Einleitung

Die letzte Auflage dieses Buches ist 2018 im Rheinwerk Verlag erschienen, und nach drei Jahren ist es nun Zeit für eine Neuauflage. Als ich an dem Manuskript der Vorauflage arbeitete, war SAP S/4HANA bereits zwei Jahre auf dem Markt, aber es liefen nur wenig Migrationsprojekte. SAP-Kundenunternehmen informierten sich über die neue Business Suite und führten Vorstudien für die Migration durch. Diese Situation sieht inzwischen grundlegend anders aus. Bereits Ende 2019 gaben laut der Lünendonk-Studie 52 % der befragten Unternehmen an, sich in einer Vorstudie zur SAP-S/4HANA-Migration zu befinden (siehe unter: *http://s-prs.de/v612212*). 98 % wollten diese Vorarbeiten bis 2021 abschließen. In dieser Auflage des Buches habe ich daher sicherheitsrelevante Themen ergänzt, die bei der Einführung und dem Betrieb von SAP S/4HANA zu beachten sind.

Verglichen mit den Entwicklungen in den letzten 24 Jahren, in denen ich mich mit der Sicherheit von SAP-Systemen befasste, ist die Umstellung von der klassischen SAP Business Suite auf SAP S/4HANA (zusammen mit der Umstellung der Datenbank auf SAP HANA) der größte Technologiewechsel in der SAP-Welt. Und auch das Bewusstsein für das Thema Sicherheit hat sich in den letzten Jahren gewandelt. War es früher »ein lästiges Übel«, werden Sicherheit und Berechtigungen heute größtenteils fest in die Vorstudien zur Migration und die Durchführung der Projekte eingeplant. Das Risiko, einem Cyberangriff zum Opfer zu fallen, ist heute so hoch wie nie. Die Gefahr eines finanziellen Schadens oder eines Reputationsschadens ist permanent vorhanden.

Zur Härtung der Systeme ist insbesondere die Sicherheit der technischen Grundkomponenten – SAP NetWeaver und der Datenbank – entscheidend. Ist hier eine entsprechende Absicherung erfolgt und sind die Berechtigungen nach dem Minimalprinzip vergeben, reduziert dies die Gefahr für Angriffe erheblich. Dieses Buch ist der Versuch, alle wesentlichen Aspekte zur Absicherung von SAP NetWeaver und der SAP-HANA-Datenbank so darzustellen, dass sie für Prüferinnen und Prüfer analysierbar und für die Sicherheitsverantwortlichen umsetzbar sind.

Daher richtet sich dieses Buch sowohl an alle, die für die Sicherheit der SAP-Systeme verantwortlich sind, als auch an diejenigen, die diese Sicherheit durch Prüfungen analysieren und bewerten.

Aufbau des Buches

Jedes Kapitel ist in sich abgeschlossen und bietet einen umfassenden Überblick zum Thema. Die jeweiligen Abschnitte sind so aufgebaut, dass sie auch als Nachschlage-

werk für einzelne Fragestellungen genutzt werden können. Um jeden Abschnitt für sich umfassend und schlüssig darzustellen, wurden Redundanzen bewusst in Kauf genommen.

Zu fast jedem Thema gibt es einen Abschnitt zu den Zugriffsrechten. Hier sind die zu prüfenden Berechtigungen aufgeführt. Zur Prüfung dieser Berechtigungen können Sie das Benutzerinformationssystem nutzen (Transaktion SUIM). Die Auswertung von Berechtigungen ist in Abschnitt 10.5, »Prüfung von Zugriffsrechten«, beschrieben.

Außerdem gibt es zu fast jedem Abschnitt eine Checkliste. In der Checkliste sind alle Prüfungsfragen zum jeweiligen Thema zusammengefasst, inklusive einer Risikobewertung:

1. hohes Risiko
2. mittleres Risiko
3. geringes Risiko

Auf der Seite *www.sap-press.de/5145* erhalten Sie im Bereich **Materialien zum Buch** das Dokument **Tiede_Checklisten_Sicherheit_und_Pruefung.pdf**. Darin erläutere ich zu jedem Punkt der Checklisten die praktische Vorgehensweise am System. Dies erlaubt es Ihnen als Prüfer*in, die jeweiligen Prüfungsschritte sofort auszuführen, auch wenn Sie nicht täglich mit dem SAP-System arbeiten.

Des Weiteren erhalten Sie im Downloadbereich das folgende Handwerkszeug:

- Die Berechtigungsrolle `IBS_SICHERHEIT_PRUEFUNG_NW755`. Sie enthält ein Menü in der Struktur dieses Buches und die erforderlichen Berechtigungen, um alle Prüfungen gemäß diesem Buch durchzuführen.
- Ein Regelwerk für SAP Access Control mit den Berechtigungsabfragen aus diesem Buch. Dies kann direkt in SAP Access Control importiert werden. Näheres dazu finden Sie in Abschnitt 1.10.4, »SAP-Access-Control-Regelwerk für dieses Buch«.
- Das Dokument **Tiede_Anhänge_Sicherheit_und_Pruefung.pdf**. Hierin sind alle sicherheitsrelevanten Parameter, Transaktionen, Reports und Tabellen sowie die sicherheitsrelevanten SAP-HANA-Tabellen aufgelistet.

In hervorgehobenen Informationskästen finden Sie in diesem Buch Inhalte, die wissenswert und hilfreich sind, aber etwas außerhalb der eigentlichen Erläuterung stehen. Damit Sie diese Informationen sofort einordnen können, haben wir die Kästen mit den entsprechenden Symbolen gekennzeichnet:

In Kästen, die mit diesem Symbol gekennzeichnet sind, finden Sie Informationen zu *weiterführenden Themen* oder Hintergrundwissen, das Sie sich merken sollten.

Beispiele, durch dieses Symbol kenntlich gemacht, weisen auf Szenarien aus der Praxis hin und veranschaulichen die dargestellten Funktionen.

Inhalt des Buches

In **Kapitel 1**, »Umgang mit dem SAP-System und Werkzeuge zur Prüfung«, stelle ich Ihnen die Funktionen vor, die zur Prüfung von SAP-Systemen erforderlich sind. Auch wenn sich für Prüfer*innen nicht allzu viel ändert, da sie Prüfungen auch in SAP S/4HANA weiterhin im ABAP-Stack durchführen, kommen doch regelmäßig neue Tools hinzu. Die gute Nachricht ist hier, dass die seit Jahren bekannten Transaktionen weiterhin verfügbar sind, teils mit aktualisierten Oberflächen, teils unverändert. Schwerpunkt einer jeden Prüfung sind Tabellen und Reports. Für die Nutzung von Tabellen ist der *Generic Table Browser* eingeführt worden, der auch für Prüfer*innen teilweise neue Möglichkeiten eröffnet. Aber auch die Zugriffsstatistik, der Quick-Viewer und der SQL-Trace können hilfreich für Analysen sein.

Wesentliche Komponenten für die SAP-Sicherheit sind Tools zur Überwachung und Prüfung von Berechtigungen und zur Überwachung von Betrugsdelikten. Daher stelle ich in diesem Kapitel die Werkzeuge SAP Access Control und SAP Enterprise Threat Detection vor. Beide Komponenten werden nicht im Rahmen von Prüfungen eingesetzt, sondern zur regelhaften Absicherung. Für SAP Access Control können Sie das Regelwerk aus dem Downloadbereich zu diesem Buch nutzen, um die kritischen Berechtigungen zur SAP-Basissicherheit zu überwachen. Der letzte Abschnitt dieses Kapitels zeigt Ihnen, wie Prüfungen in SAP HANA durchgeführt werden können.

Kapitel 2, »Aufbau von SAP-Systemen und Systemlandschaften«, stellt den Aufbau von SAP-Systemen dar. Dieses Wissen ist elementar für die Absicherung von SAP-Systemen und -Systemlandschaften. Mit SAP S/4HANA ändert sich hier einiges, da mit dem SAP Fiori Launchpad eine neue Ebene hinzukommt. Ein weiterer Schwerpunkt dieses Kapitels liegt auf der Mandantensicherheit, von der maßgeblich auch die Produktivmandanten sowie der Mandant 000, der Systemmandant, betroffen sind. Insbesondere der Mandant 000 wird im Rahmen von Sicherheitskonzepten häufig vernachlässigt, obwohl von ihm aus auch die Systemeinstellungen vorgenommen werden können und Zugriffe auf die produktiven Daten möglich sind.

In **Kapitel 3**, »Allgemeine Systemsicherheit«, behandle ich die grundsätzlichen Aspekte der Systemsicherheit. Die Anmeldesicherheit stellt ein wesentliches Element zur Absicherung dar. Richtig konfiguriert können damit bereits viele Eindringversuche geblockt werden. Themen wie das Notfallkonzept und die Zugriffe auf das Betriebssystem der SAP-Server sind grundlegende Sicherheitsthemen in jedem SAP-System. Weniger beachtet werden häufig die Funktionen von SAP Business Warehouse (SAP BW), die in jedem SAP-NetWeaver-System verfügbar sind. Dies ist abzusichern, um unberechtigte Zugriffe auf sensible Daten zu verhindern.

Die Protokollkomponenten werden in **Kapitel 4**, »Protokollierungskomponenten«, behandelt. Diese stellen eine wesentliche Komponente für Prüfungen dar. Dabei unterscheide ich nach Protokollen, die automatisch vom System erzeugt werden, und

solchen, die explizit aktiviert werden müssen. Zu Letzteren gehören die Tabellenprotokollierung, das Security-Audit-Log und die Lesezugriffsprotokollierung. Die Abschnitte zu diesen Protokollen helfen Ihnen dabei, die Komponenten gesetzes- und unternehmenskonform zu konfigurieren und deren Einsatz zu prüfen. Auch viele kleinere Protokollkomponenten sind sehr hilfreich für Prüfungen, wie die Job- oder SAP-Gateway-Protokolle. Der Abschnitt über SAP Enterprise Threat Detection zeigt Ihnen, wie SAP-Systeme effizient überwacht werden können, um Eindringversuche und Betrugsdelikte zu erkennen.

Die RFC-Sicherheit wird in **Kapitel 5**, »Remote Function Calls«, behandelt. RFC ist ein wesentliches Thema der Systemsicherheit, da eine Vielzahl von Angriffen über diese Schnittstelle erfolgt. Bedingt ist dies u. a. häufig durch eine fehlende Absicherung der RFC-Berechtigungen und der Verbindungen der SAP-Systeme untereinander.

Kapitel 6, »Der Verbuchungsvorgang«, behandelt das Thema der Verbuchung. Verbuchung bedeutet, dass Daten konsistent in die Datenbank geschrieben werden. Die Verbuchung kann von vielen Faktoren beeinflusst werden, u. a. durch die Pufferung von Belegnummern, die SAP mit der parallelen Pufferung grundlegend modernisiert hat. Die Absicherung der Verbuchung wird in diesem Kapitel dargestellt.

Ein zentrales Thema der SAP-Sicherheit ist die Benutzerverwaltung, die in **Kapitel 7**, »Benutzerauswertungen«, behandelt wird. Die Absicherung des Benutzerstammsatzes und insbesondere der Initial- und Produktivkennwörter stellt den größten Schutz vor Kennwort-Hacking dar. Die Hacking-Methoden werden ausführlich im Internet dargestellt, weshalb die Absicherung davor elementar für die Sicherheit der Systeme ist. Eine recht neue Funktion ist das datenschutzkonforme Löschen und Sperren von Benutzerstammsätzen. Einen weiteren Schwerpunkt dieses Kapitels bildet die Absicherung der SAP-Standardbenutzer.

Mit dem Customizing, behandelt in **Kapitel 8**, »Customizing des SAP-Systems«, wird das SAP-System an die unternehmenseigenen Geschäftsprozesse angepasst. Customizing bedeutet maßgeblich »Pflege von Tabelleneinträgen«. Zur Prüfung und Absicherung ist es daher hilfreich, mit dem Aufbau des ABAP Dictionarys vertraut zu sein. Zentral zu betrachten sind hier die Berechtigungen für den direkten Zugriff auf Tabellen und Views. Mit dem Generic Table Browser gibt es inzwischen die Möglichkeit, den Zugriff auf Tabellen spalten- und zeilenweise einzugrenzen.

Kapitel 9, »Entwicklung in SAP-Systemen«, zeigt die Absicherung der Entwicklungsumgebung. Es existiert kein SAP-System, das nicht individuell angepasst wurde, sei es durch eigene Auswertungsreports oder durch die Implementierung komplexer Eigenentwicklungen. Dabei sind Entwicklerrichtlinien ebenso zu beachten wie die speziellen Gefahrenpunkte im Rahmen der ABAP-Programmierung. Da Entwicklung in Entwicklungssystemen stattfindet, bildet auch die Sicherheit des Transportwesens einen Schwerpunkt dieses Kapitels.

Das SAP-Berechtigungskonzept, das ich in **Kapitel 10**, »Berechtigungskonzept in ABAP-Systemen«, behandle, wirkt sich direkt auf alle anderen Sicherheitsthemen aus. Alle sicherheitsrelevanten Vorgänge werden durch Berechtigungen abgesichert. Die Serviceberechtigungen, die in SAP S/4HANA beim Einsatz von SAP-Fiori-Apps genutzt werden, stellen eine neue Ebene für Prüfer*innen dar. Der konzeptionelle Teil dieser Absicherung ist genauso relevant wie deren technische Umsetzung. Auch können die Berechtigungen durch Customizing-Einstellungen beeinflusst werden. Dieses Kapitel erklärt den Aufbau des Berechtigungskonzepts und den konzeptionellen Teil.

In **Kapitel 11**, »Praktische Prüfung von Berechtigungen«, zeige ich dann konkrete praktische Prüfungen. Neben weiteren Berechtigungen zur Systemsicherheit werden hier auch Customizing-Berechtigungen zu den Komponenten FI, MM und SAP ERP HCM sowie Berechtigungen für SAP Business Warehouse betrachtet.

Die Sicherheit von SAP HANA wird in **Kapitel 12**, »SAP HANA«, behandelt. SAP HANA ist keine reine Datenbank. Hier werden Datenbank- und Applikationsschicht zusammengeführt. Daher sind als Benutzer dort nicht nur Datenbankadministrator*innen tätig, sondern auch Entwickler*innen und zukünftig vermehrt Endanwender*innen. Bei Einsatz von SAP HANA muss daher ein entsprechendes Sicherheitskonzept erstellt werden. Neben Daten- und Kommunikationsverschlüsselungen muss die Authentifizierung abgesichert werden, um direkte Zugriffe auf die Datenbank zu unterbinden. Das Berechtigungskonzept ist hier ebenso wesentlich wie im ABAP-Stack.

Danksagung

Ich bedanke mich bei allen, die mir bei der Fertigstellung dieses Buches geholfen haben:

- beim Rheinwerk Verlag, der mir auch diese Neuauflage ermöglicht hat,
- bei Maike Lübbers, die das Lektorat übernommen hat,
- bei der IBS Schreiber GmbH für die Nutzung der SAP-Systeme für Recherchen und Screenshots,
- bei meiner Frau Kristin, die das Buch Korrektur gelesen hat

Und zu guter Letzt möchte ich wieder an alle Leserinnen und Leser appellieren, mir jegliche positive und negative Kritik sowie Anregungen für weitere Themen zukommen zu lassen. Schreiben Sie mir gern an *thomas.tiede@ibs-schreiber.de*.

Thomas Tiede
Hamburg im Februar 2021