SAP Security Group Deutschland

Xiting Kunden-Event
mit Partnern

9./10.
MAI
2023

Entwicklung einer SAP Security Strategie

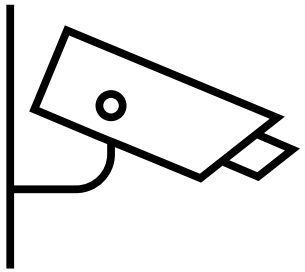
Andre Tenbuß

Agenda

1. SAP Security-Management
2. SAP Security-Strategie

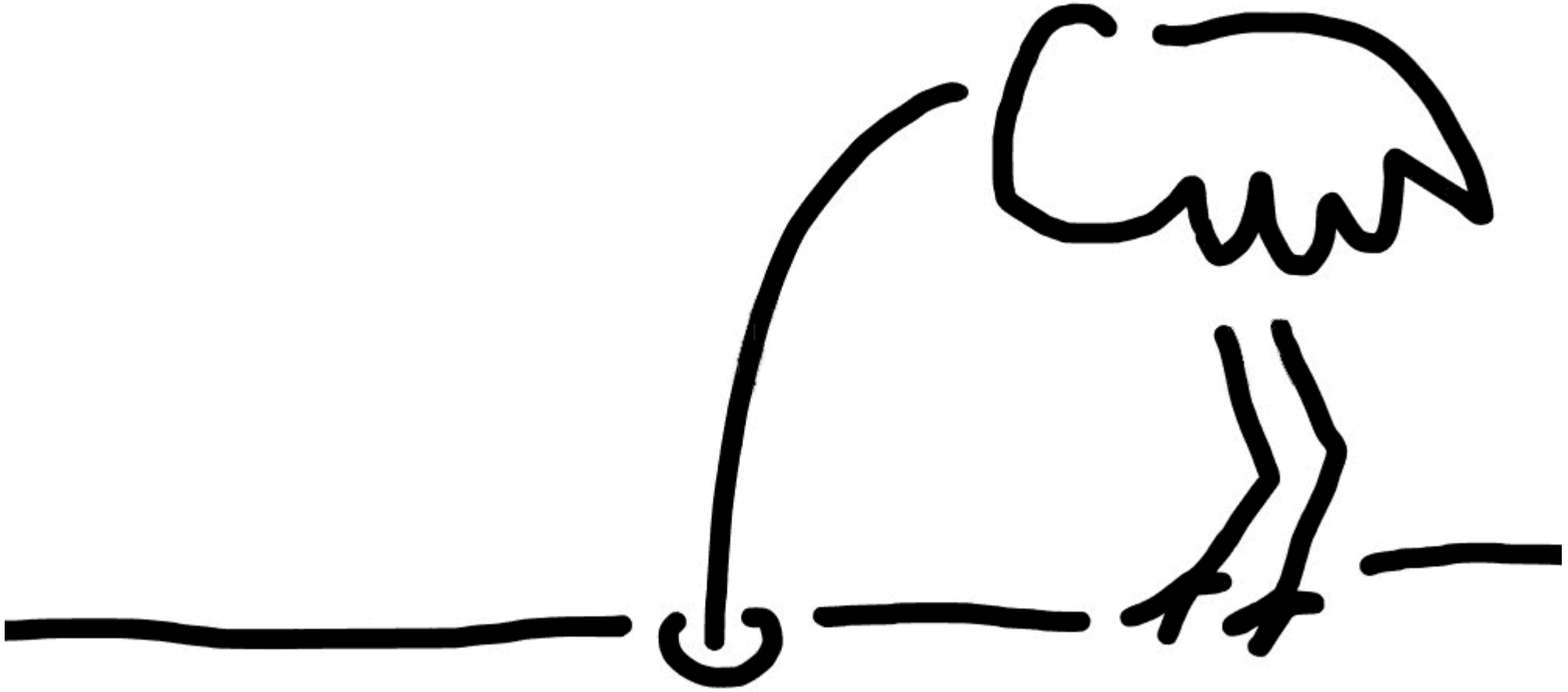
Kapitel 1

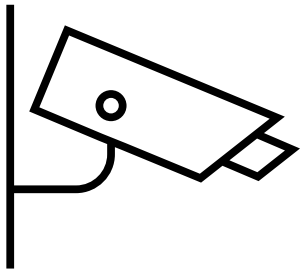
SAP Security Management



„Wie viele Schrauben verkaufe ich mehr,
wenn ich in IT-Sicherheit investiere?“

Security by denial





„Wieviel IT-Sicherheit brauche ich, um morgen noch Schrauben zu verkaufen?“

Herausforderungen

- **Know-how**
  - Zeitaufwändige Erstellung von revisionssicheren SAP-Sicherheitskonzepten und Erfordernis von Know-how
- **Ressourcen**
  - Sicherstellung der Gültigkeit und Aktualität von Sicherheitskonzepten, da die Konfiguration von SAP-Systemen an sich ständig ändernde Bedingungen angepasst werden muss
  - Die Überprüfung der Einhaltung von Sicherheitsanforderungen ist aufgrund komplexer und vernetzter Systemlandschaften zeitaufwändig und schwierig
- **Neue Technologien**
  - Häufig langwierige Projekte
- **Vorausschauendes Handeln**
  - Lücken und Fehler in den Sicherheitsanforderungen können zu Schwachstellen führen, die durch Cyber-Kriminalität ausgenutzt werden können
- **Rechtliche Anforderungen**
  - Berücksichtigung von Compliance-Anforderungen und regulatorischen Standards (DSAG Prüfleitfaden, SAP Security Baseline, DSGVO)
  - Etablierung eines internen Kontrollsystems (IKS) und ein zentrales Monitoring

Management von Cyber-Risiken (BSI)

Management

IT-Sicherheit muss von der Geschäftsführung initiiert, gesteuert und kontrolliert werden. Verständnis als strategisches Unternehmensrisiko.

Auswirkungen

Geschäftsführung muss rechtliche Auswirkungen von IT-Risiken verstehen.

Netzwerk

Geschäftsführung sollte Expertise und Austausch ermöglichen und fordern.

Rahmenbedingungen

Sicherstellung einer angemessenen Personal- und Budgetausstattung. Rahmen schaffen, um Erwartungen erfüllen zu können.

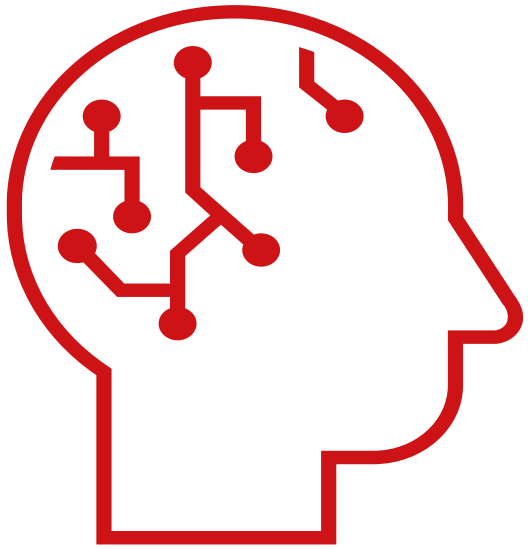
Risikomanagement

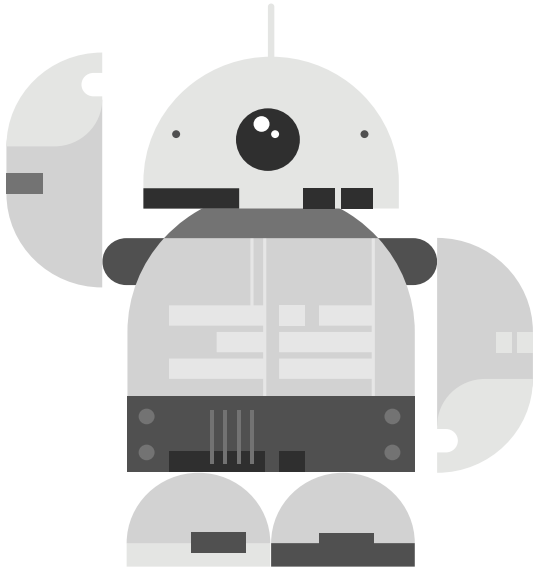
Identifizierung und Bewertung von Risiken durch Zusammenarbeit zwischen Geschäftsführung und IT-Experten.

Zusammenarbeit

Unternehmensinternen und –externen Austausch mit anderen Akteuren suchen, um Best-Practices zu fördern.

Schlüsselfaktoren für IT-Sicherheit





Qualifizierte Teams

Zusammenstellung von Expertengruppen und Entlastung von allen Tätigkeiten, die sich automatisieren lassen.

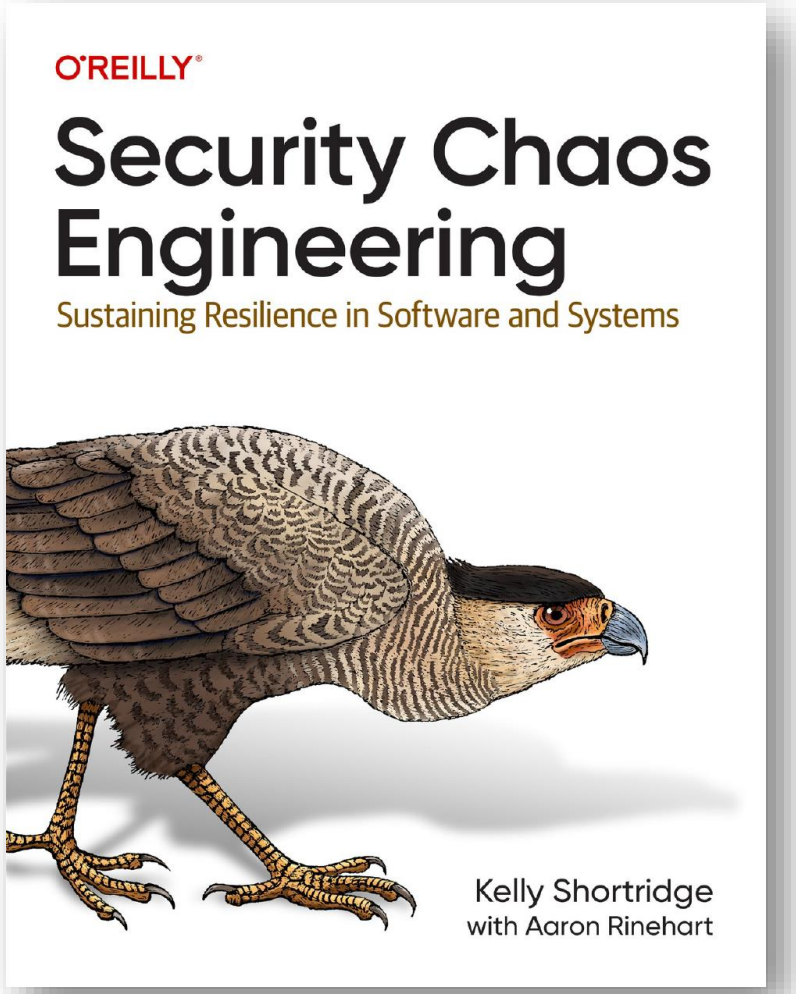
Passende Werkzeuge

Sicherstellung einer angemessenen Personal- und Budget-Ausstattung. Rahmen schaffen, um Erwartungen erfüllen zu können.

Buchempfehlung: Security Chaos Engineering

- Security Chaos Engineering:
  - Gezielte Simulation von Störungen und Angriffen
  - Identifizierung von Schwachstellen
  - Hilfestellung bei der Entwicklung und Umsetzung einer Security Strategie

- Beispiel-These:
  - “Fail-safe” vs. “Safe-to-fail”



Link zum Buch

Kapitel 2

SAP Security-Strategie

Modell der vier Kompetenzstufen

Unbewusste Inkompetenz

Ich denke, dass ich mich ziemlich gut anstelle und verhindere so Verbesserungen

Bewusste Inkompetenz

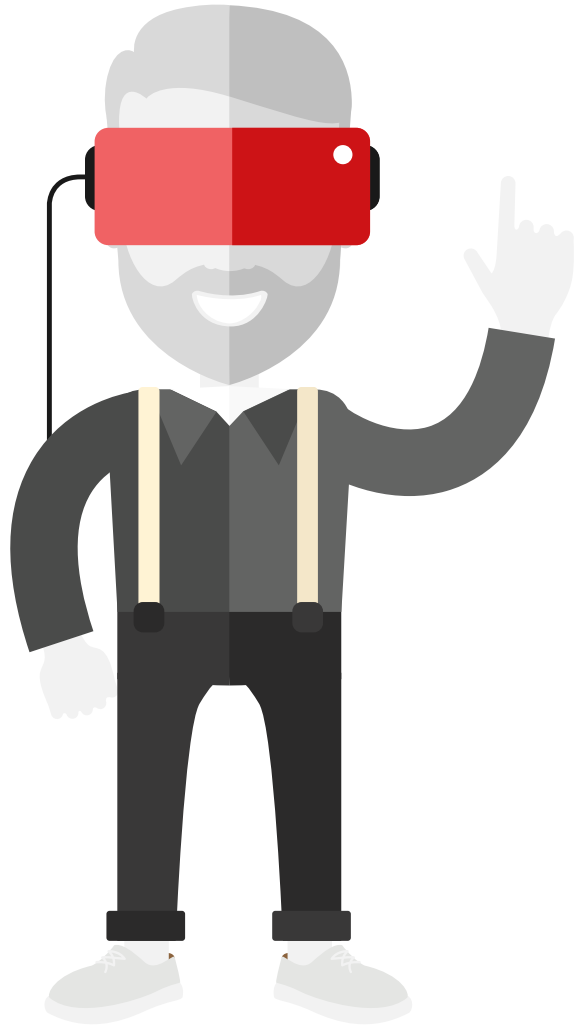
Ich erkenne, wo ich wirklich stehe und sehe ein, dass ich mehr tun muss

Bewusste Kompetenz

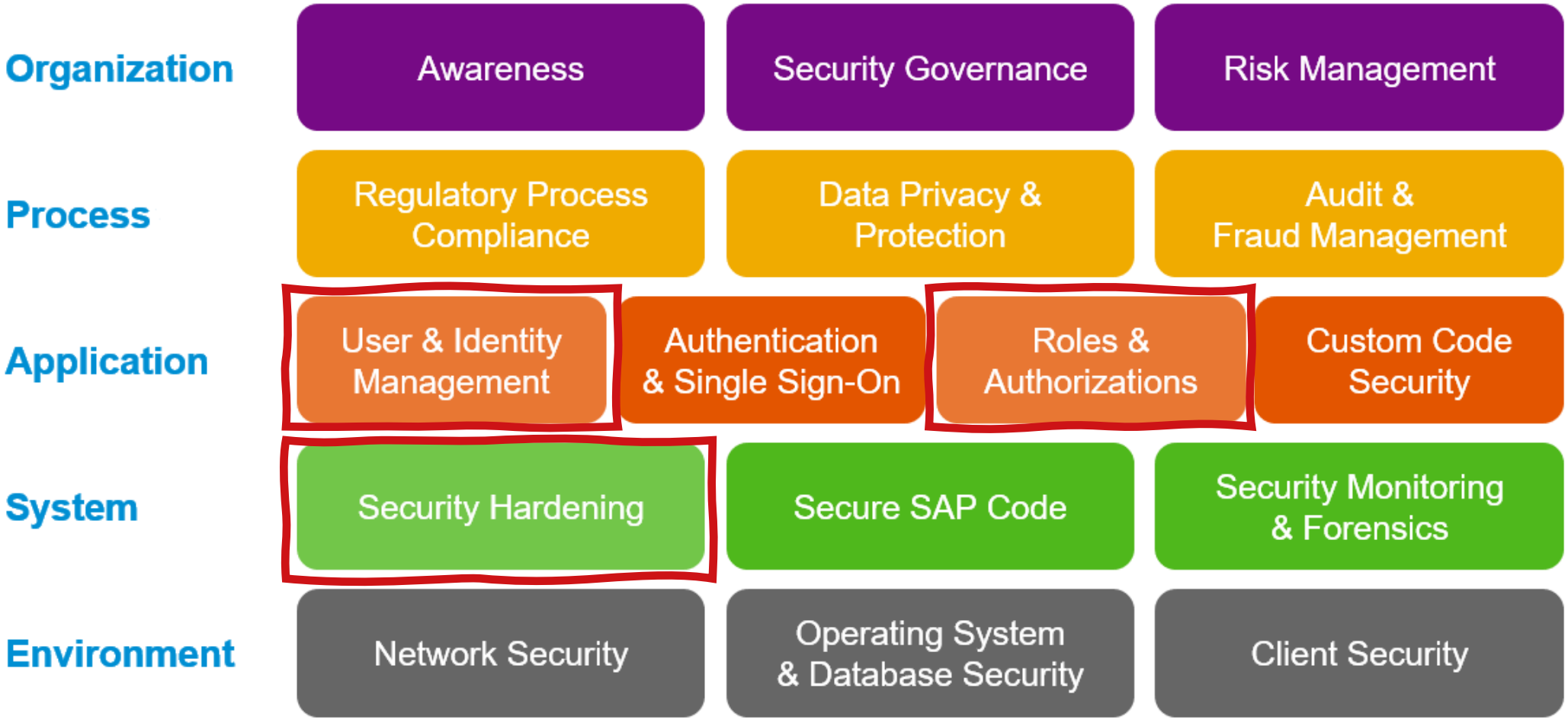
Ich Lerne, werde Schritt für Schritt besser in dem, was ich mache

Unbewusste Kompetenz

Ich habe gelernt und Systeme bzw. Prozesse geschaffen



SAP Security Baseline Template



Quelle: Security Baseline Template 2.4.1, Note 2253549

MITRE ATTACK Framework

- Taktiken
  - Erkundung (Reconnaissance)
  - Erschließung von Ressourcen (Ressource Development)
  - Erster Zugriff (Initial Access)
  - Ausführung (Execution)
  - Persistenz (Persistence)
  - Erweiterung von Berechtigungen (Privilege Escalation)
  - Umgehung der Verteidigungsmaßnahmen (Defense Evasion)
  - Zugriff auf Anmeldeinformationen (Credential Access)
  - Analyse / Entdeckung (Discovery)
  - Zugriffe auf weitere Systeme (Lateral Movement)
  - Sammlung (Collection)
  - Übernahme der Kontrolle (Command and Control)
  - Export / Diebstahl von Daten (Exfiltration)
  - Manipulation / Zerstörung von Systemen und Daten (Impact)
- Techniken
  - Demo

MITRE ATTACK Framework – Taktiken & Techniken

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Offene Services	Persona anlegen	Gültige Accounts	APIs/RFCs	Anlage weiterer Accounts	Jobsteps in Hintergrund-Jobs	Abschaltung Logging
Webseiten (z.B. Jobbörse)	Domäne anlegen	Phishing	Scripting	Einplanung Hintergrund-Jobs	Nutzung gültiger Accounts	Nutzung von blinden Flecken

MITRE ATTACK Framework – Taktiken & Techniken

- **Defense Evasion**
  - Abschaltung Logging
  - Nutzung von blinden Flecken
- **Credential Access**
  - Auslesen PW-Hashes
  - Nutzung techn. User
- **Discovery**
  - Gültige Accounts auslesen
  - Berechtig. auslesen
- **Lateral Movement**
  - System Hopping (RFC)
  - Ausführung RFCs
- **Collection**
  - Sammlung von Daten
- **Command and Control**
  - Port-Änderung
  - Missbr. Web-Services
- **Exfiltration**
  - Daten-Export
- **Impact**
  - Sperren von Accounts
  - Manipulat. von Daten

Absicherung von SAP Systemen

ANALYSE

Prüfung der Ausgangslage in den Systemen und Prozessen.

KONZEPTION

Was können Quick-Wins sein?

Wie sieht die Reihenfolge der nächsten Schritte aus?

UMSETZUNG

Bereinigung von Findings, Umsetzung von Quick-Wins, Durchführung von Projekten.

NACHHALTIGKEIT

Sicherung der Investitionen durch Kontrollen, Monitoring und Prozesse. Regelmäßigkeit sicherstellen.

Meine Empfehlung

Andre Tenbuss

SAP Security Consultant

Xiting GmbH
Obere Ringstraße 17 | DE-79859
Schluchsee

Email: info@xiting.com
Tel. +49 7656 98881 55

Überblick verschaffen

Durch ein geeignetes Security Monitoring faktenbasierte Entscheidungen treffen können.

Berechtigungen für technische User

Schneller umsetzbar, als häufig vermutet. Enorme Verbesserung der Sicherheit.

Notfallkonzept

Denken Sie den Worst-Case: Sind Verantwortung, Prozesse und rechtliche Anforderungen bekannt?

2-Faktor-Authentifizierung & SSO

Das klassische Kennwort hat ausgedient. Setzen Sie überall – wo es möglich ist – auf 2FA und SSO.

Meine Empfehlung

Andre Tenbuss

SAP Security Consultant

Xiting GmbH
Obere Ringstraße 17 | DE-79859
Schluchsee

Email: info@xiting.com
Tel. +49 7656 98881 55

Überblick verschaffen

Durch ein geeignetes Security Monitoring faktenbasierte Entscheidungen treffen können.

Berechtigungen für technische User

Schneller umsetzbar, als häufig vermutet. Enorme Verbesserung der Sicherheit.

Notfallkonzept

Denken Sie den Worst-Case: Sind Verantwortung, Prozesse und rechtliche Anforderungen bekannt?

2-Faktor-Authentifizierung & SSO

Das klassische Kennwort hat ausgedient. Setzen Sie überall – wo es möglich ist – auf 2FA und SSO.