

Hacking von SAP®-Systemen

Angriffe verstehen und abwehren

» Hier geht's
direkt
zum Buch

DIE LESEPROBE

Kapitel 2

SAP-Sicherheit per Default: Standards und aktuelle SAP-Sicherheitswerkzeuge

In diesem Kapitel werfen wir einen Blick auf die SAP-Strategie zum Thema Sicherheit sowie die Produkte in diesem Themenumfeld, die von SAP selbst angeboten werden.

SAP hat eine Vielzahl von Produkten herausgebracht, die sich dem Thema »Sicherheit« zuordnen lassen. Die vorhandenen Lösungen decken sowohl On-Premise-Systeme wie SAP ERP und die On-Premise-Variante von SAP S/4HANA als auch die Cloud-Systeme und hybride Landschaften ab, etwa im Rahmen von RISE with SAP und der SAP Business Technology Platform (SAP BTP).

Darüber hinaus hat SAP in den letzten Jahren viel getan, um seine Sicherheitsrichtlinien zu erweitern und in die sichere Grundkonfiguration der ausgelieferten Produkte (*Security by Default*) investiert. In diesem Kapitel beginnen wir in Abschnitt 2.1 zunächst mit einem Blick auf die klassische SAP-Sicherheitsarchitektur und diskutieren, wie sich dieser Blick heute verändert hat. In Abschnitt 2.2 erläutern wir, was es mit dem neuen Ansatz der Security by Default auf sich hat und was das für die Softwareentwicklung bedeutet (Abschnitt 2.3, »Integration von Sicherheitsanforderungen in den Entwicklungsprozess«).

Im weiteren Verlauf des Kapitels wollen wir darstellen, auf welchen Produkten die klassische SAP-Sicherheitsarchitektur beruht. Wir betrachten dabei ausschließlich SAP-Produkte und diskutieren, was im Sinne der Standardauslieferung dieser Produkte als sicher gilt. Dabei gehen wir auf die SAP BTP (Abschnitt 2.4), das Security Audit Log (Abschnitt 2.5), SAP Enterprise Threat Detection (Abschnitt 2.6), den SAP Code Vulnerability Analyzer (Abschnitt 2.7), das geplante SAP Security Dashboard (Abschnitt 2.8) und SAP Cloud ALM (Abschnitt 2.9) ein. Darüber hinaus gibt natürlich noch zahlreiche Sicherheitsprodukte von SAP-Partnern, die wir in diesem Kapitel jedoch nicht thematisieren werden. Wir wollen hier den Blick auf die Standardprodukte lenken und diese in den Kontext Ihrer unternehmenseigenen dauer-

Aufbau dieses Kapitels

haften SAP-Security-Initiative stellen. Abschließend stellen wir Ihnen in Abschnitt 2.10 die wichtigsten Quellen für SAP-Sicherheitsrichtlinien vor.

2.1 Der Blick auf die klassische SAP-Sicherheitsarchitektur

Der Blick auf die SAP-Sicherheit durch SAP-Teams, Berater oder SAP-Spezialisten bei Anwenderunternehmen hat sich noch nicht so drastisch geändert, wie es die aktuelle Sicherheitslage in der IT erfordern würde. Die zentrale Technologie des (On-Premise-)SAP-Systems und die tägliche Arbeit ändern sich immer noch zu langsam. Was sich geändert hat, sind wohl die ständigen Anforderungen an die Sicherheit von SAP-Systemen, die von außen durch Institutionen wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in das SAP-Umfeld herangetragen werden. Diese Anforderungen beziehen sich vor allem auf die Einhaltung des Grundschutzes und die Erfüllung der Mindestnormen für ERP-Systeme.

SAP-Welt nicht
isoliert

Aus Sicht des Chief Security Officers (CSO) Ihrer Organisation sieht die Bedrohungslage heute anders aus, als man es in der recht abgeschlossenen SAP-Welt vermuten könnte. Sicherheitsbedrohungen gelten für die gesamte Organisation und vor allem für die gesamte IT. Das SAP-System als sprichwörtliche »Insel« entspricht nicht mehr der Realität in der heutigen Zeit. Die Meldungen über ständige Angriffe und aktuelle Gefährdungen im Cyberspace sind sehr real – aber bislang nicht explizit gegen SAP gerichtet. Wichtig ist in diesem Kontext die Erkenntnis, dass die SAP-Systeme nicht isoliert von der sonstigen Unternehmens-IT zu betrachten sind. Viele Angriffe richten sich pauschal gegen alle Server und die gesamte IT-Infrastruktur und nicht, wie man meinen könnte, nur gegen die E-Mail-Server oder das Active Directory mit den zentralen Zugangsdaten. Angegriffen werden alle schwach gesicherten Systeme, die einfache Beute versprechen und für die ein Hack in kurzer Zeit zu realisieren ist. Wenn Ihre eigenen SAP-Systeme genau in diese Kategorie fallen, werden sie unweigerlich zu einem Kollateralschaden eines Angriffs, der gegen die Unternehmens-IT gerichtet ist.

SAP-Sicherheit als
Teil der Unternehmenssicherheit

Deshalb ist es wichtig, dass Sicherheitsfragen in die gesamte Infrastruktur und in die SAP-Landschaft mit einbezogen werden. Sicherheit ist ein kontinuierlicher Prozess, der nie aufhört und in immer neuen Betrachtungen bei allen Aktivitäten in der SAP-Welt berücksichtigt werden muss. Sei es ein neuer SAP-Server oder eine neue Cloud-Anwendung, sei es der Aufbau einer hybriden SAP-Landschaft im Kontext von RISE with SAP oder ein klassischer Ausbau der SAP-Anwendungen – jedes Projekt im SAP-Umfeld hat seine He-

rausforderungen im Bereich der Sicherheit und wird sich auf den sicheren Betrieb der gesamten Landschaft und Infrastruktur auswirken.

2.2 Security by Default

Security by Default ist ein Ansatz in der IT-Sicherheit, der darauf abzielt, Produkte und Systeme von Anfang an mit sicheren Voreinstellungen auszuliefern. Diese Idee, die eigentlich jedem Softwareprodukt zugrunde liegen sollte, ist erst in den letzten Jahren von den SAP-Kunden aufgenommen und in Initiativen wie der Deutschsprachigen SAP-Anwendergruppe (DSAG) an SAP herangetragen worden. Mit den vielen Forderungen nach immer höheren Sicherheitsanforderungen wird auch deutlich, warum SAP dieses Thema bisher vernachlässigt hat. Wir stellen in diesem Kapitel dar, wie es sich heute in allen neuen Systemen widerspiegeln soll.

Anstatt die SAP-Kunden dazu zu zwingen, komplexe Sicherheitskonfigurationen manuell vorzunehmen, werden die Systeme heute standardmäßig so eingerichtet, dass sie den höchsten Sicherheitsstandards entsprechen, ohne die Funktionalität oder Benutzerfreundlichkeit zu beeinträchtigen. Diese Philosophie stellt sicher, dass selbst dann, wenn keine zusätzlichen Anpassungen durch die Kunden vorgenommen werden, ein grundlegender Schutz vor Bedrohungen der Sicherheit gewährleistet ist.

Security by Default
bei SAP

Security by Default unterscheidet sich von anderen Sicherheitsansätzen durch seinen präventiven Charakter. Im Gegensatz zum Ansatz *Security by Design*, der sich auf die Implementierung von Sicherheitsfunktionen bereits während der Entwicklung eines Produkts konzentriert, bezieht sich Security by Default auf die Konfiguration des Produkts bei der Auslieferung. Der Ansatz stellt sicher, dass ein Produkt unmittelbar einsatzbereit ist, ohne dass zusätzliche Sicherheitsanpassungen erforderlich sind. Alle SAP-Produkte – sowohl On-Premise- als auch Cloud-Produkte – sollen standardisiert den aktuellen Sicherheitsvorgaben entsprechen. Die neuen SAP-S/4HANA-Systeme haben daher eine relativ robuste Security-Standardkonfiguration. Diese umfasst verschlüsselte Kommunikation, sichere Berechtigungsmodelle und eine robuste Protokollierung von Aktivitäten. Eine Härtung der SAP-Profilparameter und damit eine umfangreiche Grundsicherung der Konfiguration sind jedoch ebenso wichtig wie früher. Empfehlungen dazu werden in den SAP-Sicherheitsleitfäden formuliert. Ziel des Security-by-Default-Ansatzes ist es, Sicherheitslücken in einem Projekt bzw. bei einer Installation von Beginn an zu minimieren und damit der SAP-Administration eines Unternehmens eine solide Grundlage für den Schutz der geschäftskritischen Anwendungen und Daten zu übergeben.

Präventive
Maßnahmen

Sicherheitsvorgaben für SAP S/4HANA

Warum verfolgt SAP den Security-by-Default-Ansatz gerade jetzt? Die zunehmende Digitalisierung und Vernetzung von Projekten im Zuge der digitalen Transformation im SAP-Bereich bringt nicht nur Vorteile, sondern auch neue Herausforderungen für die IT-Sicherheit. Cyberangriffe werden immer raffinierter, und Systeme sind ohne effektive Sicherheitsvorkehrungen anfällig für Datenverluste, Manipulationen und Betriebsunterbrechungen. In einer solchen Umgebung ist es unerlässlich, dass Sicherheitsmaßnahmen nicht erst nachträglich implementiert, sondern von Anfang an fest in die Produkte integriert werden. Dieses Mantra kann nicht oft genug wiederholt werden. Es gilt nicht nur für die IT-Sicherheit, sondern auch besonders für die SAP-Systeme.

Gerade bei den aktuellen Migrationsprojekten auf SAP S/4HANA und die SAP BTP ist es für Unternehmen von grundlegender Bedeutung, eine ausformulierte SAP-Sicherheitsstrategie zu haben, zu deren Grundlagen die von SAP und anderen Institutionen wie dem BSI oder der DSAG ausgearbeitete Empfehlungen gehören.

Einstieg in eine sichere SAP-Landschaft erleichtern

Die eigentliche Idee von SAP ist es, mit dem neuen *Security by Default* von SAP S/4HANA, RISE und SAP BTP Cloud-Unternehmen den Einstieg in eine sichere Systemlandschaft zu erleichtern. Durch vordefinierte, geprüfte Sicherheitskonfigurationen ist es einfacher, die folgenden Themen richtig zu adressieren.



Übersteuerung von Sicherheitseinstellungen bei der Brownfield-Migration

Bei vielen Kunden, die mit dem Brownfield-Ansatz auf SAP S/4HANA migrieren, entsteht derzeit die Situation, dass viele dieser Grundsicherungen übersteuert werden. Dies muss bei den Migrationsprojekten immer wieder hinterfragt und geprüft werden, damit nicht eine grundlegende Sicherheit wieder mit alten Konfigurationen übersteuert wird.

SAP-Produkte operieren in unterschiedlichsten Umgebungen – von kleinen, lokal gehosteten Systemen bis hin zu komplexen, globalen Cloud-Infrastrukturen. Security by Default sorgt dafür, dass unabhängig von der spezifischen Umgebung einheitliche Sicherheitsstandards eingehalten werden. Zum Beispiel werden bei Cloud-Lösungen wie der SAP BTP Sicherheitsmaßnahmen wie Multi-Faktor-Authentifizierung und Datenverschlüsselung von Anfang an aktiviert. Für On-Premise-Produkte wie SAP S/4HANA stellt Security by Default sicher, dass sichere Berechtigungsmodelle und Transportverschlüsselung bereits in der Standardkonfiguration enthalten sind.

Sicherheitsprinzipien bilden das Fundament jeder effektiven Sicherheitsstrategie und sind auch bei der Umsetzung von Security by Default durch SAP zentral. SAP hat die folgenden Prinzipien in die Architektur und Konfiguration seiner Produkte integriert, um den Kunden eine robuste Grundlage für den Schutz ihrer Systeme zu bieten:

Prinzipien von
Security by
Default

■ Minimalberechtigungen

Das Prinzip der *Minimalberechtigungen* stellt sicher, dass Benutzer und Anwendungen nur die Berechtigungen erhalten, die sie für ihre Aufgaben tatsächlich benötigen. Durch die Begrenzung der Zugriffsrechte auf ein Minimum wird das Risiko von Missbrauch und Fehlkonfigurationen reduziert.

In SAP-Systemen wird dieses Prinzip durch ein fein abgestimmtes Berechtigungsmanagement umgesetzt. Zum Beispiel ermöglichen Rollen und Profile in SAP S/4HANA eine granulare Steuerung der Berechtigungen. Administratoren können den Zugriff auf bestimmte Transaktionen, Daten oder Funktionen präzise regeln. Dies verhindert, dass Benutzer versehentlich oder absichtlich auf sensible Daten zugreifen oder kritische Systemänderungen vornehmen können.

■ Regelmäßige Überprüfungen der Berechtigungen

Regelmäßige Überprüfungen der Berechtigungen, sogenannte *Role-Mining-Analysen*, helfen dabei, überflüssige oder zu weit gefasste Berechtigungen zu identifizieren und zu entfernen. Dies betrifft aber nicht nur die Berechtigungen. Härtungsmaßnahmen wie die Standardisierung der SAP-Security-Parameter in den SAP-Profilen oder die Passwortrichtlinien sollten ebenfalls immer regelmäßig überprüft werden.

■ Schichtenmodell oder Defense in Depth

Defense in Depth basiert auf der Idee, mehrere Sicherheitsmaßnahmen in verschiedenen Schichten zu kombinieren, um ein System umfassend zu schützen. Selbst wenn eine Sicherheitsmaßnahme umgangen wird, bleiben so andere Mechanismen wirksam. Folgende Schichten werden dabei unterschieden:

- *Netzwerkebene*: Auf der Netzwerkebene erfolgt standardmäßig eine Absicherung durch Firewalls, Virtual Private Networks (VPNs) und Intrusion Detection/Prevention-Systeme (IDS/IPS).
- *Systemebene*: Auf der Ebene der einzelnen Systeme gibt es eine Verschlüsselung (z. B. SSL/TLS), und die Systemhärtung wird durch die Deaktivierung unnötiger Dienste sichergestellt.
- *Anwendungsebene*: Auf der Anwendungsebene werden Zugriffskontrollen, Datenverschlüsselung und Sicherheitsprüfungen bei Benutzerinteraktionen eingesetzt.

Diese mehrschichtige Sicherheitsarchitektur stellt sicher, dass auch bei einem Angriff auf eine Ebene (z. B. ein kompromittiertes Benutzerkonto) weitere Schutzmaßnahmen greifen. Bei der Definition dieser übergreifenden Muster wird auch ein Verständnis dafür entwickelt, wie verschiedene Sicherheitsmaßnahmen, die bereichsübergreifend sind, sich auf die SAP-Systeme auswirken.

**Sicherheitsthemen
abteilungsübergrei-
fend behandeln**

In dem standardisierten Organisationsdenken in SAP-Abteilungen war bisher »die Basis« für diese Themen zuständig. Heute ist es wichtig, diese Sicherheitsmaßnahmen auch als abteilungsübergreifendes Thema zu sehen. Involviert werden müssen neben der allgemeinen IT-Sicherheit auch immer das Security Operations Center (SOC) oder der jeweilige Sicherheitsverantwortliche wie der CISO und seine Abteilung.



Beispiele für sichere Voreinstellungen

Im Folgenden führen wir einige Beispiele für sichere Voreinstellungen in SAP-Produkten auf:

- **Verschlüsselte Kommunikation**
SAP-Systeme sind so konfiguriert, dass Datenübertragungen standardmäßig verschlüsselt erfolgen.
- **Standardrollen**
Die mitgelieferten Benutzerrollen sind sicher vorkonfiguriert – ohne überflüssige Berechtigungen.
- **Log-Aktivierung**
Überwachungs- und Protokollierungsmechanismen wie das Security Audit Log sind in vielen Produkten standardmäßig aktiviert.
- **Profilparameter**
Die ausgelieferten SAP-Profilparameter sind nach den aktuellen Sicherheitsvorgaben ausgeprägt.

Durch regelmäßige Sicherheitsupdates stellt SAP sicher, dass diese Voreinstellungen den neuesten Standards entsprechen.

2.3 Integration von Sicherheitsanforderungen in den Entwicklungsprozess

Security by Default sollte auch die Grundlage eines jeden Entwicklungsprozesses sein. Dies gilt vor allem in den neuen hybriden SAP-Umgebungen oder für Entwicklungen auf der SAP BTP. Um die Sicherheitsprinzipien

effektiv umzusetzen, ist es entscheidend, dass Sicherheit bereits in den grundlegenden Entwicklungsprozess integriert wird. SAP verfolgt hier einen proaktiven Ansatz, der Sicherheit als festen Bestandteil des Lebenszyklus eines Produkts betrachtet.

Secure Software Development Lifecycle (SDLC) ist ein strukturierter Prozess, der sicherstellt, dass Sicherheitsaspekte in jeder Phase der Softwareentwicklung berücksichtigt werden. SAP unterstützt diesen Ansatz mit verschiedenen Werkzeugen. Bei der Integration von SDLC in den aktiven Entwicklungsprozess sollte man die folgenden Elemente berücksichtigen:

Secure Software
Development
Lifecycle

■ Anforderungsanalyse

Sicherheitsanforderungen sollten von Beginn an definiert und priorisiert werden. Die Frage nach dem Sicherheitskonzept in den Anwendungen sollte in jeder Vorlage für eine Entwicklungsanforderung berücksichtigt sein. Es kann nicht genug betont werden, dass die gesamte Anwendungsentwicklung, also SAP- und Nicht-SAP-Entwicklung, Cloud- und Webentwicklung, ausführlich in den Sicherheitsrichtlinien (*Policies*) beschrieben sein sollte.

■ Code Reviews

Entwickler sollten den Code auf Schwachstellen wie Remote Code Execution (RCE), SQL Injection oder Cross-Site Scripting (XSS) überprüfen. Es gibt sowohl für die SAP BTP als auch für ABAP-On-Premise-Systeme einen Satz von Anforderungen an eine sichere Programmierung, die für jedes Unternehmen als Richtlinie verbindlich verabschiedet werden sollten. Wichtige Anforderungen in diesem Bereich behandeln wir sowohl in Kapitel 10, »Manipulation des kundeneigenen Codes: ABAP-Angriffe«, als auch in Kapitel 13, »Angriffe auf SAP-Cloud-Anwendungen«.

■ Sicherheitszertifizierungen

Vor der Veröffentlichung sollte die Software umfassend getestet und zertifiziert werden, um Sicherheitsmängel auszuschließen. Das SSDLC-Konzept mit seinen Bausteinen ist darauf ausgelegt, Sicherheitslücken frühzeitig zu identifizieren und zu beseitigen, bevor sie in die Produktsysteme gelangen.

■ Automatisierte Tests auf Sicherheitslücken

Automatisierung spielt eine entscheidende Rolle bei der Effizienz und Wirksamkeit der Sicherheitsüberprüfungen. SAP setzt verschiedene Tools ein, um Sicherheitslücken schnell und zuverlässig zu erkennen. Die On-Premise-Systeme sind hier etwas besser aufgestellt, die entsprechenden Werkzeuge für die Cloud-Komponenten werden nach und nach fertiggestellt.

■ **SAP Code Vulnerability Analyzer**

Dieses Werkzeug analysiert Quellcode auf potenzielle Schwachstellen und gibt Empfehlungen zu deren Beseitigung und sollte in jeder Kundeninstanz eingesetzt werden. Der SAP Code Vulnerability Analyzer kann sowohl für die On-Premise-Systeme als auch für die SAP BTP eingesetzt werden (siehe auch Abschnitt 2.7, »SAP Code Vulnerability Analyzer: Schutz des kundeneigenen Codes«).

■ **Dynamic Application Security Testing (DAST)**

DAST umfasst Tests zur Analyse von Anwendungen während ihrer Laufzeit, um Schwachstellen wie unsichere Schnittstellen zu identifizieren. In den SAP-On-Premise-Systemen wird das *ABAP Test Cockpit (ATC)* für solche Tests verwendet.

■ **Penetrationstests**

Automatisierte Penetrationstests simulieren Angriffe auf SAP-Systeme, um Schwachstellen aus der Sicht eines Angreifers zu finden. Diese Tests helfen dabei, die Sicherheit von SAP-Produkten kontinuierlich zu verbessern und Kunden ein hohes Maß an Schutz zu bieten. Hervorzuheben sind hier vor allem Penetrationstests auf selbst entwickelte Anwendungen, die neben dem reinen Angriffsszenario auch Elemente eines Workshops enthalten, in dem Entwickler und »Hacker« an einem Tisch sitzen und Angriff und Verteidigung im Programmcode interaktiv diskutieren.

2.4 SAP BTP: Sicherheit mit neuer Softwaregeneration

**Sichere Cloud-
Plattform**

Die SAP Business Technology Platform (SAP BTP) ist aus der Perspektive der Sicherheit besser, als es der erste Eindruck oder die ständigen Nachrichten über Cloud-Einbrüche vermuten ließen. SAP als Cloud-Anbieter hat hier viel gelernt, und die aktuellen Versionen vermitteln ein sicheres Gesamtbild, das den Security-by-Default-Ansatz für eine Cloud-Lösung angemessen umsetzt.



Maßstab für Sicherheitsgradeinschätzungen

Es ist immer schwierig, eine Aussage über Cloud-Systeme und deren Sicherheit zu treffen. Alle Systeme sind prinzipiell angreifbar, wenn die kriminelle Energie und die Fähigkeiten entsprechend hoch sind. Wenn wir in diesem Buch eine Meinung zum Grad der Sicherheit formulieren, sind unser Maßstab immer die Fähigkeiten eines klassischen APT-Angreifers (Advanced Persistent Threat), also eines Angreifers aus der organisierten Kriminalität oder einer Gruppe, die auf Geld und Erpressung aus ist. Die Gruppe der *State*

Level Actors, also der organisierten Angreifer aus Geheimdiensten, die von Staaten finanziert und organisiert werden, sind hier nicht eingeschlossen. Diese Organisationen können sich Zero-Day Exploits (bisher unentdeckte Sicherheitslücken) leisten oder Hersteller zwingen, Backdoors einzubauen. Gegen diese Art von Bedrohung ist kaum ein Schutz möglich. Wenn man versucht, sein *Blue Team*, also seine Verteidigung, auch auf diesen Bereich auszudehnen (etwa weil man selbst ein KRITIS-Unternehmen ist), sind der Aufwand, die personelle Ausstattung und das benötigte Wissen entsprechend hoch.

2.4.1 SAP und die OWASP Top 10

Großunternehmen nutzen die SAP BTP, um cloud-native Anwendungen zu entwickeln, Geschäftsprozesse zu automatisieren, Integrationen und Erweiterungen zu ermöglichen, Daten effizient zu verwalten und Analysen zu verbessern – neben vielen weiteren Funktionen. In unserem digitalen Zeitalter gewinnt Cybersicherheit zunehmend an Bedeutung, da Unternehmen immer stärker auf Plattformen wie die SAP BTP angewiesen sind, um Innovationen voranzutreiben, Anwendungen zu modernisieren und das Geschäftswachstum zu fördern. Doch diese Abhängigkeit bringt auch erhebliche Herausforderungen im Bereich der Cybersicherheit mit sich, insbesondere im Hinblick auf die weit verbreiteten Schwachstellen, die vom *Open Web Application Security Project* (OWASP) identifiziert wurden. Die *OWASP Top 10* sind ein essenzielles Dokument für Entwicklerteams und IT-Sicherheitsfachleute, das die größten Sicherheitsrisiken für Webanwendungen aufzeigt und wertvolle Leitlinien zur Verbesserung der Cybersicherheit bietet.

SAP unterstreicht die Wichtigkeit, die umfassenden Sicherheitskontrollen und -dienste der SAP BTP auf Übereinstimmung mit den Best Practices von OWASP hin zu prüfen, um kritische Cyberbedrohungen abzuwehren. Wir werfen im Folgenden einen detaillierten Blick auf die spezifischen Funktionen der SAP BTP, die dazu beitragen, OWASP-Schwachstellen zu minimieren, und beleuchten den mehrschichtigen Sicherheitsansatz der Plattform, mit dem Unternehmensanwendungen und -prozesse geschützt werden können.

OWASP-Sicherheitskriterien für die SAP BTP

Was ist »OWASP«, und was sind die »OWASP Top 10«?

OWASP ist eine weltweit anerkannte, gemeinnützige Organisation, die sich der Verbesserung der Sicherheit von Software verschrieben hat. Die Organisation wurde 2001 gegründet und ist bekannt für ihre umfangreichen



Leitlinien, Tools und Ressourcen, die Entwicklern, Unternehmen und IT-Sicherheitsfachleuten helfen, sicherere Anwendungen zu erstellen.

Die Organisation bietet eine Plattform, auf der Best Practices, Sicherheitsrisiken und Schutzmaßnahmen für Webanwendungen diskutiert und geteilt werden. Ihre Projekte und Veröffentlichungen sind gemeinfrei und können von jedem genutzt werden, um ein besseres Verständnis für Cybersicherheitsrisiken und -lösungen zu entwickeln.

Die OWASP Top 10 sind ein Dokument, das die häufigsten und kritischsten Sicherheitsrisiken für Webanwendungen identifiziert. Es ist eine Art Leitfaden, der Entwicklern und Sicherheitsverantwortlichen hilft, die dringendsten Bedrohungen zu erkennen und zu adressieren. Die Liste wird regelmäßig aktualisiert (meist alle drei bis fünf Jahre), um den neuesten Bedrohungen und Technologien Rechnung zu tragen.

Rolle der SAP BTP

Die SAP BTP spielt eine zentrale Rolle in der Cloud-Architektur von SAP. Die Plattform ist nicht nur ein wesentlicher Bestandteil zahlreicher SaaS-Anwendungen (Software as a Service), die von Kunden sowie innerhalb von SAP genutzt werden, sondern stellt auch erweiterte Sicherheits-, Leistungs- und Zuverlässigkeitsfunktionen für SAP-Systeme bereit. Um die Cloud-Infrastruktur der SAP BTP zu sichern, setzt SAP auf zahlreiche Schutzmaßnahmen, darunter die Absicherung der Cloud-Foundry-Umgebung mit HAProxy, Load Balancern, DNS-Sicherheit, Proxy-Diensten, Netzwerkadressübersetzung (NAT), DDoS-Schutz, netzwerkbasierte Segmentierung, Sicherheitsgruppen und strikte Zugriffskontrollen. Darüber hinaus nutzt SAP die nativen Sicherheitsmechanismen führender Hyperscaler.

Neben diesen grundlegenden Schutzmaßnahmen bietet die SAP BTP Sicherheitsfunktionen, die speziell zur Abwehr von OWASP-Schwachstellen entwickelt wurden. Damit sollen den SAP-Kunden leistungsstarke Werkzeuge an die Hand gegeben werden, um ihre digitalen Infrastrukturen effektiv zu schützen und Sicherheitsrisiken nachhaltig zu minimieren.

Unsere Prüfung von OWASP-Schwachstellen

Wir haben die Liste der OWASP Top 10 in einer SAP-Cloud-Umgebung auf Basis der SAP BTP getestet und diese Sicherheitsprüfungen unterzogen. Das Ergebnis war überraschend positiv. Die meisten Angriffsvektoren konnten nicht ausgenutzt werden oder waren entsprechend gut gehärtet.

Unsere Prüfungen bezogen sich dabei auf die SAP-Anwendungen in der Cloud. Kundeneigene Implementierungen müssen Sie selbst auf ihren Schutz gegen solche Angriffe hin prüfen. Im Folgenden beschreiben wir unsere Prüfung einer allgemeinen SAP-Cloud-Instanz hinsichtlich der zehn

zentralen Schwachstellen laut OWASP, wie sie auch von SAP als Leitlinie der eigenen Sicherheitsdefinition verwendet werden und als Maßstab für den Schutz dienen sollten:

1. Broken Access Control (Schwachstellen bei der Zugriffssteuerung)

Schwache oder fehlende Kontrollen ermöglichen es Angreifern, auf sensible Daten oder Funktionen zuzugreifen, die für sie nicht vorgesehen sind. Zu den Sicherheitsmaßnahmen in diesem Bereich zählt auch die Multi-Faktor-Authentifizierung (MFA), die in einer Cloud-Umgebung zwingend erforderlich ist. Leider hat hier die *SAP Universal ID* eine entscheidende Schwäche, da man zwar optional eine MFA hinzuschalten kann, die SAP-Anmeldung kann aber weiterhin nur mit SAP-Benutzer-ID und Passwort erfolgen und damit diese Sicherungsmaßnahme unterlaufen.

2. Cryptographic Failures (Kryptografische Schwachstellen)

Eine unsichere Nutzung oder Implementierung von Verschlüsselung kann zu einem Verlust von Vertraulichkeit oder Integrität führen. Alle SAP-Anwendungen in der Cloud erfordern das Verschlüsselungsprotokoll *Transport Layer Security* (TLS) für den Zugang. Generell gilt, dass in einer SAP-Landschaft alle Verbindungen ausnahmslos den Standard TLS 1.3 erfüllen sollten (Mindeststandard des BSI zur Verwendung von Transport-Layer-Security-Version 2.3).

3. Injection (Injektionsangriffe)

Angriffe, bei denen schädlicher Code (z. B. SQL, NoSQL, LDAP) in eine Anwendung eingeschleust wird, um auf Daten zuzugreifen oder diese zu manipulieren, können auf SAP-Fiori-Anwendungen, die mit Standardbibliotheken und nach Standardregeln programmiert sind, nicht durchgeführt werden, da diese normalisiert werden und nicht ohne Bereinigung in das Backend durchgereicht werden.

4. Insecure Design (Unsicheres Design)

Sicherheitsprobleme, die durch fehlende oder unzureichende Sicherheitsüberlegungen im Designprozess entstehen, werden durch die Einhaltung der SAP-Sicherheitsrichtlinien verhindert.

5. Security Misconfiguration (Fehlkonfiguration von Sicherheitsmaßnahmen)

Falsch konfigurierte Systeme, Frameworks oder Anwendungen, die Angreifern Möglichkeiten bieten, Schwachstellen auszunutzen, sind nie auszuschließen. Deswegen sind Fehlkonfigurationen das beliebteste Suchziel der Angreifer.

6. Vulnerable and Outdated Components (Verwundbare und veraltete Komponenten)

Die Nutzung von nicht gepatchten, veralteten oder unsicheren Softwarekomponenten, wie Bibliotheken oder Frameworks, ist ein Standardangriffsvektor. Hacker suchen gezielt nach nicht gepatchten Komponenten. Sowohl für SAP-On-Premise-Systeme als auch für Cloud-Komponenten gilt daher, dass der *SAP Security Patch Day* besonderer Aufmerksamkeit bedarf und Sicherheitspatches sofort eingespielt werden müssen.

7. Identification and Authentication Failures (Fehler bei Identifikation und Authentifizierung)

Schwächen in der Benutzerverwaltung, etwa unsichere Passwörter, schlechte Authentifizierungsverfahren oder unzureichender Schutz sensibler Konten, sollten beseitigt werden. Dazu zählt auch die Benutzung der SAP Universal ID ohne Multi-Faktor-Authentifizierung.

8. Software and Data Integrity Failures (Versagen der Software- und Datenintegrität)

Eine mangelhafte Überprüfung der Software- und Datenintegrität, etwa durch nicht vertrauenswürdige Updates oder ungesicherte Datenflüsse, ist ein Angriffsvektor, der sich immer größerer Beliebtheit erfreut. Lesen Sie dazu auch unsere Ausführungen zum Thema Software Supply Chain in Abschnitt 1.2, »Die Konsequenzen für die technische Sicherheit von IT-Systemen«.

9. Security Logging and Monitoring Failures (Fehlende Sicherheitsprotokollierung und Überwachung)

Erfolgt eine unzureichende Protokollierung und Überwachung von sicherheitsrelevanten Ereignissen, werden Angriffe erst spät oder gar nicht erkannt. Generell gilt, dass SAP verantwortlich für alle Protokolle der Anwendungen auf der SAP BTP ist und diese nach Definition in SAPs Service Level Agreements als Dienste bereitstellt. Diese Protokolle werden also als gesichert angesehen. Eigene Protokolle in der Cloud müssen ebenso gesichert werden.

10. Server-Side Request Forgery (SSRF)

SSRF ist eine Schwachstelle, bei der ein Angreifer den Server dazu bringt, Anfragen an nicht vertrauenswürdige Ziele zu senden. Bei SAP-Fiori-Anwendungen, die mit Standardbibliotheken und nach Standardregeln programmiert sind, können solche Angriffe nicht durchgeführt werden. Ebenso kann dies mit einer im Standard gesicherten API-Programmierung ausgeschlossen werden.

Aus Sicht der Sicherheitsforscher und der SAP-Penetrationstester können wir den guten Sicherheitsstandard der SAP BTP nur unterstreichen. Direkte Angriffe, Brute-Force-Attacken und Angriffe auf das Identity Management müssten auf internationalem Niveau sein, um die Sicherheitsmaßnahmen der SAP BTP außer Kraft zu setzen. Die Security-by-Default-Einstellungen der SAP BTP Cloud ermöglichen keine Fehlkonfigurationen und weisen keine Schwachstellen auf, die ohne extrem großen Aufwand ausgenutzt werden könnten.

Hoher Sicherheitsstandard

2.4.2 SAP-Sicherheitskonzepte für die Cloud

SAPs Sicherheitsstrategie für die Cloud gründet auf vier Pfeilern und bildet die Basis für alle Sicherheitsprodukte, Richtlinien und Empfehlungen im Bereich SAP-Sicherheit. Diese vier Pfeiler sind in Abbildung 2.1 in einer Matrix dargestellt.

SAP-Sicherheitsmatrix

Firmenrichtlinien	Firmeneigene Sicherheitsrichtlinien	Sicherheit und Governance	Eigenes Risikomanagement	Cloud-Sicherheit	IT-Sicherheitsorganisation
SAP Identity Management	Benutzer- und Identitätsverwaltung	Authentifizierung und Single Sign-on	GRC/Rollen und Berechtigungen	Cloud Identity and Risk Management	SAP-Sicherheitsorganisation
SAP-Anwendungssicherheit	Sicherheit und Anwendungsmanagement	Betrugserkennung	Sicherheit des kundeneigenen Codes (ABAP, Cloud, Web)	Cloud-Anwendungssicherheit	
SAP-System-sicherheit	Sicherheit/Härtung	SIEM	Monitoring und Forensik	SAP-Cloud-Sicherheit	
SAP-Netzwerk-/Betriebssystem-Sicherheit/Cloud-Betrieb	Netzwerk-sicherheit	Betriebssystem- und Datenbank-sicherheit	Benutzer-sicherheit	Cloud-Interoperabilität	

Abbildung 2.1 Matrix für die SAP-Sicherheit

Die SAP-Cloud-Security-Richtlinie ist darauf ausgerichtet, alle wesentlichen Anforderungen im Bereich des Identitätsmanagements, der Anwendungssicherheit, der Systemsicherheit sowie der Netzwerksicherheit innerhalb der SAP-Umgebung zu adressieren. Im Mittelpunkt stehen dabei technische Aspekte, die ein solides Sicherheitsfundament für cloud-basierte SAP-Systeme schaffen und auf die Bedürfnisse eines technisch orientierten Publikums zugeschnitten sind.

Eine umfassende SAP-Sicherheitsrichtlinie ist essenziell, um den Schutz von Systemen, Anwendungen, Daten und Netzwerken sicherzustellen. Sie sollte alle wesentlichen Bereiche dieser Matrix abdecken, um den Anforderungen moderner IT-Infrastrukturen gerecht zu werden. Die Sicherheitsmatrix dient als Leitplanke für ein ganzheitliches Framework, das nicht nur technische Sicherheit, sondern auch die notwendige Flexibilität bietet, um den Anforderungen einer dynamischen Cloud-Umgebung gerecht zu werden.

Vier Säulen Im Folgenden gehen wir kurz auf die vier Säulen der SAP-Sicherheitsstrategie ein:

■ Identity Management

Im Bereich des Identity Managements (IDM) sind klare Vorgaben zur Verwaltung von Benutzern und deren Authentifizierung unerlässlich. Dabei kommen Mechanismen wie Multi-Faktor-Authentifizierung (MFA) oder Single Sign-on (SSO) zum Einsatz, um sowohl Sicherheit als auch Benutzerfreundlichkeit zu gewährleisten. Zudem müssen Richtlinien zur Vergabe und Überwachung von Rollen und Berechtigungen festgelegt werden, die sicherstellen, dass Governance-, Risk- und Compliance-Anforderungen erfüllt werden. Wichtig ist auch, dass Protokollierungen und Überwachungsmaßnahmen greifen, um potenzielle Risiken frühzeitig zu erkennen und gesetzlichen Vorgaben nachzukommen.

■ Anwendungssicherheit

Ein weiterer zentraler Aspekt ist die Anwendungssicherheit. Diese umfasst die Prüfung und Absicherung von benutzerdefiniertem Code, z. B. in ABAP oder Java, um Schwachstellen zu vermeiden. Sichere Entwicklungspraktiken und regelmäßige Sicherheitsscans tragen maßgeblich dazu bei, Risiken zu minimieren. Darüber hinaus sollte die Sicherheitsrichtlinie Mechanismen zur Erkennung und Vermeidung von Betrug enthalten. Bei Cloud-Anwendungen wie SAP S/4HANA Cloud müssen spezifische Maßnahmen getroffen werden, um hybride Umgebungen sicher zu integrieren.

■ Systemsicherheit

Die Sicherheit der SAP-Systeme selbst spielt ebenfalls eine große Rolle. Dazu zählen vor allem Maßnahmen zur Systemhärtung, mit denen Angriffsflächen durch sichere Konfigurationen und das Deaktivieren nicht benötigter Dienste reduziert werden. Zusätzlich sollten Überwachungssysteme wie ein Security Information and Event Management (SIEM) implementiert werden, um sicherheitsrelevante Ereignisse in Echtzeit zu analysieren und zu überwachen. Regelmäßige Updates und Sicherheitspatches sind ein weiterer entscheidender Bestandteil, um bekannte

Schwachstellen zu beseitigen. Auch der Umgang mit Sicherheitsvorfällen sollte in der Richtlinie klar definiert sein, um durchdacht und effektiv darauf reagieren zu können.

■ Netzwerksicherheit

Ein nicht zu unterschätzender Bereich ist die Sicherheit der Netzwerke sowie der Betriebssysteme und Datenbanken. Netzwerksicherheit umfasst Maßnahmen wie die Verwendung von Firewalls, die Einrichtung von VPNs und die Segmentierung von Netzwerken, um SAP-Systeme vor Bedrohungen von außen zu schützen. Betriebssysteme und Datenbanken, die die Basis der SAP-Systeme bilden, müssen ebenfalls abgesichert werden, um Manipulationen oder unbefugten Zugriff zu verhindern. Für die Integration von On-Premise- und Cloud-Systemen sind spezielle Sicherheitsanforderungen erforderlich, die eine sichere Interoperabilität gewährleisten.

Die Richtlinie sollte außerdem klare Vorgaben zur Governance und Organisation der SAP-Sicherheit enthalten. Dabei geht es um die Definition von Verantwortlichkeiten innerhalb der IT-Sicherheitsorganisation sowie um das Risikomanagement, das eine regelmäßige Bewertung und Minimierung potenzieller Risiken umfasst. Die Sicherheitsrichtlinie muss zudem an unternehmensspezifische Vorgaben und gesetzliche Anforderungen angepasst werden. Regelmäßige Audits und Sicherheitsprüfungen stellen sicher, dass Standards wie ISO 27001, die EU-Datenschutz-Grundverordnung (DSGVO) oder der Sarbanes-Oxley Act (SOX) eingehalten werden.

Governance und
Organisation

Abschließend sollten auch externe Dienstleister und Cloud-Anbieter berücksichtigt werden. Für Drittanbieter, die Netzwerke und Rechenzentren betreiben, müssen Sicherheitsanforderungen klar formuliert und durch entsprechende Vereinbarungen wie Service Level Agreements festgelegt werden. Bei der Zusammenarbeit mit großen Cloud-Anbietern wie Amazon Web Services (AWS), Azure oder Google Cloud sind strenge Sicherheitsvorkehrungen erforderlich, um den Schutz der Systeme und Daten zu gewährleisten.

Management von
Dritten und Soft-
warelieferanten

Eine solche Sicherheitsrichtlinie muss regelmäßig überprüft und an neue Bedrohungen angepasst werden, um den langfristigen Schutz der SAP-Systeme sicherzustellen. Sie bildet die Grundlage für eine widerstandsfähige IT-Infrastruktur, die den aktuellen und zukünftigen Herausforderungen gewachsen ist. Weitere Empfehlungen zur Implementierung einer solchen Sicherheitsstrategie in der eigenen Organisation erhalten Sie auch in Abschnitt 1.4, »Strategie für eine resiliente SAP-Sicherheitsorganisation«.

Dauerhafte
Anpassung und
Prüfung

Sie erkennen hier anhand von Beispieldaten, wie das Fortschreiben dieser sicherheitsrelevanten Einträge und deren Analyse in der SAP-Standardtransaktion abgebildet sind. Eine solche Übersicht wird immer wieder von SAP-Auditoren und -Revisoren oder zur Analyse der Ergebnisse von SAP-Penetrationstests verwendet. Denn viele Angriffsvektoren können eindeutig über Einträge im Security Audit Log identifiziert werden. Deshalb kommt diesem Log eine Schlüsselrolle bei SAP-Abwehrstrategien zu.

Ein Stolperstein auf dem Weg zu mehr SAP-Sicherheit ist allerdings die Datenschutzgesetzgebung (dieser Faktor spielt außerhalb Europas eine geringere Rolle). Man muss im Security Audit Log nämlich festlegen, welche Events und welche Benutzergruppen protokolliert werden sollen. Analysten und SIEM-Spezialisten werden sofort sagen, dass alle Events für alle Benutzer protokolliert werden müssen. Denn nur so kann man auch statistische Methoden und SIEM-Systeme verwenden, um verhaltensbasierte Auffälligkeiten und untypische Zugangsmuster zu erkennen. Dies widerspricht aber in vielen Einzelheiten den Auffassungen von Betriebsrat und Datenschutzverantwortlichen.

**Umfang des
Loggings festlegen**

Die Datenschutzkriterien müssen jeweils gegen das Ziel abgewogen werden, dass man mit dem Security Audit Log nicht einzelne Benutzer überwachen, sondern kriminelle Muster finden will. Hier muss eine eindeutige Festlegung getroffen werden, die persönlichen Schutz, Firmenbelange und Straftatbestände (die auch Betrug einschließen) gegeneinander abwägt. Obwohl am Nutzen einer kompletten Protokollierung in Zeiten von Angriffen organisierter Kriminalität, Staatsspionage und interner Sabotage kein Zweifel bleiben sollte, kann man als Kompromiss alle Events kritischer Benutzergruppen (System, Administratoren und SAP Power User) mitschreiben. Auch auf diese Weise lassen sich kritische Events und Muster schon gut isolieren.

Transaktion SM19 dient als Einstieg in die Konfiguration des Security Audit Logs (siehe Abbildung 2.3).

Der Security Audit Log muss bis Release SAP NetWeaver 7.1 manuell in den SAP-Profilen aktiviert werden, soweit dies nicht durch die Security-by-Default-Auslieferung bereits der Fall ist. Setzen Sie dazu den Profilparameter `rsau/enable` auf den Wert 1. Nach einem Neustart des Systems beginnt das SAP-System, die definierten Security Events zu protokollieren.

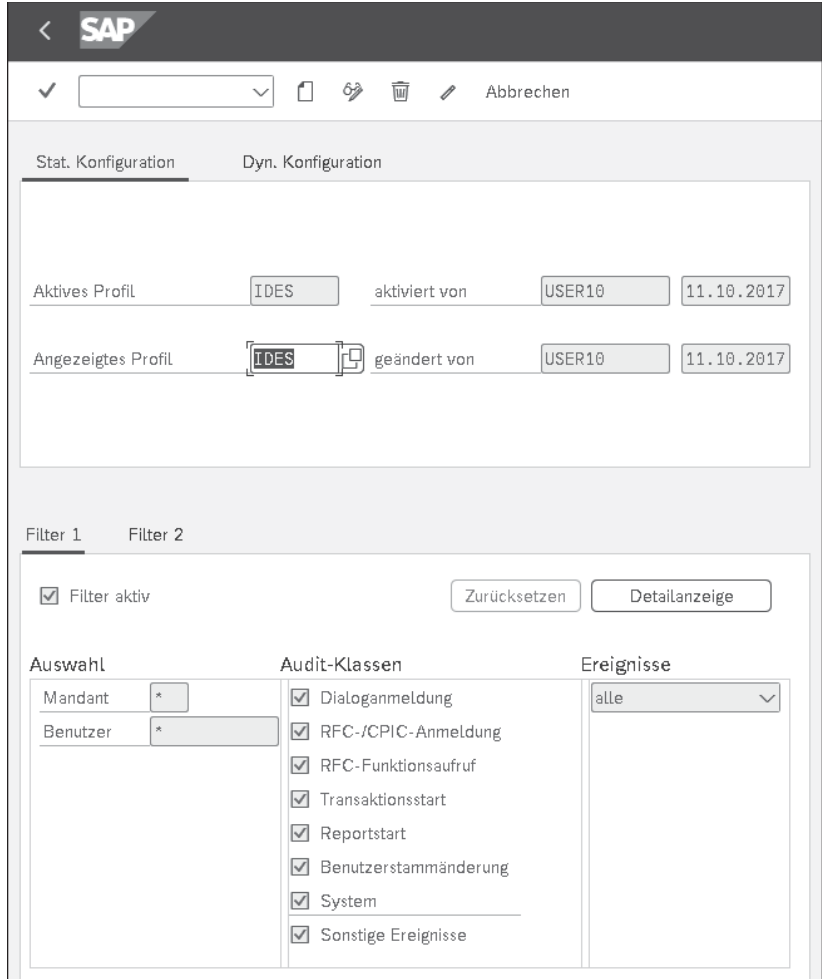


Abbildung 2.3 Konfiguration des Security Audit Logs

Wer wertet
das Security Audit
Log aus?

Der wohl kritischste Teil der Betrachtungen, wie ein Konzept zur SAP-Sicherheitsüberwachung mittels Security Audit Log umgesetzt werden kann, ist die Frage, wer diese Events in welcher Häufigkeit kontrolliert. Denn in einem einzigen System mit mehreren Hundert bis zu Tausenden von Benutzern tauchen auch Hunderte von Security Events auf, die von formellen Benachrichtigungen bis zu kritischen Events eingestuft werden. Selbst wenn man nur ein System manuell überwacht, hat der Sicherheitsbetreuer eines SAP-Systems mehrere Hundert Events pro Tag zu analysieren, zu bewerten, zu verfolgen und anschließend zu dokumentieren. Aber auch die Frage nach der Dauer der Aufbewahrung muss im Sinne von betrieblichen Belangen und EU-DSGVO geklärt werden.

In großen Firmen mit mehreren Tausend Benutzern gibt es dazu das *Security Operations Center (SOC)*. Hier sitzen konstant mehrere Mitarbeiter, meistens an SIEM-Konsolen wie Splunk, und hier laufen die meisten sicherheitsrelevanten Informationen zusammen, z. B. gespeist aus der E-Mail-Überwachung auf Trojaner und Malware oder der Überwachung von Server-Log-Dateien. Die Überwachung von SAP-Systemen ist noch eher selten Aufgabe der SOCs, aber der Security Audit Log wäre das erste und wichtigste Element für deren Integration.

Security Operations Center (SOC)

Wie für alle Lösungen gilt auch für das Security Audit Log: Ohne Personen, die sich explizit um die SAP-Sicherheit kümmern, gehen alle technischen Lösungen ins Leere. Dies sollte jedoch nicht dazu führen, das Security Audit Log gar nicht erst einzusetzen. Unserer Ansicht nach führt kein Weg an dessen Nutzung vorbei.

Sicherheitslösungen ersetzen kein Team

Die aktuelle Bedrohungslage nicht unterbewerten!

Wir möchten Ihnen ein aktuelles Beispiel für ein potenzielles Bedrohungsszenario aus unserer eigenen Arbeit geben: Zwischen dem 16. Dezember 2024 und Anfang Januar 2025 baten uns (als vergleichsweise »kleines« SAP-Sicherheitsunternehmen) zwei bestehende Kunden und drei neue Kunden um sofortige Hilfe, da alle ihre Server von Ransomware betroffen und verschlüsselt waren, einschließlich eines vollständigen Cloud-Rechenzentrums. Die Festplattenverschlüsselung wirkte sich als Kollateralschaden auf bis zu 180 SAP-Server aus. In einem Fall war auch das gesamte Backup durch Trojaner unbrauchbar gemacht worden.

Und auch die massive Verbreitung von Homeoffice und Remote Work ist ein sicherheitsrelevantes Thema. Denn interne Bedrohungen, etwa durch Mitarbeiterrechner an den Remote-Arbeitsplätzen, müssen verstärkt kontrolliert und überwacht werden. Es gibt heute mehr interne Angriffsvektoren als zu Zeiten, in denen noch alle im Büro arbeiteten.



Im Security Audit Log kann man sowohl den Übergang vom klassischen Netzwerk auf die SAP-Server sehen als auch Muster erkennen, wenn unerwartete Aktionen mit gestohlenen Passwörtern ausgeführt werden. Zusammen mit einer forensischen Analyse und einem SIEM-System wie SAP Enterprise Threat Detection lassen sich so Angriffsversuche aufdecken (weitere Informationen dazu erhalten Sie in Kapitel 19, »Erkennung von Angriffen, Abwehr und Forensik«). Mit einem aktiven Security Audit Log und einem zentralen SIEM-System hätte man im oben dargestellten Beispiel Auffälligkeiten festgestellt und den Schaden durch die Ransomware minimieren können. Ein SOC und die Log-Datei-Überwachung allein sind jedoch immer

noch passive Elemente, wenn sie nicht mit einem Zonenkonzept des Unternehmensnetzwerks korrespondieren, das Benutzergeräte und Clients separiert, aber auch Test- und Produktivsysteme trennt sowie ein spezielles Administrator-Netzwerk-Segment vorsieht. Nur so lässt sich im Ernstfall eine flächendeckende Verschlüsselung aller Systeme verhindern. Auf dem Security Audit Log setzen also die anderen, ebenso wichtigen Elemente (Netzwerktrennung, SIEM-Analyse, Security Operations Center) auf.

**Mindestmaßnahme:
direkte Auswertung
des Logs**

Denken Sie immer noch, dass es Ihr Unternehmen nicht treffen wird? Als Mindestmaßnahme empfehlen wir Ihnen, wenigstens damit zu beginnen, das Security Audit Log zu aktivieren und die Events zeitnah zu protokollieren. Außerdem sollten Sie wenigstens über eine Ressource im Unternehmen verfügen, die sich diese Logs ansieht.

2.6 SAP Enterprise Threat Detection

SAP Enterprise Threat Detection ist das SAP-Standardprodukt für den Bereich SIEM. Viele Unternehmen setzen jedoch bereits ein anderes SIEM-Produkt ein oder befinden sich in der Evaluationsphase, um eines auszuwählen. SAP hat SAP Enterprise Threat Detection entwickelt, um der internen SAP-Sicherheitsabteilung eine Lösung an die Hand zu geben, um auf der Anwendungsebene, basierend auf den Informationen aus den SAP-Protokolldateien, verdächtige Aktivitäten zu erkennen. Da bestehende Lösungen die spezifischen Anforderungen auf der SAP-Anwendungsebene nicht erfüllten, wurde ein neues Produkt entwickelt.

**Bedrohungserkennung
in Echtzeit**

SAP Enterprise Threat Detection ist ein leistungsstarkes Sicherheitswerkzeug, das speziell entwickelt wurde, um Bedrohungen innerhalb von SAP-Systemlandschaften in Echtzeit zu erkennen, zu analysieren und darauf zu reagieren. Die Lösung ermöglicht es Unternehmen, sicherheitsrelevante Aktivitäten und Anomalien in ihren SAP-Systemen zu überwachen und potenzielle Angriffe frühzeitig zu identifizieren. Dazu nutzt SAP Enterprise Threat Detection moderne Technologien wie Mustererkennung und maschinelles Lernen, um verdächtige Verhaltensweisen oder Angriffe innerhalb des Systems aufzudecken.

SAP Enterprise Threat Detection arbeitet mit einem zentralen Ansatz, indem es Log-Daten und sicherheitsrelevante Ereignisse aus den SAP-Systemen sammelt und analysiert. Die Software kann dabei große Datenmengen verarbeiten und ermöglicht Unternehmen, spezifische Angriffsmuster zu definieren. Diese Muster können bekannte Bedrohungen wie Brute-Force-

Angriffe, unerlaubte Berechtigungs eskalationen oder Datenexfiltration erkennen. Darüber hinaus bietet SAP Enterprise Threat Detection die Möglichkeit, Echtzeitbenachrichtigungen bei verdächtigen Aktivitäten zu generieren, sodass Sicherheitsvorfälle sofort untersucht und entsprechende Maßnahmen eingeleitet werden können.

Ein weiteres wichtiges Merkmal ist die Integration in bestehende Sicherheitsinfrastrukturen wie SIEM-Systeme anderer Anbieter. Dadurch können SAP-spezifische Sicherheitsdaten mit Informationen aus anderen IT-Systemen kombiniert werden, um eine ganzheitliche Sicherheitsstrategie zu ermöglichen. Die Datenmenge, die SAP-Protokolldateien erzeugen können (mehr als 1 Terabyte pro Tag), kann jedoch die Leistung und Lizenzanforderungen eines SIEM-Produkts erheblich beeinflussen. In Abschnitt 19.3, »Microsoft Sentinel als SIEM für SAP-Systeme«, stellen wir Sentinel als alternative Lösung vor, die ebenfalls gut mit den SAP-Systemen integriert ist.

Integration mit anderen SIEM-Systemen

SAP Enterprise Threat Detection sammelt Daten auf Anwendungsebene, indem es Informationen aus verschiedenen SAP-Protokolldateien (z. B. für SAP HANA, ABAP- und Java-Stack) verarbeitet. Das Security Audit Log dient als Informationsquelle für SAP Enterprise Threat Detection und wurde im vorangegangenen Abschnitt bereits vorgestellt.

Die Protokollüberwachung auf Anwendungsebene hat folgende Vorteile: Aktionen innerhalb von SAP-Anwendungen, wie Debugging, das Aufrufen kritischer Transaktionen, Berechtigungsänderungen oder das Herunterladen von Daten, sind auf der Infrastrukturebene nicht sichtbar. Metainformationen, wie die Position eines Mitarbeiters, sind ebenfalls auf dieser Ebene nicht verfügbar.

Protokollüberwachung auf der Anwendungsebene?

SAP Enterprise Threat Detection stellt, basierend auf Erkenntnissen von SAP-Kunden, -Partnern und Sicherheitsbehörden, regelmäßig neue Sicherheitsmuster bereit. Dies ermöglicht einen »virtuellen Patch«, um Schwachstellen zu schützen, auch wenn der Patch wegen möglicher Probleme nicht ausgeführt werden kann. »Virtuell« ist dieser Patch deshalb, weil man den eigentlich benötigten Patch nicht durchführen kann, aber zumindest einen Angriff erkennt, der diese Schwachstelle ausnutzt.

Aktualisierte Sicherheitsmuster

Hacker versuchen oft, ihre Spuren zu verwischen, indem sie Protokolleinträge löschen. SAP Enterprise Threat Detection speichert diese Informationen in Echtzeit an anderer Stelle, sodass sie weiterhin einsehbar bleiben, selbst wenn der Angreifer die Originaldaten entfernt.

Schutz vor der Löschung von Spuren

Die aktuelle Version von SAP Enterprise Threat Detection unterstützt Multi-Tenant-Cloud-Umgebungen und die Integration in die SAP BTP.

Cloud-Integration

2.7 SAP Code Vulnerability Analyzer: Schutz des kundeneigenen Codes

Sicherheitslücken im ABAP-Code

Ein wichtiger Bereich der SAP-Sicherheit, der erst in den letzten Jahren als solcher erkannt wurde, ist die Analyse der kundeneigenen SAP-Programme, die klassisch in der proprietären SAP-Sprache ABAP geschrieben werden. Auch hier können, wie in jeder Programmiersprache, klassische Sicherheitslücken programmiert werden – sei es nun bewusst oder unbewusst.

Besonderheiten von ABAP-Programmen

Allerdings sind die Muster hier deutlich anders gelagert als in einem Java-Stack oder einem Windows-Programm. Ziel bei herkömmlichen Schadprogrammen ist es meistens, durch gezielte Falscheingaben das Programm entweder zum Absturz zu bringen (*Buffer Overflow*) oder künstlich eigenen Code zur Ausführung zu bringen (*Code Injection*). Beides ist in einem ABAP-System nicht möglich, da ein Absturz eines Prozesses nichts anderes bewirkt als das Erzeugen eines Eintrags in der Log-Datenbank (Dump in Transaktion ST22) und ein Beenden des Programms mit Rückkehr an den Startpunkt des Menüs. Eine direkte Manipulation wie in anderen Hochsprachen oder Servern ist so also in ABAP nicht möglich. Allerdings gibt es andere Manipulationsmöglichkeiten.



Vergessener ABAP-Code

Immer mehr Angriffsvektoren auf SAP-Systeme haben mit ABAP-Code zu tun, der als Trojaner benutzt wird oder der schon für sich eine Gefahr darstellt. Bei einer unserer letzten Untersuchungen bei einem SAP-Kunden haben wir einen ABAP-Report in der Produktivumgebung gefunden, der kommentarlos alle FI-Tabellen löscht (*DROP TABLE-Anweisung*) – ohne Warnung. Ein unbeabsichtigtes Ausführen hätte desaströse Folgen gehabt. Es stellte sich heraus, dass dieser ABAP-Code bei der Ersteinführung des Kundensystems in den 1990er-Jahren benutzt wurde, um bei Fehlern in der initialen Beladung das System wieder zurückzusetzen. Er wurde danach vergessen und nie gelöscht.

Kundeneigene Programme prüfen

Es gibt Werkzeuge wie den *SAP Code Vulnerability Analyzer*, mit denen sich alle kundeneigenen Programme in einem Massenverfahren analysieren lassen. Die daraus gewonnenen Ergebnisse und Erkenntnisse müssen dann in ein Projekt zur Beseitigung der Schwachstellen (*Get Clean*) und anschließend in ein Projekt zur zukünftigen Sicherstellung einer sicheren ABAP-Programmierung (*Stay Clean*) überführt werden.

2.7.1 Get Clean: vorhandenen ABAP-Code prüfen

Die Phase *Get Clean* ist der Ausgangspunkt eines Code-Sicherheitsprojekts und hat das Ziel, vorhandenen benutzerdefinierten SAP-Code (z. B. in ABAP oder SAP HANA SQL) auf Sicherheitsrisiken hin zu überprüfen und diese zu beseitigen. Der Fokus liegt dabei darauf, die bestehende Codebasis systematisch zu analysieren, Schwachstellen zu identifizieren und zu beseitigen.

Der SAP Code Vulnerability Analyzer scannt den gesamten benutzerdefinierten Code auf bekannte Schwachstellen wie SQL Injection, Cross-Site Scripting (XSS), Hardcoded Credentials und andere potenzielle Risiken. Eine Priorisierung der gefundenen Schwachstellen erfolgt basierend auf ihrer Kritikalität.

Initiale Sicherheitsanalyse

Die identifizierten Probleme werden durch Entwicklerteams gelöst. Dabei müssen bewährte Methoden und Sicherheitsstandards wie die von OWASP definierten Standards berücksichtigt werden (siehe Abschnitt 2.4.1, »SAP und die OWASP Top 10«). Falls nötig, werden Sicherheitspatches eingespielt, oder es wird ein Code Refactoring durchgeführt.

Beseitigung von Schwachstellen

Entwickler und Teams werden geschult, um ein besseres Verständnis für Sicherheitsprobleme im Code zu entwickeln. Ziel ist es, zukünftige Fehler zu vermeiden. Am Ende dieser Phase wird ein dokumentierter Sicherheitsstandard definiert, der die Anforderungen an die Codequalität und Sicherheitschecks beschreibt.

Sensibilisierung und Schulung

Der Abschluss der Phase *Get Clean* markiert den Punkt, an dem der vorhandene Code frei von bekannten Schwachstellen ist, und damit die Grundlage für die nächste Phase gelegt wurde.

2.7.2 Stay Clean: Sicherheitsrichtlinien für die ABAP-Programmierung

Nach der Bereinigung des bestehenden Codes liegt der Fokus in der Phase *Stay Clean* darauf, kontinuierlich sicherzustellen, dass neu erstellter oder geänderter Code den festgelegten Sicherheitsstandards entspricht. Ziel ist es, Sicherheitsrisiken frühzeitig zu erkennen und die Codequalität langfristig zu sichern.

Neue oder geänderte Codes werden automatisch durch den SAP Code Vulnerability Analyzer geprüft, bevor sie in produktive Systeme integriert werden. Diese Scans können in Entwicklungs- und Testumgebungen erfolgen.

Kontinuierliche Codescans

Sicherheitsprüfungen werden als fester Bestandteil der Entwicklungs- und Freigabeprozesse etabliert (z. B. im Rahmen von Continuous Integration/Continuous Delivery Pipelines). Entwickler erhalten so unmittelbar während der Codierung Feedback zu potenziellen Schwachstellen.

Sicherheitsprüfungen im Entwicklungsprozess

Regelmäßige Updates und Wartung

Sicherheitsrichtlinien und die Regeln für den SAP Code Vulnerability Analyzer werden regelmäßig aktualisiert, um auf neue Bedrohungen und Schwachstellen reagieren zu können. Die Einhaltung der Sicherheitsrichtlinien wird durch regelmäßige Audits und Berichte überprüft. Um sicherzustellen, dass das Sicherheitsbewusstsein ein integraler Bestandteil der Unternehmenskultur bleibt, werden regelmäßige Schulungen und Workshops für Entwickler durchgeführt.

Berichtswesen und Monitoring

Automatisierte Berichte und Dashboards liefern eine Übersicht über die Sicherheitslage der Codebasis und ermöglichen ein effektives Monitoring.

2.8 Das neue SAP Security Dashboard

Reaktion auf wachsende Anforderungen

Das *SAP Security Dashboard* sollte sich in den letzten Jahren zu einem zentralen Instrument entwickeln, um die Sicherheitsanforderungen moderner SAP-Systeme zu überwachen und zu verwalten. Doch die Entwicklung dieses Dashboards ging langsamer und schleppender voran als geplant. Ursprünglich als Reaktion auf die wachsenden Anforderungen von SAP-Kunden und der Deutschsprachigen SAP-Anwendergruppe (DSAG) konzipiert, sollte es eine umfassende Übersicht über sicherheitsrelevante Ereignisse, Risiken und Compliance-Status bieten. Die zunehmende Komplexität von IT-Landschaften und die Verschärfung gesetzlicher Vorgaben, insbesondere im Bereich Datenschutz und Datensicherheit, haben dazu geführt, dass die Anforderungen an ein SAP Security Dashboard stetig wuchsen, aber außer einigen Konzeptstudien und Fallbeispielen kein einsetzbares Produkt entstanden ist. Unternehmen erwarten heute nicht nur die Erkennung und Meldung von Sicherheitsvorfällen, sondern auch präventive Analysen und Handlungsempfehlungen, um potenzielle Risiken bereits im Vorfeld zu minimieren.

Dashboard in SAP Analytics Cloud und SAP Cloud ALM

Inzwischen hat SAP das Konzept der Implementierung erweitert und sieht die Zukunft des SAP Security Dashboards in der *SAP Analytics Cloud* und dem Application Lifecycle Management von *SAP Cloud ALM*. Vor diesem Hintergrund ist es ein positiver Schritt, dass SAP plant, ein spezielles Security-Dashboard für die SAP Analytics Cloud bereitzustellen, das sich insbesondere an mittelständische Kunden richtet. Dieses Dashboard wird parallel zu den Schnittstellen (APIs) und entsprechenden Partnerlösungen verfügbar gemacht, um eine umfassende Sicherheitsabdeckung zu gewährleisten.

Einschätzung der DSAG

»Damit erfüllt SAP eine langjährige Forderung der DSAG und unterstützt insbesondere Kunden, die über keine umfassende Monitoring-Infrastruktur

tur verfügen«, erklärte der Fachvorstand Technologie der DSAG, Sebastian Westphal auf den DSAG-Technologietagen 2024. »Trotz dieser positiven Entwicklung besteht weiterhin Klärungsbedarf hinsichtlich der Bereitstellung von Security-Tools des Solution Managers über das Jahr 2027 hinaus. Erste Signale deuten darauf hin, dass wesentliche Funktionalitäten wie die Konfigurationsvalidierung zur Konsistenzprüfung von Systemen und die System Recommendations künftig in SAP Cloud ALM integriert werden könnten. Dies stellt einen wichtigen Schritt dar, um die Sicherheitsanforderungen moderner SAP-Umgebungen langfristig zu erfüllen.« Eine gute Quelle, um über aktuelle Entwicklungen im Bereich der SAP-Sicherheitsprodukte informiert zu werden, ist die Themenseite »Security« in der SAP Community (<https://pages.community.sap.com/topics/security>, siehe auch Abschnitt 2.10.3, »Empfehlungen der SAP Community«).

2.9 SAP Cloud ALM für das Security Monitoring

SAP Cloud ALM ermöglicht eine zentralisierte Echtzeitüberwachung der gesamten SAP-Landschaft, unabhängig davon, ob diese als On-Premise-System, in der Cloud oder in hybriden Umgebungen betrieben wird. Die Lösung bietet eine umfassende Übersicht über alle Systemkomponenten, Anwendungen, Benutzeraktivitäten und Schnittstellen. Die Plattform verwendet integrierte Dashboards, die sicherheitsrelevante Metriken und Ereignisse visualisieren, wie z. B. fehlerhafte Anmeldungen, ungewöhnliche Datenzugriffe oder verdächtige API-Aufrufe. Durch die Bereitstellung zentralisierter Monitoring-Tools wird die Transparenz der Sicherheitslage erhöht, und potenzielle Schwachstellen können schneller identifiziert werden. Dies ist besonders wichtig in komplexen, verteilten Architekturen, in denen Sicherheitsvorfälle schwer zu erkennen sind.

Kostenlose Demoversion

Möchten Sie sich mit den Möglichkeiten von SAP Cloud ALM vertraut machen, können Sie eine kostenlose und frei nutzbare Demoanwendung verwenden: <http://s-prs.de/v1052600>



Über die Webseite, die in Abbildung 2.4 zu sehen ist, gelangen Sie zur Demoversion von SAP Cloud ALM. Die Betriebsplattform basiert auf der SAP BTP und kann sowohl von SAP als auch von den SAP-Kunden für den Betrieb der SAP-Lösungen genutzt werden. Sie wurde entwickelt, um hybride Landschaften zu unterstützen und dabei eine nahtlose Verwaltung und Überwachung von SAP-Lösungen zu ermöglichen.

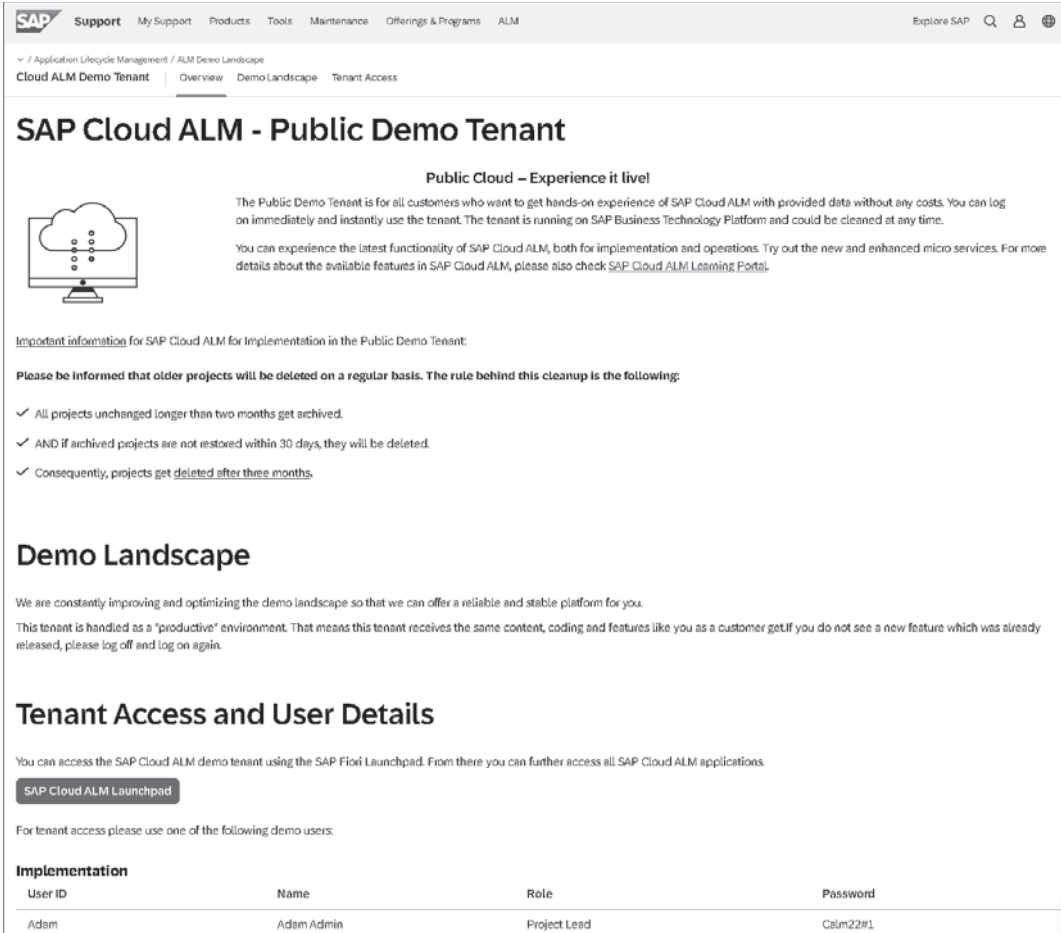


Abbildung 2.4 Webseite zur Demoversion von SAP Cloud ALM

Im Mai 2020 kündigte SAP eine Reihe von Updates an, die den Funktionsumfang von SAP Cloud ALM erweitern und die Implementierung sowie den laufenden Betrieb vereinfachen sollten. Diese Verbesserungen tragen dazu bei, Kunden den Übergang in die Cloud zu erleichtern. Mit diesen Aktualisierungen unterstützt SAP Cloud ALM nun SAP-Lösungen wie SAP S/4HANA Cloud, SAP SuccessFactors, SAP Customer Experience und SAP Ariba. Diese Funktionen helfen Kunden, ihre Anforderungen an Cloud-Lösungen zu verwalten und den Fortschritt ihrer Projekte zu überwachen. Besonders nützlich sind die bereitgestellten Workshops, etwa im Bereich Onboarding oder Fit-to-Standard, die den Implementierungsprozess begleiten und automatisierte Statusmeldungen zum Projektfortschritt liefern.

Typischerweise sucht man im Rahmen des Sicherheits-Monitorings in einer SAP-Landschaft nach kritischen Ereignissen. SAP Cloud ALM bietet dazu vielfältige Möglichkeiten. Allerdings richtet sich diese Lösung eher an Administratoren als an Sicherheitsanalysten. Trotzdem lassen sich viele benötigte Informationen und Logs auch über SAP Cloud ALM finden, und bei Bedarf kann man sich eigene Dashboards mit den benötigten Informationen zusammenstellen. In der Demoverision von SAP Cloud ALM erhalten Sie einige Einblicke in das *Security Event Management* mit dieser Lösung.

Security Event Management

Sie erreichen die in diesem Bereich bereitgestellten Dashboards (siehe Abbildung 2.5) mit entsprechenden Berechtigungen im Launchpad über den Pfad **Operations • Integration & Exception Monitoring**. Hier haben Sie einen Überblick über alle Systeme in Ihrer Landschaft. Die Security Events werden nach Kritikalität sortiert.

Integration and Exception Monitoring

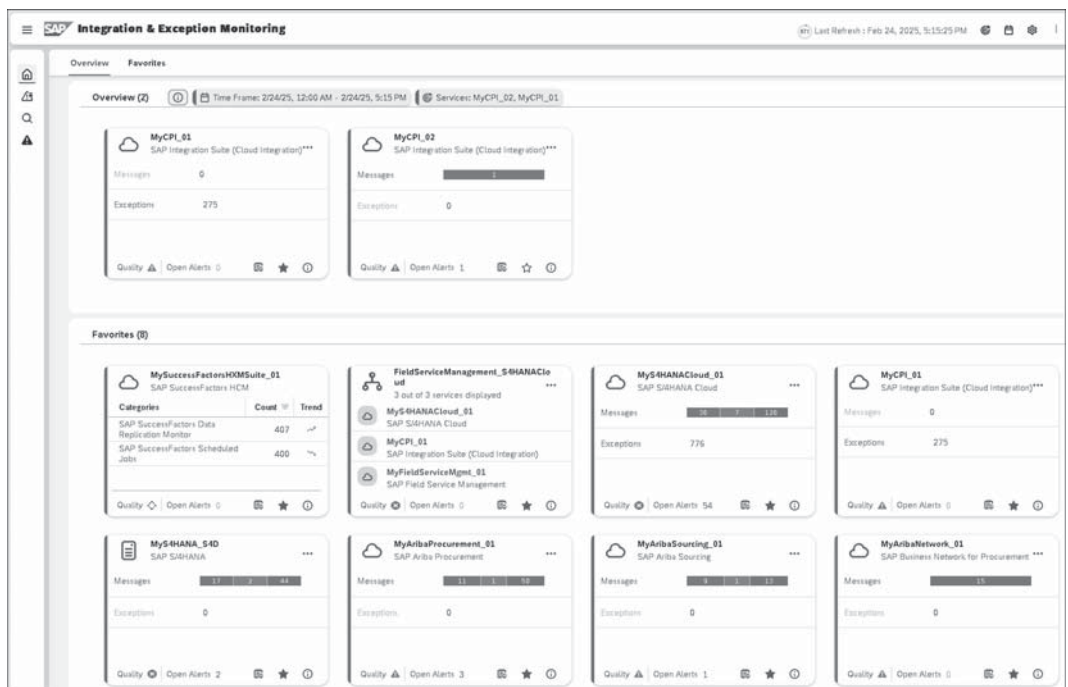


Abbildung 2.5 Dashboards im Bereich »Integration & Exception Monitoring« in SAP Cloud ALM (Quelle: Demoverision)

Rufen Sie die Details zu einem System auf, gelangen Sie zu einem Dashboard, wie es Abbildung 2.6 zeigt. Hier werden die einzelnen Alerts grafisch aufbereitet und tabellarisch angezeigt.

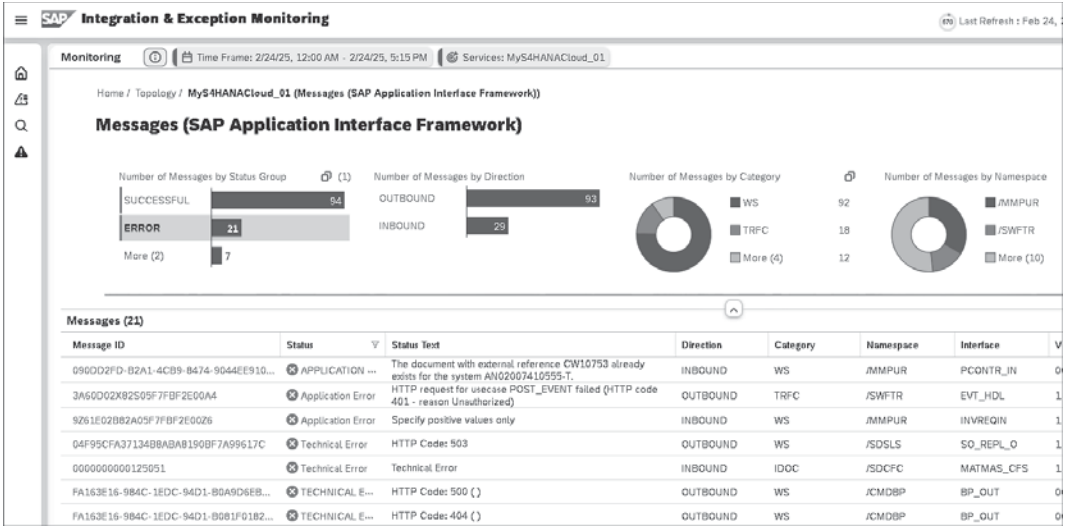


Abbildung 2.6 Alerts zu den Security Events eines Systems in SAP Cloud ALM (Quelle: Demoversion)

Details zu einem Security Event

Sehen wir uns als Beispiel einen Alert zu einem HTTP Return Code 404 an, der auf einen Fehler in der HTTP-Kommunikation hindeutet, was aus Security-Sicht Ihr Interesse wecken sollte. Abbildung 2.7 zeigt die detaillierte Sicht auf einen einzelnen Fehler. Diese Sicht ist ein guter Ausgangspunkt für weitere Nachforschungen über die Administrationstools von SAP Cloud ALM.

Weitere ALM-Lösungen von SAP

Neben SAP Cloud ALM bietet SAP verschiedene weitere ALM-Lösungen, die je nach Kundenanforderungen und IT-Landschaft unterschiedlich eingesetzt werden:

- **SAP Solution Manager**

Eine vollständig integrierte ALM-Suite, ideal für größere Kunden mit überwiegend On-Premise-Landschaften und einem stabilen Funktionsumfang.

- **SAP Focused Run**

Eine Plattform für High-End-Kunden und Service Provider, die über die Funktionen des SAP Solution Managers und von SAP Cloud ALM hinausgehende Anforderungen haben.

SAP Cloud ALM wird dagegen als cloud-basierte ALM-Lösung für Unternehmen jeder Größe positioniert, die besonders für hybride Landschaften mit Fokus auf den cloud-basierten Betrieb geeignet ist. Da der Support für den SAP Solution Manager im Jahr 2027 endet, stehen Unternehmen vor der Herausforderung, Alternativen zu finden. SAP empfiehlt eine schrittweise Um-

stellung auf SAP Cloud ALM oder, für anspruchsvollere Umgebungen, auf SAP Focused Run. Bei der Auswahl der passenden Lösung sollten IT-Strategie, bestehende Infrastruktur und Kosten sorgfältig abgewogen werden.

The screenshot displays the SAP Integration & Exception Monitoring interface. The main heading is 'Monitoring' with a sub-heading 'FA163E16-984C-1EDC-94D1-B081F01823DC'. The interface is divided into several sections:

- Status Details:**
 - Status: TECHNICAL ERROR
 - Status Text: HTTP Code: 404 ()
 - Direction: OUTBOUND
 - Start Time: Feb 24, 2025, 4:58:26 PM
 - End Time: Feb 24, 2025, 4:58:26 PM
 - Processing Time (in milliseconds): 0
 - Local Monitoring: [Icon]
 - Technical Correlation: [Icon]
- Application Data:**
 - AIF Interface name: BP_OUT
 - AIF Interface version: 00001
 - AIF Namespace: /CMDBP
 - Category: WS
 - Location Consumer / Provider: C
 - Message id: FA163E16-984C-1EDC-94D1-B081F01823DC
 - Message Monitoring: https://my301149.s4hana.ondemand.com:443/sap/bc/ui2/tp?sa...
 - Sender Interface Name: BusinessPartner:SUITEBjkkReplicateRequest_Out
 - Sender Namespace: http://sap.com/b2/SAP_BS_FND/MDG/Global2
- LogMessage (1):**

Package	Sequence No.	Parameter	STATUS	MESSAGE	MESSAGE_CLASS
	1	LogMessage	ERROR	HTTP Code: 404 ()	/AIFMES

Abbildung 2.7 Detailansicht eines Security Events in SAP Cloud ALM (Quelle: Demoversion)

2.10 Die wichtigsten SAP-Sicherheitsrichtlinien

In diesem Abschnitt sehen wir uns abschließend einige wichtige SAP-Richtlinien zum Thema Sicherheit an.

2.10.1 SAP Security Baseline

Eine *Security Baseline* für SAP stellt die Mindestsicherheitsanforderungen dar, die in Ihrer Organisation für alle SAP-Systeme verbindlich gelten sollten. Diese Baseline bildet den Sicherheitsrahmen, der unabhängig von spezifischen Risikobewertungen für alle Systeme einheitlich angewandt wird. Sie dient als universelle Richtlinie, um eine solide Sicherheitsgrundlage zu

Grundlage für
eine sichere
SAP-Landschaft

schaffen, und gilt systemübergreifend – unabhängig von der Kritikalität oder dem Zweck eines Systems.

SAP hat alle relevanten Information in SAP-Hinweis 2253549 (SAP Security Baseline Template) zusammengefasst. Das Konzept einer *Baseline* ist hier entscheidend: Alle SAP-Systeme müssen diese Vorgaben erfüllen, unabhängig von ihrer individuellen Sicherheitsstufe. Die Baseline basiert auf bewährten Best Practices und stellt sicher, dass grundlegende Sicherheitsmaßnahmen überall implementiert sind. Doch es ist ebenso wichtig, Systeme zu identifizieren, die aufgrund ihrer besonderen Kritikalität oder Nutzung einer zusätzlichen, spezifischen Risikoanalyse bedürfen. Für solche Systeme werden individuelle Maßnahmen entwickelt und implementiert, die über die Vorgaben der Baseline hinausgehen.

Erstellung und
Implementierung
der SAP Security
Baseline

Der Prozess zur Erstellung einer SAP Security Baseline beginnt mit der Konsolidierung der oben genannten Quellen. Mithilfe von SAP-Sicherheitservices wie dem *SAP Security Optimization Service* oder dem Sicherheitskapitel des *SAP EarlyWatch Alerts* wird zunächst eine Analyse beispielhafter Systeme durchgeführt. Diese Analysen vergleichen den aktuellen Systemstatus mit den Empfehlungen von SAP, um allgemeine Anforderungen abzuleiten, die für alle SAP-Systeme gelten.

Zusätzlich werden spezifische Anforderungen aus internen Quellen wie allgemeinen Sicherheitsrichtlinien oder maßgeblichen Entscheidungen integriert. Daraus entsteht eine unternehmensspezifische SAP Security Baseline, die sowohl SAP-Standards als auch individuelle Sicherheitsanforderungen abdeckt.

SAP stellt eine Vorlage für eine solche Security Baseline bereit. Wie Sie auf deren Basis Ihre eigene Baseline entwickeln und welche Bereiche Sie dabei berücksichtigen sollten, erfahren Sie in Abschnitt 18.2.1, »Security Baseline als Grundlage für eigene Sicherheitsrichtlinien«.

2.10.2 SAP-Empfehlungen für Sicherheitsdienste

SAP bietet eine Vielzahl von Sicherheitservices und Tools an, wie das Sicherheitskapitel des *SAP EarlyWatch Alerts*, den *SAP Security Optimization Service* oder spezifische SAP-Hinweise (z. B. Hinweis 863362). Diese Ressourcen liefern konkrete Vorschläge zur Absicherung von SAP-Systemen und dienen als Grundlage für eine robuste Baseline.

SAP-Doku-
mentation

Produktspezifische Sicherheitsleitfäden, die auf help.sap.com bereitgestellt werden, bieten detaillierte Anleitungen zur sicheren Konfiguration von

SAP-Produkten. Die auf der Webseite <http://s-prs.de/v1052601> dargestellten Security Whitepapers und Sicherheitshinweise von SAP (siehe Abbildung 2.8) liefern regelmäßige Updates und Best Practices zu neuen Sicherheitsanforderungen und -features.

Security Whitepapers

To increase the security of your SAP systems, SAP provides you with *Security Whitepapers*. The objective of this series is to give you concise, easy-to-understand and easy-to-implement information on how to improve the security of your IT systems. The series covers various aspects of security including recommendations for system configuration as well as guidance and support for the implementation of SAP security fixes.

Search:

Title	Description	Download	Date	Language
SAP Business Technology Platform in GxP	Discover how SAP helps enterprises in the life sciences industry address the challenges of integrating and extending processes while paying careful attention to industry and government regulations. Find out how SAP Business Technology Platform and its built-in services can help you create 21st-century applications.	PDF	2024-06	English
The Secure Software Development Lifecycle at SAP	Learn how SAP has implemented a secure software development lifecycle (secure SDL) for software development projects. Discover how secure SDL provides a framework for training, tools, and processes.	Link	2020-09	English
SAP's Standards, Processes, and Guidelines for Protecting Data and Information	This document describes how SAP helps to ensure that the software systems, information, and data of its customers are fully protected.	PDF	2016-08	English
Managing Security with SAP Solution Manager	Explore the various aspects of building, setting up, and operating a secure system landscape and the ways in which SAP Solution Manager supports these tasks as an IT services and operations management tool.	PDF	2015-06	English
SAP Security Recommendations: Securing Remote Function Calls (RFC)	SAP reviewed and improved the security controls used by Remote Function Calls (RFC). RFC is an SAP-proprietary communication protocol. Most SAP customers run business-critical system communication using RFC technology. Keeping business data that is processed via RFC secure is as important to SAP and its customers as ensuring uninterrupted business operations.	PDF	2023-03	English

Abbildung 2.8 Security Whitepaper von SAP

2.10.3 Empfehlungen der SAP Community

Es gibt darüber hinaus eine aktive SAP Community zum Thema SAP-Sicherheit. Diese tauscht sich auf der Themenseite »Security« in der SAP Community z. B. über Blogs und die zugehörigen Diskussionen aus (siehe <https://pages.community.sap.com/topics/security> und Abbildung 2.9).

Die neue SAP Community ist der Nachfolger des alten SAP Developer Networks. Hier werden alle Beiträge zu Sicherheitsthemen rund um SAP aus der SAP Community gesammelt und aufbereitet.

In diesem Kapitel haben wir die wichtigsten Elemente einer SAP-Sicherheitsstrategie aus der Sicht von SAP abgebildet. Neben den Sicherheitslösungen ist es vor allem die inzwischen sehr umfangreiche Sammlung von Richtlinien, Whitepapers und Webbeiträgen zum Thema SAP-Sicherheit,

die es erlaubt, eine umfangreiche Sicherheitsstrategie innerhalb des SAP-Ökosystems aufzubauen. In den folgenden Kapiteln greifen wir immer wieder einzelne Lösungen und Empfehlungen aus der hier vorgestellten Übersicht auf.

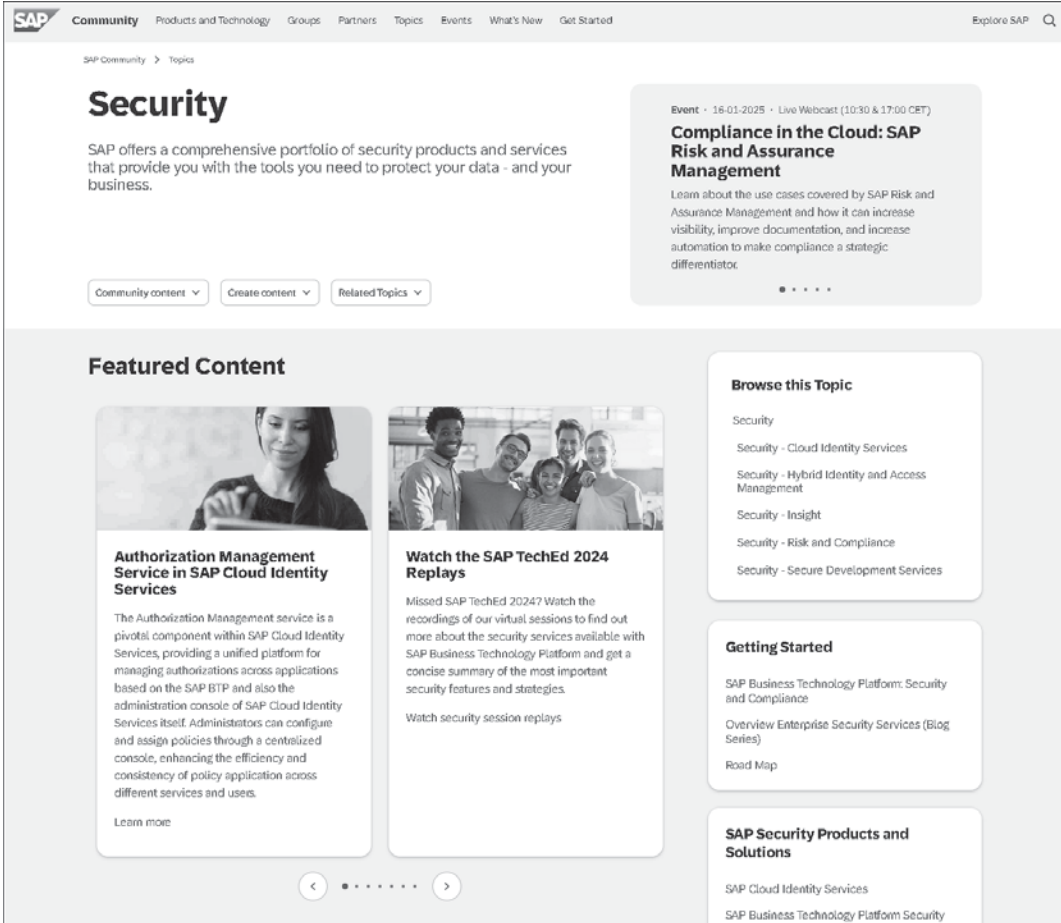


Abbildung 2.9 Themenseite »Security« der SAP Community

Kapitel 3

Wie kommen Hacker an die erforderlichen Informationen?

Dieses Kapitel soll Ihnen verdeutlichen, wie einfach es ist, Informationen zu Sicherheitslücken und Hacking im SAP-Umfeld im Internet zu finden.

Der Vorgang des Hackings hat für viele noch etwas Ehrfurchtgebietendes. Man hat einen technisch extrem versierten Nerd vor Augen, der in einem dunklen Keller sitzt, umringt von vielen Monitoren, auf denen etliche Kommandozeilenfenster geöffnet sind. Und in der Praxis? Dort ist für das Eindringen in Systeme von außen zwar natürlich umfangreiches technisches Know-how erforderlich, was auch für das Hacking von SAP-Systemen gilt. Allerdings handelt es sich bei einem großen Teil dieses Know-hows nicht um Insider-Wissen, ganz im Gegenteil: Es ist frei im Internet verfügbar. Die meisten Betrugsdelikte erfolgen auch nicht, wie man meinen könnte, durch organisierte Kriminalität, sondern gehen von Privatpersonen sowie von aktuellen und ehemaligen Mitarbeitern aus. Einer der Gründe dafür ist, dass das Know-how für fast jegliche Art von Betrug frei im Internet verfügbar ist. Die Hürde zum Hacking von SAP-Systemen (bzw. grundsätzlich aller IT-Systeme) liegt daher nicht mehr in erster Linie bei der technischen Durchführung.

In diesem Kapitel erfahren Sie, wie Sie die benötigten Informationen mit einfachen Mitteln finden können. Mit den richtigen Suchbegriffen erhalten Sie alle Informationen, die zum Hacking von SAP-Systemen erforderlich sind. Dazu gehen wir in Abschnitt 3.1 zunächst auf Internetsuchmaschinen und -foren als Informationsquelle ein. In Abschnitt 3.2 stellen wir Ihnen die Nutzung von Künstlicher Intelligenz (KI) als aktuellen Gamechanger vor. Dieses Kapitel soll vor allem dazu dienen, Ihnen aufzeigen, dass SAP-Systeme auch ohne umfangreiches Insider-Wissen angegriffen werden können. Diese Erkenntnis ist die beste Voraussetzung, um Ihre SAP-Systeme effektiv und effizient abzusichern.

Aufbau dieses Kapitels