Veränderung als Chance begreifen

S/4HANA-TRANSFORMATION ALS BOOSTER FÜR MEHR SAP-SICHERHEIT

Die in vielen Unternehmen anstehende Migration zu S/4HANA bietet eine einzigartige Gelegenheit, die häufig vernachlässigte Sicherheit ihrer SAP-Landschaft zu stärken. Durch eine ganzheitliche Sicherheitsstrategie, die organisatorische Aspekte, Prozesse und technische Maßnahmen umfasst, können sich Unternehmen proaktiv gegen die ständig wachsenden Bedrohungen im SAP-Umfeld wappnen. Statt als Bedrohung sollte die Transformation als Chance zur Optimierung der IT-Sicherheit betrachtet werden.

Kaum ein größeres Unternehmen in Deutschland kommt ohne SAP-Produkte aus. Häufig spielen sie sogar eine zentrale Rolle, verwalten kritische Informationen und steuern Geschäftsprozesse, ohne die eine Firma nicht funktionsfähig wäre. Den Kern bildet oft ein vor Jahrzehnten eingeführtes SAP ECC (ERP Central Component), das als On-Premises-System betrieben und allgemein als „SAP ERP" bezeichnet wird. Es besteht aus einer Reihe von Modulen, zum Beispiel für die Personal- oder Materialwirtschaft, und wird durch eine Vielzahl von Drittprogrammen und Eigenentwicklungen ergänzt.

Trends aus der IT-Welt fassen mit einer gewissen Verzögerung auch in der SAP-Welt Fuß. Besonders der notwendige Umstieg auf die neueste ERP-Plattform SAP S/4HANA und die Abkündigung anderer weit verbreiteter SAP-Produkte forciert die Verschiebung von selbstbetriebenen On-Premises-Systemen hin zu Cloud-Lösungen. Aus technischer Sicht ergeben sich damit eine Vielzahl von Fragestellungen, die entweder völlig neu sind oder nach Jahren der gelebten Praxis modifiziert werden müssen. Das gilt sowohl für veränderte organisatorische Rahmenbedingungen wie Verantwortlichkeiten (Stichwort „Shared Responsibility" mit dem Cloud-Provider) als auch für die technische Ausgestaltung wie die Integration in die nun hybride Systemlandschaft des Unternehmens. Klar ist, dass die Einführung von SAP S/4HANA zu einer veränderten IT-Architektur mit einer Vielzahl neuer Komponenten und Schnittstellen führt.

Parallel hierzu nimmt die Bedrohungslage durch Cyberangriffe stetig zu. Das veränderte Betriebsmodell und die steigende Anzahl von Schnittstellen durch die Einführung der neuen Lösungen bedeuten aber auch, dass sich die Menge potenzieller Angriffsvektoren für SAP-Systeme erhöht. In diesem Kontext treffen Angreifer auf eine für sie günstige Situation, denn oft ist zu beobachten, dass sowohl die existierenden SAP-Systeme als auch die neu eingeführten Komponenten unsicher betrieben werden. Die Gründe hierfür sind simpel: SAP ECC wurde aus Kompatibilitätsgründen unsicher ausgeliefert. Die Unternehmen mussten und müssen sich selbst um verschiedenste Aspekte der Absicherung kümmern. Gleichzeitig sind der Betrieb und die Transformation eines SAP-Systems zu S/4HANA sehr komplex. Wenn hier zu häufig „Lift and Shift" genutzt wird und bestehende Einstellungen und Prozesse ohne Berücksichtigung von geänderten Angriffsvektoren übernommen werden, dann erhöht sich das Risiko von ausnutzbaren Schwachstellen. Mit der Vielzahl neuer Schnittstellen entsteht eine risikoreiche Gemengelage: Bislang nur intern kompromittierbare Sicherheitslücken können nun „von außen" – also beispielsweise von Angreifern aus dem Internet oder über Supply-Chain-Angriffe – ausgenutzt werden.

Bestes Beispiel hierfür ist der SAP-Patchprozess. Bisher hielten es viele Unternehmen für ausreichend, die monatlich von SAP bekannt gegebenen Schwachstellen nur selten – etwa jährlich oder halbjährlich – zu schließen, da die SAP-Systeme tief „im internen Netzwerk" standen und somit als vermeintlich wenig angreifbar galten. In hybriden Architekturen und beim Betrieb kritischer SAP-Systeme bei einem Cloud Provider mit vielen neuen Zugriffsmöglichkeiten reicht das nicht mehr aus.

Ein weiteres Beispiel sind die vielen Eigenentwicklungen, mit denen ein SAP-System an die eigene Unternehmenswirklichkeit angepasst worden ist. Dieser sogenannte „Custom Code" hat häufig wichtige Sicherheitspraktiken für die ABAP-Entwicklung nicht beachtet. Im Zuge einer S/4HANA-Transformation muss zwar geprüft werden, ob der Custom Code fit für S/4HANA ist, aber diese Prüfungen berücksichtigen in der Regel keine sicherheitsrelevanten Aspekte, zum Beispiel hart codierte Anmeldenamen und Passwörter oder fehlende Berechtigungsprüfungen. Eine gute Gelegenheit, solchen Code zu korrigieren, die leider allzu oft ungenutzt verstreicht.

GESTIEGENER HANDLUNGSBEDARF

Die Tatsache, dass der in vielen Unternehmen unsichere Betrieb in den letzten 20 Jahren häufig problemlos funktioniert hat, ist mit Blick auf die Bedrohungslage keine Garantie, dass ein „weiter so" ebenso gut funktionieren wird. Ganz im Gegenteil: Angesichts der gestiegenen Cyberrisiken und heterogenen Bedrohungslagen sollte die S/4HANA-Transformation allem voran als Chance begriffen werden, das Sicherheitsniveau an die aktuellen Anforderungen anzupassen. SAP unterstützt das inzwischen nach eigener Aussage durchaus: Schon im Auslieferungszustand ist die Sicherheit von S/4HANA höher als bei den Vorgängerversionen – Stichwort „Secure by Default".

Zudem gibt es weitere Möglichkeiten und Maßnahmen, um die Systemsicherheit in diesem Zuge langfristig zu verbessern und zukunftsfähig zu gestalten. Von zentraler Bedeutung wird es sein, die Sicherheit von Anfang an und in allen Phasen des Aufbaus der S/4HANA-Plattform und darüber hinaus zu berücksichtigen („Security by Design"). SAP kann das Sicherheitsdesign im konkreten Unternehmenskontext allerdings naturgemäß nur sehr begrenzt vorgeben. Unternehmen müssen daher auch zukünftig selbst prüfen, ob die Standardeinstellungen von SAP in ihrem Kontext ausreichen oder ob strengere Werte und Maßnahmen notwendig sind.

ZUR ZENTRALEN BEDEUTUNG DER CYBERSECURITY FÜR SAP-SYSTEME

Zunächst ist die grundsätzliche Frage zu beantworten, warum SAP-Systeme überhaupt aus der Sicherheitsperspektive betrachtet werden sollten. Dazu muss man sich bewusst machen, dass SAP-Systeme häufig für die Kerngeschäftsprozesse unverzichtbar sind. In der fertigenden Industrie ist über diese Systeme beispielsweise oft die Produktion mit der Warenwirtschaft verbunden.

Dadurch entstehen einerseits Absprungpunkte und Einfallstore in kritische Bereiche, in denen sensible Daten lagern. Andererseits geht damit die Gefahr einher, dass im Zuge eines Angriffs im schlimmsten Fall beispielsweise die Produktion stillsteht oder hochsensible Informationen öffentlich werden. Der Schutz kritischer Bereiche, sensibler Information und die Verfügbarkeit kritischer Unternehmensprozesse stellt somit die wichtigste Motivation dar, sich nachhaltig um das Thema Cybersecurity für SAP-Systeme zu kümmern.

Bisher wurde und wird SAP-Sicherheit in vielen Organisationen als eine reine Frage von Rollen und Berechtigungen verstanden. Dies ist zwar in der Tat ein zentraler Bestandteil, aber im Folgenden werden weitere wichtige Bereiche aufgezeigt, die erfahrungsgemäß zu häufig vernachlässigt werden.

DIE AUSGANGSLAGE ERMITTELN: EINE SCHUTZBEDARFSANALYSE SCHAFFT KLARHEIT

Unter anderem aufgrund des Fachkräftemangels ist es oftmals schwierig, im Unternehmen Expertise für Cybersicherheit aufzubauen und zu halten. Dies gilt umso mehr für die nochmals speziellere Cybersicherheit im SAP-Kontext. Hinzu kommt, dass die Bedrohungslage diffus und unübersichtlich ist und ein solides Sicherheitskonzept eine komplexe Herausforderung darstellt. Laut dem Lagebericht 2023 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) findet eine zunehmende Professionalisierung im Bereich Cyberkriminalität statt, wodurch sich die Wahrscheinlichkeit, Ziel eines Angriffs zu werden, signifikant erhöht.

Um einen Überblick über den Status quo zu erhalten, ist es daher sinnvoll, als ersten Schritt eine Schutzbedarfsanalyse durchzuführen, um den tatsächlichen Schutzbedarf der SAP-Systeme zu ermitteln und daraus grundlegende Sicherheitsanforderungen abzuleiten. Sobald diese bekannt sind, ist es anschließend zielführend, eine Bedrohungsmodellierung vorzunehmen, um Angriffsvektoren zu identifizieren und die damit verbunden Risiken zu bewerten. Als primäres Einfallstor müssen dabei alle Systeme betrachtet werden, die mit dem Internet verbunden sind oder die Schnittstellen zu externen Partnern wie beispielsweise Lieferanten haben. Weitere denkbare Angriffspfade kommen von internen Quellen oder nutzen Schwachstellen der Datenbank oder des Betriebssystems aus.

Die Tragweite von Angriffsszenarien wurde beispielsweise vor einigen Jahren deutlich, als Onapsis über die Gefahren informierte, die mit dem sogenannten „10KBLAZE-Exploit" verbunden sind. Über eine Schwachstelle im System

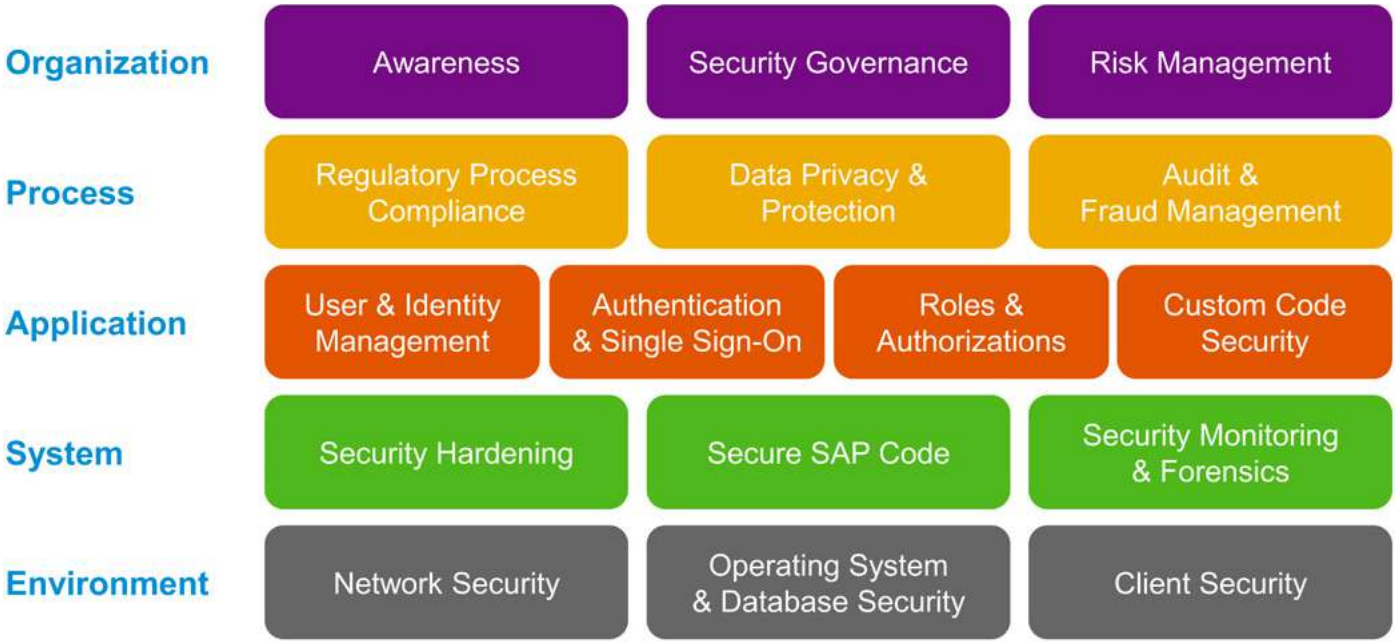

Abbildung 1: Die SAP Secure Operations Map strukturiert wesentliche Sicherheitsthemen rund um SAP Security. (Bild: SAP 2020)

bestand dabei das Risiko einer vollständigen Kompromittierung des SAP-Systems, verbunden mit dem möglichen kompletten Stillstand des Unternehmens – und zwar innerhalb von Sekunden. SAP hatte bereits 2005 auf die korrekte Konfiguration der Sicherheitseinstellungen hingewiesen, trotzdem waren weiterhin viele Systeme verwundbar.

Auf Basis der identifizierten Bedrohungen und Angriffswege lassen sich dann die notwendigen Sicherheitsmaßnahmen definieren, um diesen Risiken zu begegnen. Hilfreich ist dabei die Orientierung an der SAP Secure Operations Map, die in fünf Ebenen strukturiert ist (siehe Abbildung 1). Sie deckt viele relevante organisatorische, prozessuale und technische Aspekte der Sicherheit von SAP-Systemen ab. Damit ist sie ein guter Startpunkt für einen ganzheitlichen Blick auf SAP-Sicherheit. Sie kann bei Bedarf um weiteren Themen, wie zum Beispiel Business Continuity, ergänzt werden. Nachfolgend gehen wir konkret auf vier Themen ein, die dabei erfahrungsgemäß besonders wichtig sind.

DIE PFLICHT: PATCH-MANAGEMENT UND „SECURITY BY DESIGN“

Um einen gewissen Sicherheitsstandard zu erreichen, müssen die Grundlagen stimmen: Erstens stellt – wie oben bereits erwähnt – ein sauberes Patchmanagement eine große Herausforderung dar. SAP veröffentlicht monatlich Behebungsmaßnahmen („Security Notes“) zu Schwachstellen, die zu einer potenziellen Bedrohung werden können. Die Implementierung dieser Maßnahmen ist eine kontinuierliche Aufgabe, die es unabhängig von einzelnen Transformationsprojekten zu lösen gilt. Um diese Informationen zu verarbeiten, die damit verbundenen Risiken zu prüfen und nach Relevanz zu filtern, sollten Unternehmen einen Prozess aufsetzen. Im Idealfall wird im monatlichen Turnus überprüft, welche Security Notes für die eigene Landschaft relevant sind, und deren Einspielen gemäß einer definierten Patch-Policy eingeplant. Da beim Aktualisieren zum Teil die SAP-Systeme heruntergefahren und neu gestartet werden müssen, ist eine sorgfältige Prüfung im Vorfeld ratsam.

Das zweite wichtige Thema ist das Erkennen von Schwachstellen in der Konfiguration der Systeme („Härtung“). Dazu sollte man einerseits den eigenen Reifegrad analysieren. Hier können zum Beispiel Konfigurationsvorgaben wie das Security Baseline Template der SAP helfen, um die Sicherheit der Konfiguration zu beurteilen und die Systeme zu härten. Andererseits sollte vor oder nach der Umstellung mindestens ein Penetrationstest der neuen Systeme durchgeführt werden, um mögliche Schwachstellen zu identifizieren.

Eine Lösung dafür ist „Security by Design“: Dafür werden schon in einer frühen Projektphase die spezifischen Sicherheitsanforderungen betrachtet. Zudem sieht dieses Vorgehen eine Bedrohungsmodellierung in der Architekturphase vor. Denn nur wenn festgelegt und identifiziert ist, vor welchen Bedrohungen man sich schützen muss, können entsprechende Maßnahmen eingeleitet werden. Auf diese Weise werden auch die Risiken für die angebundenen Systeme erkannt und am Ende von einer unabhängigen Instanz getestet. Im besten Fall bestätigt der anschließende Penetrationstest die erfolgreiche Umsetzung durch wenige oder keine Feststellungen.

DIE KÜR: SICHERE SOFTWAREENTWICKLUNG UND ÜBERWACHUNG DER SAP-LANDSCHAFT

Nach den Grundlagen kann man sich an die komplexeren Sicherheitsthemen wagen. Das erste große Thema bei der Umstellung ist hier die in vielen Unternehmen fehlende sichere Softwareentwicklung (Secure Software Development Lifecycle) für SAP-Eigenentwicklungen. Da

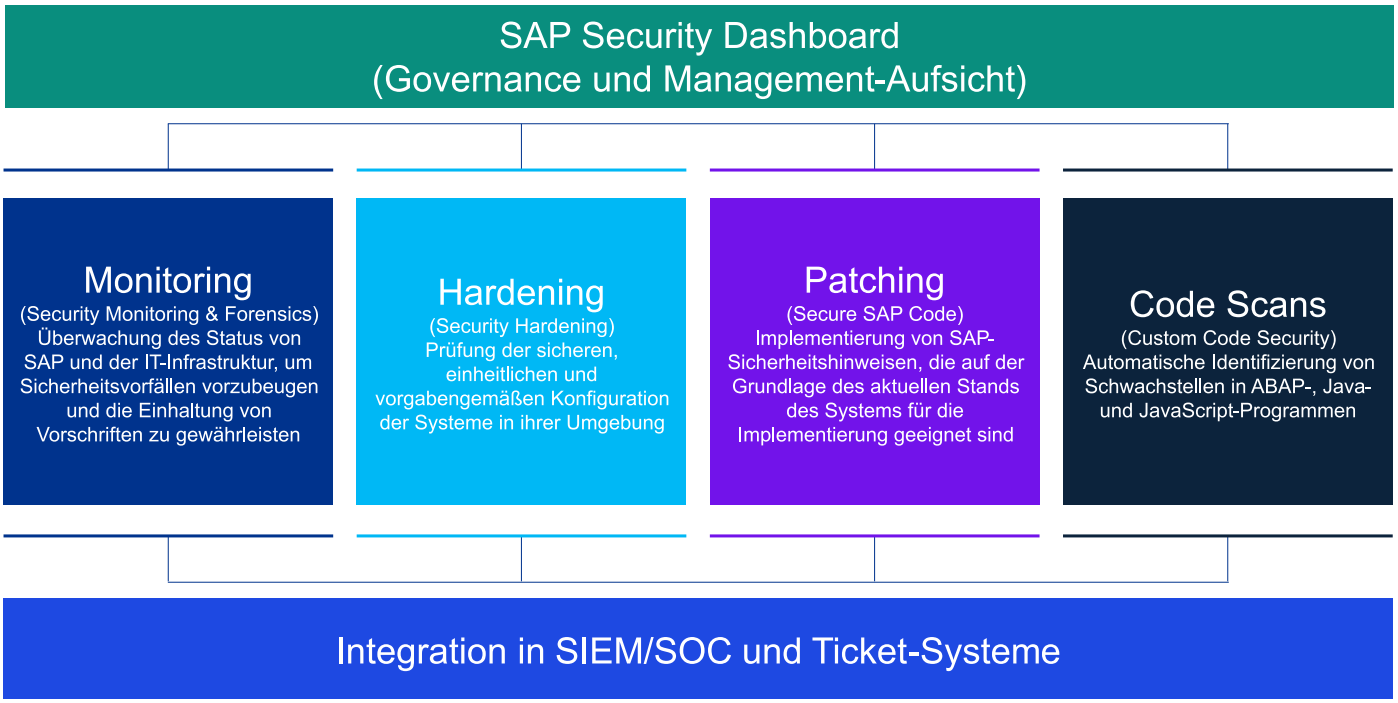

Abbildung 2: SAP Security Tools können bei den wichtigsten Aufgaben unterstützen.

SAP-Lösungen eigentlich immer an das Unternehmen angepasst werden müssen, sind solche Eigenentwicklungen weit verbreitet. Viel zu häufig wird aber vernachlässigt zu prüfen, ob der Code sicher ist und ob die Softwareentwicklung den nötigen Sicherheitsstandards entspricht. So kann es vorkommen, dass Eigenentwicklungen keine Berechtigungen überprüfen oder unsichere, manipulierbare Instruktionen verwenden. Dementsprechend müssen SAP-spezifische Regelungen für die Entwickler vorgegeben werden, die auch in die Verträge mit Entwicklungsdienstleistern aufgenommen werden. Dies gilt naturgemäß für die SAP-eigene Programmiersprache ABAP, insbesondere im Web-Entwicklungsumfeld aber auch für Java oder JavaScript. Durch spezielle Code-Scanner für SAP lässt sich zudem der „Custom Code", also der selbstentwickelte Code, auf Schwachstellen prüfen.

Neben den Eigenentwicklungen selbst können aber auch eingekaufte SAP Add-ons oder die in Eigenentwicklungen verwendeten Bibliotheken ein Sicherheitsrisiko darstellen. Besonders bei JavaScript-Entwicklungen sammeln sich hier schnell Dutzende Abhängigkeiten, die Schwachstellen aufweisen können. Vor allem in Open-Source-Bibliotheken werden Sicherheitslücken regelmäßig bekannt und entsprechende Patches in Form fehlerbereinigter Versionen bereitgestellt. Eine Übersicht dieser Code-Bestandteile in einer „Software Bill of Materials" (SBOM) sollte also gepflegt und auf Schwachstellen und Updates hin überwacht werden. Ohne diese Übersicht ist es praktisch nahezu unmöglich, alle wichtigen Sicherheitspatches kontinuierlich einzuspielen.

Die bisher dargestellten Sicherheitsmaßnahmen sind vor allem präventiver Natur. Da eine perfekte Sicherheit aber niemals erreicht werden kann, müssen diese präventiven Maßnahmen auch um aufdeckende und reaktive Schritte ergänzt werden. Wichtig hierfür ist eine Aggregation der durch die verschiedenen SAP-Produkte generierten Protokolle an einer zentralen Stelle. Das verhindert zum einen, dass Angreifer diese Protokolle manipulieren, und es ermöglicht zum anderen die Analyse der Logdaten mit Security-Information-and-Event-Management-(SIEM)-Tools, um verdächtige Aktivitäten und mögliche Angriffe zu erkennen und an das Security Operations Center (SOC) zu melden. In SAP-ERP-Systemen ist hier besonders das Security Audit Log zu erwähnen, das viele relevante Aktivitäten erfassen kann. Dafür muss dieses Log aber auch aktiviert und entsprechend konfiguriert sein, sodass vor allem kritische Aktionen von Standard- und hochprivilegierten Nutzern erfasst werden.

Um auf einen erkannten Sicherheitsvorfall angemessen reagieren zu können, sollten hierfür schon im Vorfeld Pläne erstellt werden. Diese legen zum Beispiel fest, welche Maßnahmen zur Eindämmung eines Angriffs angebracht sind und wie die Systeme bereinigt und wiederhergestellt werden können. Mit diesen Plänen und ihrer regelmäßigen Überprüfung ist ein Unternehmen gut auf den Ernstfall vorbereitet.

AUTOMATISIERUNG VON SICHERHEITSAUFGABEN

Während einzelne Sicherheitsmaßnahmen in einem ersten Schritt häufig noch manuell durchgeführt werden können, erfordert eine kontinuierliche Absicherung typischerweise eine Automatisierung durch entsprechende Sicherheitslösungen. Dies gilt umso mehr für größere SAP-Landschaften. Auf SAP spezialisierte Dienstleister bieten hier diverse Lösungen an, die voll automatisiert mehrere oder sogar alle der oben besprochenen Handlungsfelder abdecken, die beispielsweise die Konfiguration auf Schwachstellen prüfen, fehlende Patches identifizieren und verdächtiges Verhalten erkennen und mel-

den. Zusätzlich kann über eine solche Lösung auch die Integration in unternehmensweite Sicherheitslösungen, in Ticketsysteme und in das Reporting gestaltet werden. In Abbildung 2 ist das Zusammenspiel der verschiedenen Funktionen dargestellt.

Durch den Einsatz solcher Lösungen können Unternehmen das Sicherheitsniveau noch einmal erheblich steigern und auf einem einheitlichen Standard halten. Hierbei dürfen die Verantwortlichen allerdings nicht vergessen, dass die identifizierten Schwachstellen und Probleme auch behoben werden müssen. Eine Integration solcher Lösungen in die internen Ticketsysteme und in die entsprechenden Prozesse ist also zwingend notwendig. Ebenso sollte sichergestellt werden, dass die Lösungen auch wirklich die gesamte SAP-Landschaft abdecken und zuverlässig Probleme erkennen. Hier sind entsprechende Tests der Wirksamkeit unverzichtbar.

DIFFUSE SICHERHEITSVERANTWORTUNG IN DER CLOUD

Besonders mit dem Lizenzmodell „SAP RISE" (von SAP als „Business-Transformation-as-a-Service" beworben), ist das Thema Cloud für SAP-ERP-Kunden seit 2024 stärker in den Vordergrund gerückt. Im Kern wird dabei auf eine Platform-as-a-Service-Variante (PaaS) von SAP ERP gesetzt. Obwohl die Entscheidung für SAP RISE in der Regel finanziell und nicht durch Sicherheitsaspekte motiviert ist, geht damit natürlich eine Verschiebung der Verantwortlichkeiten für die Sicherheit einher. Teilweise führt das zur falschen Annahme, dass die Verantwortung für die IT-Sicherheit bei Cloud-Diensten exklusiv beim Anbieter – beispielhaft seien hier SAP, Google, Amazon oder auch Microsoft genannt – liegt. SAP selbst versucht, durch das „Shared Responsibility Modell" und eine Liste mit über 1.300 Aktivitäten und Verantwortlichkeiten für das zentrale Produkt „SAP S/4HANA Cloud, Private Edition" mehr Klarheit zu schaffen. Die Erfahrung zeigt jedoch, dass es im Detail dennoch oft diffus und schwer zu greifen ist, wer am Ende für welche Sicherheitsaspekte des SAP-Systems zuständig ist. Es ist also essenziell, genau zu verstehen, welche Aufgaben konkret beim Unternehmen verbleiben.

Auch sollte stets berücksichtigt werden, dass die Durchführung einzelner Sicherheitsaufgaben zwar an die SAP – oder einen anderen Provider – übertragen werden kann; die Gesamtverantwortung für die IT-Sicherheit verbleibt aber beim Unternehmen. Schließlich betreffen eventuelle Sicherheitsvorfälle immer noch die eigenen Geschäftsprozesse und Daten.

REGULIERUNG WIRKT SICH AUCH AUF SAP AUS

Neben der intrinsischen Motivation des Unternehmens, sich vor Schäden durch Cyberangriffe zu schützen, gibt es mittlerweile zahlreiche externe Faktoren. Weltweit ist eine Verschärfung und Erweiterung der Regulierung zu beobachten, die die Cybersicherheit national wichtiger Unternehmen verbessern sollen – im europäischen Raum aktuell zum Beispiel durch die Network-and-Information-Systems-2-(NIS-2)-Richtlinie oder den Cyber Resilience Act (CRA). Sobald Organisationen von diesen Regelungen betroffen sind, müssen auch die SAP-basierten Kernsysteme und -prozesse betrachtet werden.

Da die Übersetzung und die Implementierung von „klassischen" Cybersicherheitsmaßnahmen in die SAP-Landschaft alles andere als trivial sind, sollten sich Unternehmen damit frühzeitig auseinandersetzen. So ist etwa die Einführung von Systemen zur Angriffserkennung im SAP-Kontext nochmals herausfordernder als in der „normalen" Office-IT. Im Idealfall ist das SAP-Universum auch nicht losgelöst von allgemeinen Cybersicherheitsmaßnahmen, sondern es wird stets versucht, dieses zu integrieren. Damit kann man Synergien nutzen und unnötige Doppelarbeiten vermeiden.

FAZIT

Cybersicherheit und Datensicherheit sind für die SAP-Systeme eines Unternehmens aufgrund ihrer zentralen Bedeutung enorm wichtig. Je nach Risikoprofil müssen Organisationen ihr Sicherheitsnetz entsprechend auslegen. Es ist jedoch nicht zielführend, dies als einmaligen Vorgang zu betrachten. Sicherheit ist eine kontinuierliche Aufgabe, die als dauerhafter Prozess im Unternehmen verankert werden sollte. Dazu müssen entsprechende Ressourcen eingeplant, Verantwortlichkeiten verteilt und Kompetenzen aufgebaut werden.

Besonders der Rahmen einer S/4-Transformation bietet hier die Möglichkeit, SAP-Sicherheit neu zu denken und systematisch zu planen. Die Umsetzung der Sicherheitsmaßnahmen kann dann entlang der Transformation erfolgen. Auf diese Weise wird sukzessive eine verlässliche Grundlage geschaffen, die einen langfristig sicheren SAP-Betrieb auf einer abgesicherten Infrastruktur ermöglicht. ■

STEFAN HÖLZNER
ist Senior Manager Cyber Security bei der KPMG AG und beschäftigt sich seit 25 Jahren mit SAP Security, davon zehn Jahre als Sprecher des Arbeitskreises Sicherheit in der Deutschsprachigen SAP-Anwendergruppe (DSAG). Weiterhin verantwortet er technische Sicherheitsanalysen und Penetrationstests, sowohl im Mittelstand als auch bei international tätigen Konzernen.

CONSTANTIN VON HORNUNG
ist Senior Consultant Cyber Security bei der KPMG AG und beschäftigt sich seit zehn Jahren mit SAP und Security. Er berät zu technischen, organisatorischen und prozessualen Security-Fragestellungen für SAP-Produkte On-Premises und in der Cloud.

KAI-OLIVER KOHLEN
ist Consultant Cyber Security bei der KPMG AG und beschäftigt sich seit fünf Jahren mit Security. Im Kontext von SAP berät er sowohl zu technischen als auch organisatorischen Themen. Außerdem beschäftigt er sich mit Bedrohungsanalysen und Penetrationstests unter anderem für SAP-Systeme.