Sicherheitsstrategie in der S/4HANA-Transformation

Nicht die Augen verschließen, sondern mutig anfangen

Eine von der SAP abgekündigte IT-Architektur durch SAP S/4HANA zu ersetzen ist das eine. Das Projekt in einem tragfähigen Security-by-Default-Konzept abzubilden, das andere. Die Vorgehensweise und die Umsetzung bei thyssenkrupp Materials Services brachte wichtige Erkenntnisse hervor.

Thomas Kircher, blaupause-Redaktion

Die SAP-Systemlandschaft von thyssenkrupp Materials Services, einem der größten werksunabhängigen Werkstoffhändler und -dienstleister weltweit, soll erneuert werden. Historisch gewachsen, war das System durch viele kundenspezifische Anpassungen komplex geworden, zudem wird SAP 2027 die Wartung einstellen. So wurde beschlossen, SAP S/4HANA einzuführen, um die Unternehmens-Software zu modernisieren, Innovationen nutzen zu können, die Komplexität zu verringern sowie agiler und flexibler zu werden. „Das Ziel ist eine modernisierte, skalierbare IT-Architektur mit einem ‚Clean Core', um das System standardisieren, End-to-End-Prozesse entwickeln und aktuelle Anforderungen der SAP-Sicherheit direkt umsetzen zu können", beschreibt Dr. Alexander Ziesemer, SAP-Security-Manager bei der thyssenkrupp Materials Services und Sprecher des DSAG-Arbeitskreises Security & Vulnerability Management, die Ausgangslage.

Governance-Strategie zwingend erforderlich

Bei einem S/4HANA-Projekt wie das von thyssenkrupp Materials Services ist eine Governance-Strategie für das Gesamtkonstrukt und für die eingesetzte Business Technology Platform (BTP) mit ihren Vorschriften und Richtlinien zwingend erforderlich. Wichtig bei der Security-Governance ist u. a., dass der Chief Information Security Officer (CISO) und der Chief Information Officer (CIO) bezüglich der SAP-Sicherheit an einem Strang ziehen. „Es ist essenziell, dass der CISO die Sprache des SAP-Umfelds und damit auch die SAP-Security versteht. Eine enge Zusammenarbeit zwischen SAP Operations, dem CISO und der SAP-Security ist daher ein wichtiger Baustein für ein erfolgreiches Projekt", fasst Dr. Alexander Ziesemer zusammen.

Sicherheitsstandard sehr hoch angesetzt

Bei thyssenkrupp Materials Services lässt sich die Sicherheitsstrategie für S/4HANA ganz pragmatisch zusammenfassen: „Idealerweise beginnt ein neues Transformationsprojekt mit Start Secure, bei bestehenden Systemen ist Get Secure das Ziel, und die Daueraufgabe ist Stay Secure", berichtet der SAP-Security-Manager. Start Secure bedeutet z. B., die Sicherheitsvorgaben mit allen Projektbeteiligten zu Beginn zu definieren sowie die technischen Designs und die Implementierung zu überprüfen. Das soll sicherstellen, dass sich alle Beteiligten an die Vorgaben halten. Dementsprechend wurden die Entwickler:innen beim Werkstoffhändler und -dienstleister zum Thema sichere SAP-Entwicklung geschult, um mit diesem Schritt „unsichere" Entwicklungen von Anfang an zu verhindern.

Mit dem Security-by-Default-Konzept wurde der allgemein gültige Standard in puncto Sicherheit bewusst sehr hoch angesetzt. „Wir haben auf unsere bestehende SAP-Sicherheitsrichtlinie aufgesetzt, die auf der SAP Secure Operations Map (siehe Glossar Seite 42) beruht. Darauf aufbauend wurde unser SAP-Security-Konzept erarbeitet", erläutert Dr. Alexander Ziesemer. Im Zuge von Security-by-Default hatte SAP zwar einige Sicherheitseinstellungen mit ausgeliefert, nach dem Systemaufbau mussten jedoch noch weitere Einstellungen angepasst werden, z. B. die Konfiguration gemäß SAP-Baseline, die UCON-Funktion sowie Secure-Network-Communications (SNC) und HTTPS-by-Default (siehe Glossar Seite 42). „Hier muss SAP den Security-by-Default-Ansatz mit einer deutlich umfangreicheren Basisfunktionalität ausstatten", kommentiert der SAP-Security-Manager.

Ohne Governance keine Verantwortlichen

Die Umsetzung einer Sicherheitsstrategie muss auf allen Ebenen der Organisation ansetzen und greifen. Von der Architektur und Konzeption über das operative Team mit Entwickler:innen und Supporter:innen bis hin zum Management durch konkrete Key Performance Indica-

thyssenkrupp Materials Services GmbH

thyssenkrupp Materials Services ist mit rund **380 Standorten** – davon ca. 270 Lagerstandorte – in mehr als **30 Ländern** einer der **weltweit führenden** werksunabhängigen Werkstoffhändler und -dienstleister. Im **Geschäftsjahr 2022/23** hat das Unternehmen einen **Umsatz von 13,6 Mrd. Euro** und ein Ergebnis von 178 Mio. Euro erwirtschaftet.

thyssenkrupp-materials-services.com

Key-Design-Prinzipien für SAP-Security

- Security- und Privacy-by-Design-and-Default
- Einhaltung der thyssenkrupp-Policies und internationaler Standards
- Sichere Parametereinstellungen im thyssenkrupp-Materials-Baseline-Template erarbeiten
- Sichere Code-Entwicklung gewährleisten
- Verschlüsselung von Anfang an aktivieren und umsetzen
- Sichere Schnittstellen definieren
- Zero-Trust-Ansatz verfolgen
- Transparenz, Change-Management und Awareness für SAP-Security immer berücksichtigen und Zeit dafür einplanen

tors, inklusive eines umfassenden Reporting. Dafür sind Prozessbeschreibung, Dokumentation und Change-Management essenziell. „Für die erste Projektphase war es wichtig, sich bereits im Vorfeld kritisch mit bestehenden Sicherheitsproblemen auseinanderzusetzen und daraus folgend neue aktualisierte Sicherheitsvorgaben zu definieren, um diese dann im System gleich von Beginn an richtig aufgesetzt zu haben", so Dr. Alexander Ziesemer.

Entscheidend war auch, die Risiken im Hinblick auf die Cloud-Technologie, und damit konkret die BTP-Services, sowie die Verantwortlichkeiten zu erarbeiten und diese entsprechend zu etablieren. „Cloud-Anwendungen können mitunter leicht dazu verführen, einfach mal einen Service zu buchen, ihn an die vorhandene Umgebung anzubinden und loszulegen. Das macht dann eine sichere Integration in die vorhandene IT-Landschaft sehr schwer", berichtet Alexander Ziesemer. Darum muss die BTP den gleichen Governance-Vorgaben wie im Backend unterworfen werden: z. B. der architektonischen Betrachtung, den Change-Incident- und Betriebsprozessen und klaren Verantwortlichkeiten.

Security- und Privacy-by-Default waren von Anfang an gesetzt

Die notwendige Evaluierung der Security-Recommendations (siehe Kasten) war ebenfalls Team-Arbeit, bei der Vertreter:innen aus den Bereichen Entwicklung, Integration, Security und Business mitwirkten. Die Entwickler:innen z. B. benötigen Trainings für sicheres Programmieren mit leicht verständlichen Hinweisen. Bei der Integration sind dann Key-Design-Principles festzulegen, wie z. B. konsequent verschlüsseltes Arbeiten, die Umsetzung der Datenschutz-Grundverordnung (DSGVO), eine risikobasierte Authentifizierung sowie der Ver-

→

„Bei einem S/4HANA-Transformationsprojekt sollte der Ansatz ‚Security- und Privacy-by-Design-and-by-Default' von Anfang an gelten: SAP-Sicherheit-Awareness und -Governance vom Management für eine erfolgreiche Umsetzung sind entscheidend und in der Projektplanung zu berücksichtigen."

Dr. Alexander Ziesemer, SAP-Security Manager bei der thyssenkrupp Materials Services GmbH und Sprecher des DSAG-Arbeitskreises Security & Vulnerability Management

zicht auf Direktverbindungen. Diese Leitlinien werden beim Verwenden der Plattformen berücksichtigt und sollten von allen Beteiligten verinnerlicht und umgesetzt werden. Für thyssenkrupp Materials Services hieß das konkret: Security- und Privacy-by-Default wurden im Projekt von Anfang an als wesentliche Key-Design-Principals beachtet.

Aufwand und Gewinn gegenüberstellen

Die Kosten für die Umsetzung der Sicherheitsstrategie zu Beginn einer S/4HANA-Transformation fallen grundsätzlich deutlich geringer aus, als dies der Fall ist, wenn in ein bestehendes System eingegriffen werden muss.

Einsparpotenzial bei der BTP-Security kann im Vergleich zur klassischen S/4HANA-Security On-Premises im Bereich Infrastruktursicherheit, wie z. B. beim Netzwerk oder Betriebssystem, nicht ermittelt werden, da diesen SAP als Plattformbetreiber verantwortet. Dafür stellen reine Cloud-Anwendungen höhere Anforderungen bezüglich Vertrags-Management, Authentifikation, Verschlüsselung und Integration. In puncto Sicherheitsempfehlungen für die BTP und deren Implementierung herrscht erheblicher Nachholbedarf bei SAP. Die Übersicht an Empfehlungen mit Verweisen auf die Dokumentation ist leider nicht immer aussagekräftig genug, um sie einfach umsetzen zu können. „Das Thema Cloud-Plattform-Integration/Application-Programming-Interface (CPI/API) fehlt z. B. leider in der Gesamtübersicht der Security-Recommendation der BTP, zudem muss für das Zertifikats-Management die Prinicipal Propagation (siehe Glossar Seite 42) zur Standardlösung werden", beschreibt Alexander Ziesemer mögliches Verbesserungspotenzial ein Plus an Sicherheit.

Sicherheitsbewusstsein verbessert

Bei thyssenkrupp Materials Services hat die Sicherheitsstrategie die Mitarbeitenden nachhaltig sensibilisiert, das Thema von Anfang an auf dem (Bild-)Schirm zu haben. Dadurch konnten Risiken deutlich gesenkt und das Sicherheitsbewusstsein aller Beteiligten enorm verbessert werden.

Die Botschaft an alle Unternehmen lautet: Egal, ob Sie am Anfang einer Sicherheitsstrategie stehen oder mittendrin sind, verschließen Sie nicht die Augen vor den Herausforderungen einer sicheren SAP-Landschaft, und gehen Sie einfach mutig voran. ■

Glossar

SAP Unified Connectivity (UCON)
Das Konzept Unified Connectivity fasst die zentralen Connectivity-Technologien des ABAP-Server (RFC, HTTP, HTTPS) in einem Administrations-Framework zusammen. Das Ziel ist eine erhöhte Sicherheit der Kommunikation, z. B. durch Reduktion extern sichtbarer und aufrufbarer Funktionen.

Secure-Network-Communications (SNC)
Secure-Network-Communications (SNC) integriert SAP Single Sign-On oder ein externes Sicherheitsprodukt in SAP-Systeme. SNC schützt die Datenkommunikationspfade zwischen verschiedenen Client- und Server-Komponenten des SAP-Systems, die das SAP-Protokoll RFC oder DIAG verwenden.

Principal Propagation
Mithilfe einer Laufzeit-Engine von SAP Process Integration (Integration Engine oder Advanced Adapter Engine) lässt sich definieren, dass Benutzeridentitäten sicher von einem Sender zu einem Empfänger weitergeleitet werden. Dieser Vorgang wird als Principal Propagation bezeichnet.

HTTPS-by-Default
HTTPS-by-Default verbessert die Web-Sicherheit und den Datenschutz bei verstärktem HTTPS-Einsatz.

SAP Secure Operations Map
Die Secure Operations Map strukturiert bewährte Sicherheitsverfahren nach 16 Themen auf fünf Ebenen:

- Organisation
- Prozess
- Anwendung
- System
- Umfeld

spc.2bm.dk/wp-content/uploads/2021/08/The-Secure-Operations-Map_-Highlights-and-Best-Practices-for-Securing-SAP-Solutions.pdf