KPMG

# SAP Security & Compliance

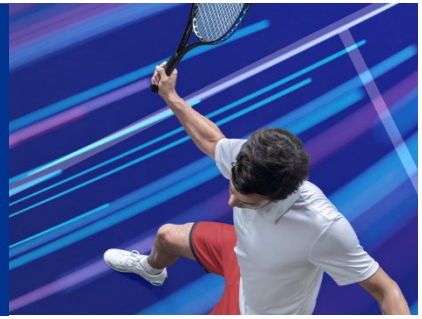
Wir meinen, bei SAP-Sicherheit stehen Ihre Chancen im Mittelpunkt – und nicht die Risiken.

kpmg.at

# Worum geht es?


**01** Wie wichtig es ist, Ihre SAP-Landschaft zu schützen

**02** S/4HANA-Transformation aus Sicht der Cybersicherheit



**03** Schlüsselfragen zur Bestimmung Ihrer Sicherheitslage

**04** Einblicke in die SAP-Sicherheitsreise

**05** Wie KPMG helfen kann

**06** Fallstudien, die unsere Expertise veranschaulichen

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# 01

# Wie wichtig es ist, Ihre SAP-Landschaft zu schützen

# Warum ist es wichtig, Ihre SAP-Systeme zu schützen?

**Sichern Sie Ihre SAP-Landschaft vor Cyberangriffen. Die Bedrohung durch interne oder externe Angriffe ist eines der größten Risiken, mit denen Unternehmen heute konfrontiert sind. Die Anzahl und Raffinesse der Bedrohungen haben exponentiell zugenommen und führen zu einer Welle von Sicherheitsvorfällen, die Reputationsschäden durch Datenschutzverletzungen, hohe finanzielle Verluste oder Nichtverfügbarkeit von Systemen beinhalten.**

## SAP-Sicherheit neu definiert

Erhöhte Sicherheit und Governance rund um die buchhaltungsführenden Systeme sind angesichts dieser ausgeklügelten Angriffe von entscheidender Bedeutung. Bis vor kurzem wurde die SAP-Landschaft eines Unternehmens nur als internes Finanzsystem betrachtet. Dieser enge Blickwinkel führte zu der Annahme, dass Sicherheit lediglich eine Frage der Kontrolle des Benutzerzugriffs, der Beseitigung von Konflikten bei der Funktionstrennung und der Implementierung einer starken Change Policy sei. Diese Ansichten beginnen sich aufgrund der jüngsten Ereignisse langsam zu ändern.

## SAP als Ziel

SAP-Systeme werden aufgrund des hohen Werts der Daten, die im System gespeichert werden, zunehmend zum Ziel von Cyberangriffen von innen und außen. Angreifer:innen haben es auf die geschäftskritischen SAP-Systeme und Informationen abgesehen, indem sie interne Kontrollsysteme umgehen oder (bekannte) Sicherheitslücken in den technischen Infrastrukturschichten von SAP ausnutzen.

## Schutz der SAP-Landschaft

Aufgrund der zunehmenden Bedrohung durch Cyberangriffe reichen die bestehenden Sicherheits- und Governance-Strategien schlicht nicht mehr aus, um die vernetzte SAP-Landschaft zu schützen. Unternehmen müssen ihren Ansatz zur Sicherung der SAP-Landschaft ändern und eine ganzheitliche Sicherheits- und Governance-Strategie verfolgen, die den gesamten SAP-Technologie-Stack schützt. Dies erfordert die Bereitschaft, SAP-Cyberbedrohungen proaktiv zu identifizieren und eine nachhaltige Strategie zu implementieren, um dynamisch Risiken zu begegnen.

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation u
Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehal

## SAP-Security in Zahlen

**92 %**
der Forbes-Global-2000-Unternehmen betreiben SAP

**64 %**
der ERP-Systeme (einschließlich SAP) verzeichneten in den letzten 24 Monaten Sicherheitsverstöße

**50.000 € pro Stunde**
durchschnittliche Kosten bei Nichtverfügbarkeit des ERP-Systems

**768**
Security Notes (Patches) durchschnittlich pro Jahr

*Ponemon Institute: Bericht über die Kosten einer Datenschutzverletzung im Jahr 2024*

# 02

# S/4HANA-Transformation aus Sicht der Cybersicherheit

# Überlegungen zur SAP-Sicherheit angesichts zunehmender Bedrohungen

Zahlreiche Unternehmen starten derzeit Transformationsprojekte zur Migration auf SAP S/4HANA. Aus technischer Sicht wirft dies eine Vielzahl von Fragen auf, angefangen beim Betriebsmodell (Cloud vs. On-Prem) bis hin zur Integration in die bestehende Systemlandschaft. Die Implementierung führt zu einer veränderten IT-Architektur, oft verbunden mit vielen neuen Komponenten und Schnittstellen.

Gleichzeitig steigt die Bedrohung durch Cyberangriffe. Neue Prozesse und ein Mehr an Schnittstellen, die mit dem Einsatz von S/4HANA einhergehen, bedeuten gleichzeitig mehr Angriffsmöglichkeiten auf SAP-Systeme. In diesem Zusammenhang stoßen Angreifer:innen auf eine für sie günstige Situation. Unsere Beobachtung ist, dass die bestehenden SAP-Systeme oft unsicher betrieben werden. Die Gründe dafür sind einfach: SAP R/3 und ECC wurden unsicher ausgeliefert. Kunden müssen sich selbst um die Sicherheit kümmern. Gleichzeitig ist der Betrieb eines SAP-Systems sehr komplex. Das beste Beispiel dafür ist der SAP-Patch-Prozess mit SAP Security Notes. Darüber hinaus wurden in der Vergangenheit viele Eigenentwicklungen erstellt, die gängige Security Best Practices für die ABAP-Entwicklung nicht berücksichtigen.

## Erhöhter Handlungsbedarf

Viele Unternehmen haben in den letzten 20 Jahren relativ unsicher operiert, aber von einem „Business as usual“ bei der aktuellen Bedrohungslage ist stark abzuraten. Angesichts höherer Risiken sollte die S/4HANA-Transformation vor allem als Chance gesehen werden, das Sicherheitsniveau an die aktuellen Herausforderungen anzupassen. Auch wenn die Sicherheit von S/4HANA besser als die der älteren Versionen ist. (Security-by-Default)

Über den Standard hinaus gibt es weitere Möglichkeiten und Schritte, um die Systemsicherheit langfristig zu erhöhen und fit für die Zukunft zu bleiben. Es ist von essenzieller Bedeutung, Security von Anfang an ganzheitlich und in allen Phasen der Entwicklung von S/4HANA mitzubetrachten. Da das Sicherheitsdesign von SAP nur minimal greift, müssen Kunden überprüfen, ob die Standardeinstellungen für ihre Bedürfnisse angemessen sind oder ob sich strengere Maßnahmen empfehlen.

Sicherheit ist ein wesentlicher Aspekt der S/4HANA-Transformation, da IT-Systeme für Kerngeschäftsprozesse von entscheidender Bedeutung sind.

Wenn Schwachstellen und Angriffsvektoren, welche den Zugriff auf wichtige Bereiche mit sensiblen Daten erlauben, unzureichend gesichert sind, besteht die Gefahr, dass ein Angriff das Worst-Case-Szenario wie einen Produktionsstopp auslösen könnte.

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# Ausgangspunkt für Entscheidungsträger:innen. Den Handlungsbedarf verstehen

Einer der Hauptgründe bei der Herausforderung, Security-Kompetenzen intern zu aufzubauen, ist der Mangel an qualifizierten Fachkräften. Darüber hinaus ist die Bedrohungslandschaft breit gefächert und äußerst vielfältig, was die Einführung eines robusten Sicherheitskonzepts erschwert. Gleichzeitig nimmt die Professionalität der Cyberkriminellen zu (z. B. Ransomware-as-a-Service), was das Risiko von Angriffen auf Unternehmen erhöht.

Unser erster Schritt ist ein Security Assessment, um die Sicherheitslage Ihrer S/4HANA-Systemumgebung zu bewerten und empfohlene Sicherheitsanforderungen zu ermitteln. Nach Analyse der grundlegenden Architektur führen wir eine Schnittstellenanalyse durch, um mögliche Angriffspfade zu identifizieren und die damit verbundenen Risiken abzuschätzen. Alle Portale mit Internetverbindungen oder Schnittstellen zu externen Partnern sollten als potenzielle Gateways betrachtet werden. Weitere Angriffspfade können Schwachstellen in der Datenbank oder im Betriebssystem sein.

Ein effektives Patch-Management und automatisiertes Schwachstellen-Scanning sind unerlässlich, um die Systemintegrität zu wahren. Diese Praktiken gewährleisten, dass Sicherheitsupdates systematisch angewendet und Schwachstellen proaktiv identifiziert und behoben werden. Die Verwaltung von Patches erfordert einen systematischen Ansatz zur monatlichen Bewertung und Priorisierung relevanter Sicherheitshinweise. Eine sorgfältige Planung ist notwendig, um mögliche Systemausfälle während des Patchings zu berücksichtigen. Penetration Tests vor oder nach der Umstellung auf neue Systeme helfen, Schwachstellen zu identifizieren. Sicherheitsanforderungen sollten von Anfang an in das Projekt integriert und ein frühzeitiges Security Assessment durchgeführt werden, um spätere Mehraufwände zu vermeiden.

## Cybersecurity als ganzheitliche und kontinuierliche Aufgabe

Die S/4HANA-Umstellung erfordert eine starke konzeptionelle Grundlage für die Sicherheit. Unternehmen müssen ihre Maßnahmen entsprechend ihrem Risikoprofil gestalten. Dabei handelt es sich nicht um einen einmaligen Vorgang. Security ist eine kontinuierliche Aufgabe, die als fester Prozess im Unternehmen etabliert werden muss. Um dies zu erreichen, müssen angemessene Ressourcen sowie Verantwortlichkeiten zugewiesen und Fähigkeiten aufgebaut werden.

Zu diesem Zweck müssen alle ergriffenen Maßnahmen während der Transformation dokumentiert werden. Die angemessene Verschriftlichung ist nicht nur eine wichtige Voraussetzung für Tests, sondern auch für Compliance und Audit. Insbesondere die Überwachung von Benutzeraktivitäten auf sicherheitskritische Ereignisse wird immer wichtiger.

So wird nach und nach eine verlässliche Basis geschaffen, die einen langfristig sicheren Betrieb und eine sichere IT-Infrastruktur gewährleistet.

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhä
Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# Potenzielle Risiken bei der Umstellung auf S/4 HANA

S/4HANA liefert neue funktionale und technische Innovationen, um die digitale Transformation voranzutreiben. Durch bedeutende Veränderungen entstehen jedoch neue Risiken, wenn der Sicherheit nicht die Aufmerksamkeit geschenkt wird, die sie erfordert. Zu diesen Herausforderungen gehören:

## Neue Funktionalitäten

Neue oder obligatorische Funktionen führen dazu, dass ältere Applikationskontrollen unwirksam sind, während neue Kontrollen nicht identifiziert, konfiguriert oder implementiert wurden.

## Datenmigration

Mit neuen Tabellen und Datenbankstrukturen müssen migrierte Daten ausreichend validiert und getestet werden. Mit SAP HANA entstehen zudem gänzlich neue Sicherheitsanforderungen, die angepasste Konzepte und Lösungen erfordern.

## Zugriff in Echtzeit

Der Echtzeitzugriff auf Daten birgt das Risiko für unbefugten Zugriff auf vertrauliche Informationen. Dieser Zugriff ist über mehrere Schichten möglich, z. B. über Berichte und Analysen auf der SAP-HANA-Datenbankebene oder erweitertes Reporting auf der S/4HANA-Anwendungsebene – und das von einer wachsenden Anzahl von Anwender:innen im gesamten Unternehmen.

## Härtung

Mehrere neue Schnittstellen können unzureichend gehärtet sein. Zwischen den verschiedenen SAP-Schnittstellen gibt es mehrere Berührungspunkte mit der Datenbank sowohl über Public- als auch über Private-Cloud-Umgebungen. All diese neuen Gefahren erfordern starke Schnittstellen-Kontrollen und Überwachung.

## Zugriff durch Dritte

Sicherheitslösungen von Drittanbietern erfordern eine neue Systemarchitektur. Diese ist komplexer, mit mehr Public Cloud Integrationen, die sich mit externen Lösungen vernetzen. Unternehmen müssen überlegen, welche Sicherheits- und Kontrollmechanismen von Drittanbietern genutzt werden sollen.

## Verantwortung

In der sich entwickelnden Landschaft von SAP und seinen Hyperscalern/Anbietern, einschließlich SAP RISE, kann die Abgrenzung der Verantwortlichkeiten oft verschwimmen. Die Festlegung klarer Verantwortungsbereiche ist unerlässlich, um sicherzustellen, dass jede Partei ihre Aufgaben und Pflichten versteht, um Risiken zu verringern und die Sicherheit zu stärken.

# 03

# Schlüsselfragen zur Bestimmung Ihrer Sicherheitslage

# Die richtigen Fragen stellen

Das Verständnis des Reifegrads Ihrer SAP-Landschaft in Bezug auf die Sicherheit ist entscheidend für Unternehmen, die ihre Abwehr gegen sich entwickelnde Cyberbedrohungen stärken wollen. Durch die Bewertung von Aspekten wie Zugriffskontrollen, Schwachstellenmanagement und Incident Response können Schwachstellen lokalisiert und Verbesserungsmaßnahmen priorisiert werden. Dieses Wissen ermöglicht die Optimierung der Ressourcenallokation und konzentriert die Bemühungen dort, wo sie die größte Wirkung erzielen können. Darüber hinaus fördert das Verständnis des Reifegrads der SAP-Sicherheit eine Kultur der kontinuierlichen Verbesserung, die es unseren Kunden ermöglicht, ihr Vorgehen im Einklang mit neuen Bedrohungen und regulatorischen Anforderungen weiterzuentwickeln.

Die richtigen Fragen zu stellen, ist in diesem Prozess von entscheidender Bedeutung und hilft Unternehmen, sich mit Schlüsselbereichen zu befassen und wichtige Schwachstellen aufzudecken. Fragen in Bezug auf Zugriffskontrollen können Diskrepanzen in den Benutzerberechtigungen aufdecken, während Fragen zum Schwachstellenmanagement Aufschluss über Patching-Praktiken und Strategien zur Risikominderung geben. Überwachungsfunktionen können durch gezielte Nachforschungen im Bereich Echtzeit- und Anomalieerkennung eingeführt und effektiv eingesetzt werden. Außerdem können die richtigen Fragen dazu beitragen, dass die Compliance gewährleistet ist, indem gesetzliche Anforderungen sowie interne und externe Audit-Vorgaben betrachtet werden.

## Was sind Schlüsselfragen, die Sie sich stellen müssen?

**SAP-Sicherheitsstrategie**
Haben Sie eine SAP-Sicherheitsstrategie eingeführt, die alle relevanten Aspekte der SAP-Security abdeckt?

**Verantwortlichkeiten**
Sind die Verantwortlichkeiten für die verschiedenen Aspekte der SAP-Security klar definiert? Wird die Funktions-trennung eingehalten?

**Sicherheitsstandards**
Welche Sicherheitsstandards verwenden Sie, um SAP-Systeme zu härten? Wie aktuell ist Ihr Prüfregelwerk?

**SAP-Sicherheitstools**
Welche SAP-Sicherheitstools verwenden Sie, um die Transparenz zu erhöhen und manuelle Aufwände zu reduzieren?

**Rollen und Berechtigungen**
Gibt es ein Konzept für die Rollen und Berechtigungen von Benutzer:innen/Admins ? Welche User:innen haben kritische Rechte?

**SAP-Landschaft**
Wie sieht das Netzwerk aus, sind Schnittstellen, die Betriebssysteme und Datenbanken, die das SAP-System hosten, gesichert?

**Penetration Test**
Wann wurde zuletzt ein realer Angriff auf Ihre Systeme simuliert, um Schwachstellen präventiv aufzudecken?

**Audit-Konformität**
Wie revisionssicher und dokumentiert sind Ihre Access-Governance-Prozesse? Weicht das Soll-Konzept vom Ist-Zustand ab?

**Überwachung**
Wie überwachen Sie verdächtige Aktivitäten? Welche Anwendungsfälle für Monitoring werden umgesetzt?

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# 04

# Einblicke in die SAP-Sicherheitsreise

# Sicherheit ist nicht nur ein Ziel, sondern eine Reise

Sicherheit ist ein kontinuierlicher Prozess des Lernens, Anwendens und Verbesserns. Es liegt in unserer Verantwortung, SAP-Systeme vor böswilligen Angriffen und Schwachstellen zu schützen. Aber Sicherheit kann herausfordernd und komplex sein, insbesondere in einem schnelllebigen und dynamischen Umfeld.

- Wie können Sie mit den neuesten Bedrohungen, Compliance Anforderungen und Best Practices Schritt halten?
- Wie können Sie Sicherheit in Ihr Tagesgeschäft integrieren, ohne die Produktivität und Qualität zu beeinträchtigen?
- Wie können Sie Ihre Sicherheitsfortschritte und -erfolge effizient messen und nachweisen?

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# Die Vorteile optimierter SAP-Security

- Bewertung der Sicherheitslage von SAP-Systemen. Identifikation von Sicherheitslücken und Schwachstellen.
- Verhindern und Erkennen von Cyberbedrohungen und -vorfällen in SAP mit fortschrittlichen Analysen und Automatisierung.
- Reaktion auf Cyberangriffe und Wiederherstellung des Normalzustands mit Funktionen für Incident-Management und -Behebung.
- Einhaltung von regulatorischen Vorgaben, branchenspezifischen Standards und Best Practices.
- Erhöhtes Vertrauen in Ihr Unternehmen, verbesserte Markenreputation und Wettbewerbsfähigkeit sowie Verhinderung von Geldstrafen.
- Voraussetzung für die SAP-Transformation, Migration und die allgemeine digitale Transformation.
- Beschleunigung der digitalen Transformation und Cloud-Einführung.

Durch die verbesserte Sicherheit in Ihrer SAP-Landschaft können Sie kritische Ressourcen schützen, sich vor neuen Bedrohungen sichern, die Einhaltung gesetzlicher Vorschriften gewährleisten und eine Kultur des Vertrauens und der Zuverlässigkeit fördern. Nutzen Sie unsere Services, um Ihre digitalen Assets zu schützen.

Die Vorteile eines sicheren SAP-Ökosystems gehen über den reinen Schutz von Daten hinaus. Sie tragen zur allgemeinen Resilienz, Compliance und zum Erfolg eines Unternehmens in einer zunehmend vernetzten und datengetriebenen Welt bei.

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KP
Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. A

# 05

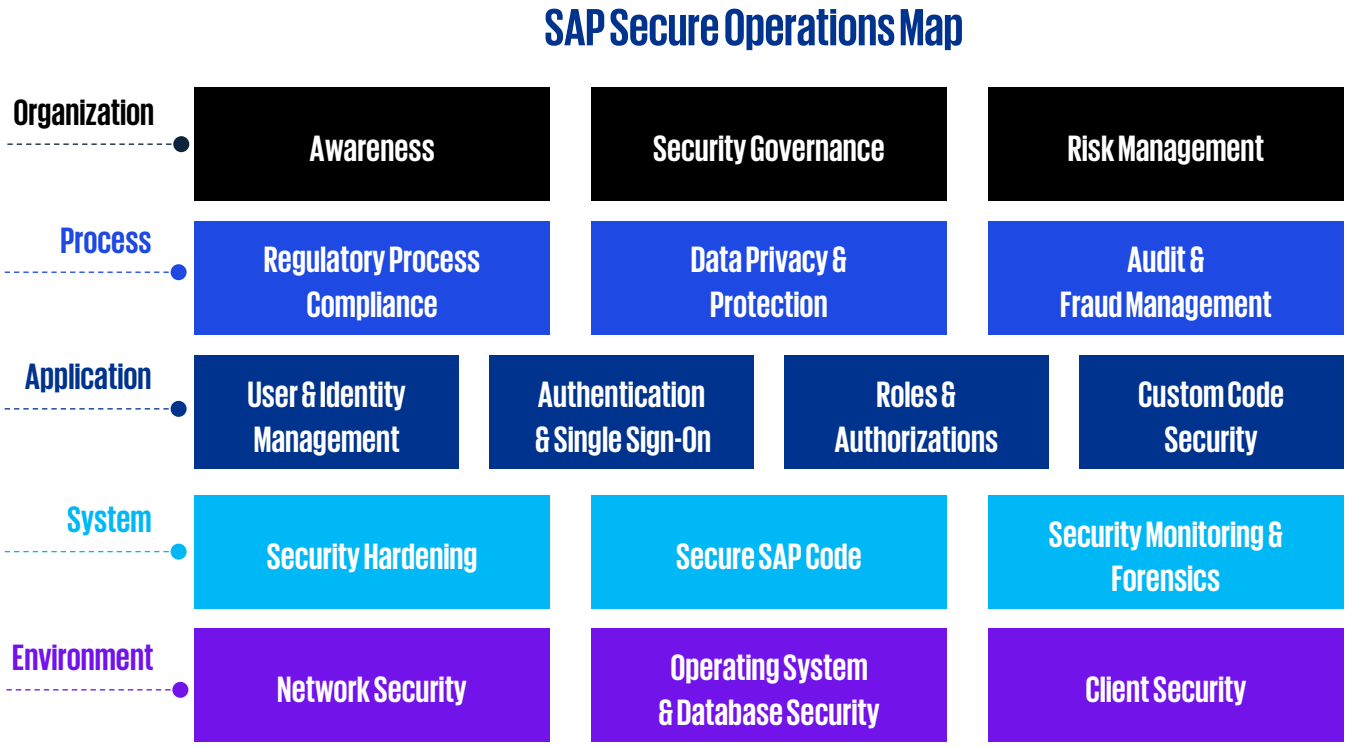
# Wie KPMG helfen kann

# KPMG Trusted SAP Framework – Ein umfassender Ansatz in einem komplexen Umfeld

SAP organisiert den Bereich Sicherheit strategisch im Rahmen ihrer „SAP Secure Operations Map“, welche 16 Schlüsselthemen umfasst, die wiederum auf fünf Ebenen verteilt sind.

Bei KPMG gehen wir über die reine Einhaltung der SAP-Empfehlungen hinaus, indem wir sie durch bewährte Praktiken ergänzen. Unser Ansatz für SAP-Sicherheitsdienstleistungen und -software umfasst eine tiefgehende Analyse aller betrieblichen Aspekte, die durch Kombination aus Best-Practice-Ansätzen, datengetriebener Tool-Unterstützung und unserer Erfahrung in der Absicherung von komplexen und sich verändernden SAP-Landschaften sorgfältig unter die Lupe genommen werden.

Unser ganzheitliches Vorgehen stellt sicher, dass jeder Blickwinkel der Sicherheit innerhalb des SAP-Ökosystems gründlich beleuchtet wird, um unseren Kunden robuste und maßgeschneiderte Sicherheitslösungen mit hoher Zielorientierung anbieten zu können. Wir meinen, bei Cybersecurity stehen Ihre Chancen im Mittelpunkt – und nicht die Risiken.




© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# Unser Ansatz

Wir bei KPMG wissen, wie wichtig es ist, SAP-Umgebungen zu sichern, um die Integrität und Vertraulichkeit von Geschäftsdaten zu schützen. Unser Angebot konzentriert sich darauf, eine breite Palette spezialisierter SAP-Sicherheitsdienstleistungen anzubieten, um Ihr Unternehmen dabei zu unterstützen, Risiken zu minimieren und die Cyberabwehr zu stärken.

## SAP Security Assessments

– Das SAP Security Assessment von KPMG bietet eine tiefgreifende technische und organisatorische Prüfung der SAP-Landschaft. Basierend auf der SAP Secure Operations Map blickt unser Ansatz über die traditionelle Linse der finanziellen und regulatorischen Compliance hinaus und bietet eine ganzheitliche Sicht auf die Sicherheit für das gesamte SAP-Technologiespektrum.

## SAP Security Governance

– Basierend auf Ihrem aktuellen SAP-Sicherheitsreifegrad und der Risikoexposition des Unternehmens kann KPMG bei der Definition effektiver Strategien und Maßnahmenpläne helfen. All dies begleitet von erprobten Verfahren, Vergleichsmetriken und datengetriebenen Automatismen, die die Entscheidungsfindung erleichtern.

## SAP Security Operation Definition

– Definition und Roadmap von Sicherheitsmaßnahmen und -lösungen innerhalb von SAP-Systemen zum Schutz vor Compliance-Verstößen und Bedrohungen. Dazu zählen vor allem: Notfallbenutzerverfahren, Automatisierte Rollenerstellung & Risikoprüfung, Vulnerability- & Patch-Management, Threat Detection & Response, Transport- & Code-Scanning.

## SAP Security Monitoring

– Unser Angebot an SAP Security Monitoring Services umfasst **Threat Intelligence** und **Managed Services**, die speziell auf SAP-Umgebungen zugeschnitten sind. Wir bieten umfassende Lösungen zur proaktiven Identifizierung und Mitigation von Sicherheitsbedrohungen, zur kontinuierlichen Überwachung auf verdächtige Aktivitäten und zum effizienten Management von Sicherheitsvorfällen in SAP-Systemen.

## SAP Security Incident Management

– Und wenn Ihre SAP-Systeme kompromittiert wurden? Bei KPMG verfügen wir über ein engagiertes Incident-Response-Team, welches Sie bei der Eindämmung, Wiederherstellung und Durchführung forensischer Untersuchungen unterstützt.

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# Unsere Teams, an Ihrer Seite

Die Berater:innen von KPMG nutzen ihr Know-how im Bereich SAP-Security, um Unternehmen beim Schutz ihrer SAP-Infrastruktur zu unterstützen. Durch unser umfangreiches globales Netzwerk von Mitgliedsfirmen nutzen wir das kollektive Wissen von Fachexpert:innen, um für Sie einen Ansatz zu entwickeln, der auf die spezifischen SAP-Cyberbedrohungen zugeschnitten wird, mit denen sich Ihr Unternehmen konfrontiert sieht.

- **SAP PartnerEdge**: Durch die Kombination unserer branchenorientierten Herangehensweisen mit der marktführenden Technologie von SAP beschleunigen wir die digitale Transformation und helfen Unternehmen dabei, sich auf die Zukunft vorzubereiten.
- **Global**: Im Netzwerk der Mitgliedsfirmen beschäftigen unsere KPMG-Unternehmen über 155.000 Berater in 155 Ländern. Wir verfügen über umfassende Expertise, wo auch immer Ihr Unternehmen operiert.
- **Akkreditiert:** KPMG wurde 2024 von Forrester als Leader im Bereich Cybersecurity Consulting Services in Europa anerkannt.
- **Engagiert**: Die Beziehungen zu den Kunden unserer Mitgliedsfirmen basieren auf gegenseitigem Vertrauen und langfristigem Engagement für die Bereitstellung effektiver und effizienter Lösungen.

**KPMG. Make the Difference.**

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# 06

# Fallstudien, die unsere Expertise verdeutlichen

# Fallstudie 1

**Umfassende Stärkung der SAP-Sicherheit durch Konfigurationsvalidierung, automatisiertes Monitoring und standardisierte Richtlinien bei einem Chemieunternehmen.**

## Herausforderungen

- Heterogene Landschaft mit unklaren Zuständigkeiten.
- Keine einheitliche Sicht auf die SAP-Sicherheit.
- Herausforderungen in den Bereichen Monitoring, sicherer SAP-Code, Custom Code Security, Dashboard etc.
- Laufende S/4HANA-Transformationsprojekte.
- Laufende globale Sicherheitsinitiative mit Auswirkungen und Anforderungen an den Betrieb der SAP-Landschaft.

## KPMG – Lösung

- Bewertung des aktuellen SAP-Sicherheitsstatus für 24 SAP-Systeme über Workshops und datengetriebene Checks mit 200+ Kontrollen/Baseline gemäß SAP Secure Operations Map.
- Best Practices für Governance: sowohl für klassische/Legacy- als auch für S/4-Systeme.
- Design eines verbesserten SAP Security-Zustands, inkl. Toolauswahl für SAP Vulnerability Management, ABAP Code Security Scan, Security Monitoring und Technical Compliance/Baseline Checks.

## Ergebnis

- Bewertung des Reifegrads der SAP-Sicherheit für On-Prem- und Cloud-Systeme.
- Klare Roadmap zur Verbesserung des SAP-Security-Reifegrads.
- Unterstützung bei der Organisation der SAP-Sicherheit.
- Unterstützung bei der Toolauswahl für verbesserte Prozesse in den Bereichen Security Monitoring, Patch Management, Code Scanning und Härtung von SAP-Systemen.

## Kennzahlen

**> 200**
SAP-spezifische Sicherheitskontrollen

**24**
Analysierte Systeme

**6**
SAP-Produkte im Anwendungsbereich

**11**
Beteiligte KPMG-Expert:innen

## Kontext (Klient)

- Ein Chemieunternehmen mit 48 Produktionsstätten und 63 Service- und Forschungslaboren weltweit, sowie rund 7.000 Mitarbeiter:innen und einem Jahresumsatz von 3,0 Mrd. EUR.
- Der Kunde nutzt über mehrere Tochtergesellschaften hinweg eine vielfältige Landschaft an SAP-Produkten, für die ein einheitlicher Sicherheitsstandard erreicht werden soll. Dazu gehören neben typischen ERP-Systemen auch Cloud-Anwendungen.

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# Fallstudie 2

**Konzeption und Umsetzung von IT-Sicherheitsmaßnahmen für das zentrale SAP-basierte HR-System eines staatlichen IT-Dienstleisters.**

## Herausforderungen

- Umfangreiche regulatorische Anforderungen auf Landes- und Bundesebene.
- Extrem hohe Sicherheitsanforderungen und -bedenken bestimmter Behörden.
- Große Vielfalt an Verwaltungsstellen mit unterschiedlichen Anforderungen und Lösungszugängen.
- Komplexe SAP-Landschaft mit mehreren Lösungen von Drittanbietern.

## KPMG - Lösung

- Integration von SAP-spezifischen Sicherheitsrichtlinien in allgemeine Sicherheitsrichtlinien auf Basis des BSI-IT-Grundschutzes.
- Unterstützung des SAP-Basisteams bei der Implementierung von Security Best Practices.
- Entwicklung eines Konzepts für die sichere Nutzung von SAP-Cloud-Produkten, um mehr Lösungsansätze zu bieten.
- Unterstützung bei der Auswahl einer SAP-Monitoring-Lösung.

## Ergebnis

- Richtliniensetzung für Kryptographie, Baseline-Härtung, Autorisierung und Überwachung mit SAP-spezifischen Komponenten.
- Security Best Practices, die im SAP-HCM-System implementiert sind.
- Ausgearbeitete Konzepte zur Überwachung von SAP- und Nicht-SAP-Systemen.
- Workshops und effektive Kommunikation als Sicherheits- und Qualitätsmarker der umgesetzten Lösungen.

## Kennzahlen

**460.000**
vom SAP-HCM-System verwaltete Personenanzahl

**4**
Jahre Projektlaufzeit

**9**
SAP-Systeme im Anwendungsbereich

## Kontext (Klient)

- Zentraler IT-Provider für ein deutsches Bundesland. Sie realisieren und betreiben IT-Projekte für die Landesregierung und Behörden.
- Das Projekt zielt darauf ab, HR-Prozesse für die meisten Ministerien und Behörden des Landes zu standardisieren und zu bündeln, um eine einzige HR-Lösung zu schaffen.

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

# Kontakte

**Christopher Kobald**
Senior Manager – SAP Security & Compliance
+43 664 889 316 48
ckobald@kpmg.at

**Thomas Hohenauer**
Partner – SAP Advisory Lead
+43 664 132 07 57
thohenauer@kpmg.at

**Thomas Grasser**
Director – SAP Data & Analytics
+43 664 884 477 43
tgrasser@kpmg.at

Einige oder alle der beschriebenen Leistungen sind für KPMG Audit-Kunden, deren Tochterfirmen oder verbundene Unternehmen möglicherweise nicht zulässig.

**kpmg.at**

Die hierin enthaltenen Informationen sind allgemeiner Natur und sollen nicht auf die Umstände einer bestimmten Person oder Organisation eingehen. Obwohl wir uns bemühen, genaue und zeitnahe Informationen zur Verfügung zu stellen, kann nicht garantiert werden, dass diese Informationen zum Zeitpunkt ihres Erhalts korrekt sind oder auch in Zukunft korrekt sein werden. Niemand sollte auf der Grundlage solcher Informationen handeln, ohne nach einer gründlichen Prüfung der jeweiligen Situation angemessen professionell beraten zu werden.

© 2025 KPMG Advisory GmbH, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.

Der Name und das Logo von KPMG sind Marken, die unter Lizenz von den unabhängigen Mitgliedsfirmen der globalen KPMG-Organisation verwendet werden.