in unseren kostenlosen Webinaren.



UNSERE DIENSTLEISTUNG – SCHRITT FÜR SCHRITT

1

Prüfung des SAP-Systems

- Scannen des SAP-Systems mit Hilfe der XAMS
- Prüfung von Berechtigungen auf Qualität und IKS-Konformität
- Prüfung der technischen Absicherung des Produktivsystems
- Verifizierung der Aktualität und Korrektheit des SAP-Berechtigungskonzepts

2

Auswertungen

- Detaillierte Auswertungen und Dokumentation der Analysen
- Management-Summary zur Gesamteinschätzung der Analyseergebnisse
- Aufzeigen der Schwachstellen und Risiken
- Maßnahmenkatalog mit Empfehlungen zur Behebung der Schwachstellen

3

Durchführung

- Vereinbarung über die zu prüfenden Systeme, Module, Teilbereiche, Prozesse und Dokumente
- Implementierung der XAMS per Transport
- Planung von Vor-Ort-Terminen und die Berichterstellung
- Durchführung der Analysen vor Ort oder remote mit Hilfe der XAMS
- Erstellung und Abstimmung des Berichtes
- Abschlusspräsentation
- Optional: Darstellung wie mit Hilfe der XAMS die gefundenen Schwachstellen effektiv und schnell bereinigt werden können

Auf einen Blick:

- Analyse ihrer Berechtigungsinfrastruktur und Konzepte als Vorbereitung für externe und interne Audits
- Übersicht und Risikobewertung von potentiellen Schwachstellen
- Empfehlungen zu weiterführenden Maßnahmen im Zuge der Schwachstellenbereinigung