Shortcut

Webinar

Identify: SAP Risiken und Angriffsvektoren verstehen

Systematische Identifizierung von Schwachstellen
Einfluss von Compliance-Vorgaben

www.gonext.gmbh

Jessica Wolf
Daniel Vander Putten

15. April 2025

1. Warum ist “Identify” aus dem NIST Framework so entscheidend?

- Identify ist die strategische Grundlage für alle weiteren Sicherheitsmaßnahmen
- Ohne Risikoerkennung bleibt Sicherheit reaktiv
- Es geht nicht nur um Technik, sondern auch um Organisation, Verantwortlichkeiten und Prozesse
- „Je später Security berücksichtigt wird, desto teurer wird es“ – Frühzeitige Risikoerkennung spart Aufwand und Kosten

Typische Fragen der Identify-Phase:

- Was muss geschützt werden?
- Wo befinden sich sensible Daten?
- Welche Systeme sind kritisch?
- Wer ist verantwortlich?

2. Warum sind SAP-Systeme besonders gefährdet?

- SAP steuert geschäftskritische Prozesse (Finance, HR, SCM, Produktion)
- Systeme sind oft langlaufend, komplex und schlecht dokumentiert
- Sicherheitsverantwortung ist oftmals unklar oder fehlt ganz

Angriffsszenarien:

- Phishing mit SAP GUI Zugang
- Exploits ungepatchter Services
- Insider mit kritischen Berechtigungen
- Offene Schnittstellen oder externe RFC-Zugriffe

3. Typische SAP-spezifische Risiken

Zugriffsrisiken
- Übermäßige Berechtigungen
- Fehlen von SoD-Kontrollen (Segregation of Duties)

Systemrisiken
- Veraltete Komponenten
- Fehlendes Patch-Management

Integrationsrisiken
- Externe RFCs, IDocs, Odata-Services

Transaktionsrisiken
- Kritische Prozesse (Buchungen, Zahlungen) ohne Kontrolle

Organisatorische Risiken
- Unklare Zuständigkeiten
- SAP Security „hängt irgendwo“ – kein klares Ownership

Diese Risiken können nur erkannt werden, wenn SAP im Identify-Prozess voll mitgedacht wird

4. So funktioniert SAP-Risikoanalyse

1. Systeminventur (welche SAP-Systeme, Module, Schnittstellen?)
2. Rollenanalyse (wer darf was, wo sind Berechtigungsrisiken?)
3. Bedrohungsszenarien definieren
4. Schwachstellen identifizieren (z. B. per Tools oder Audit)
5. Bewertung nach Kritikalität (z. B. mit Risikomatrix)

Wichtig

- ✓ Risiken ehrlich bewerten – nichts „schönrechnen“
- ✓ Auch organisatorische & prozessuale Aspekte betrachten
- ✓ Beteiligung von IT, SAP-Team, Fachbereichen & Datenschutz

5. Regulatorische Anforderungen & Identify

NIS2 → Pflichten für Risikoanalyse, Sicherheitsmaßnahmen & Meldepflichten – SAP ist betroffen, wenn es geschäftskritische Prozesse steuert

DORA → Für den Finanzsektor: SAP als kritisches ICT-System – Anforderungen an Resilienz & Planung

DSGVO → Risikoanalyse bei personenbezogenen Daten in SAP (HCM, FI, CRM) Pflicht

6. Was heißt das konkret für SAP?

- Identify ist keine Option, sondern Pflicht
- SAP muss als Teil der IT-Risikolandschaft betrachtet und integriert werden
- Risiken dokumentieren, Verantwortlichkeiten klären, Notfallpläne erstellen
- Auch bei Angriffsszenarien (z. B. Ransomware) vorbereitet sein:
  - Offline-Dokumentation (z. B. Notfallhandbuch auf Papier)
  - Regelmäßige Überprüfung der Sicherheitsmaßnahmen

7. Handlungsempfehlungen

- ✓ Strukturiert mit Risikoanalyse starten (Systeme, Rollen, Schwachstellen)
- ✓ Risiken nach Kritikalität priorisieren
- ✓ Frühzeitig Management & Compliance einbinden
- ✓ Geeignete Tools einsetzen (z. B. XAMS, SIEM, Readiness Checks)
- ✓ Rollen- & Berechtigungskonzepte als nächster Schritt mitdenken
- ✓ Schulungen & Awareness im Unternehmen aufbauen

Interesse geweckt?
Dann nimm gerne auch am nächsten Webinar teil!

An einem persönlichen Gespräch interessiert?
Buche hier direkt deinen Termin!

Scanne oder klicke hier!

Deine Ansprechpartnerin:

Jessica Wolf
SAP Security Consultant

info@gonext.gmbh