Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein APP.4.2 SAP-ERP-System

1. Einleitung

Enterprise Resource Planning Systeme von SAP (kurz SAP-ERP-Systeme) werden eingesetzt, um interne und externe Geschäftsabläufe zu automatisieren und technisch zu unterstützen. Die SAP-ERP-Systeme verarbeiten daher typischerweise vertrauliche Informationen, sodass alle Komponenten und Daten geeignet geschützt werden müssen.

Ein SAP-ERP-System (aktuell unter den Produktbezeichnungen SAP Business Suite und SAP S/4HANA auf dem Markt) setzt sich aus verschiedenen Modulen zusammen, mit denen die Organisationsstruktur einer Institution abgebildet werden kann. Zu den Modulen eines SAP-ERP-Systems zählen unter anderem Rechnungswesen, Personalwirtschaft und Logistik. Die Kernkomponenten des SAP-ERP-Systems sind SAP NetWeaver (Applikationsserver-Middleware) und SAP HANA (Applikationsserver und Datenbank). SAP NetWeaver ermöglicht es, SAP-ABAP- und SAP-JAVA-Anwendungen anzubinden und Prozesse systemweit zu steuern. SAP HANA kann in Echtzeit große Datenmengen für alle Geschäftsbereiche analysieren.

Die Grundlage und die Struktur für diese Umsetzungshinweise sind die Richtlinien aus verschiedenen SAP-Dokumenten, z. B. SAP Security Baseline Template, SAP Security Guides (siehe [SAPSG]) und SAP Security Whitepapers (siehe [SAPSWP]). Das SAP Security Baseline Template setzt sich aus verschiedenen SAP-Empfehlungen und Quellen zusammen, z. B. SAP EarlyWatch Alert, SAP Security Optimization Service, Security Notes. Die fünf Themenschwerpunkte des Baseline Templates sind:

- Infrastruktursicherheit (Infrastructure Security: SAP verwendet den Begriff Infrastruktursicherheit, anders als im IT-Grundschutz, weniger umfassend und geht weniger auf bauliche Maßnahmen und Gebäude ein),
- Sicherheitscode (Secure Code),
- sichere Installation (Secure Setup),
- sicherer Betrieb (Secure Operation),
- Sicherheitsrichtlinien (Security Compliance).

Im SAP-Hinweis 2253549 - The SAP Security Baseline Template (S-User notwendig) (siehe [SECNOTE]) finden sich aktuelle Hinweise zum SAP Security Baseline Template.

Alle Maßnahmen und Empfehlungen aus den vorliegenden Umsetungshinweisen sollten gemeinsam mit den genannten SAP-Dokumentationen betrachtet werden. Die angegebenen SAP-Hinweise (SAP-Notes, OSS-Hinweise) sind im SAP Support Portal (siehe [SECNOTE]) zu finden.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins APP.4.2 *SAP-ERP-SYSTEM* sowie für weitere Bausteinen aufgeführt, die hiermit im Zusammenhang stehen:

OPS.1.1.3 *Patch- und Änderungsmanagement*

OPS.1.1.5 *Protokollierung*

Diese zusätzlichen Maßnahmen sollten bei der Umsetzung der genannten Bausteine berücksichtigt werden. Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein APP.4.2 SAP-ERP-System

APP.4.2.M1 Sichere Konfiguration des SAP-ABAP-Stacks (B)

Die initiale Konfiguration des ABAP-Stacks ist aufwändig und umfasst viele Einzelschritte. Der Aufwand erhöht sich, wenn neben der Konfiguration der SAP-Basis auch Applikationen und Module konfiguriert werden müssen. Im Folgenden werden die wichtigsten Schritte dargestellt, die bei der initialen Konfiguration des ABAP-Stacks durchzuführen sind. Dabei wird nur auf die sichere Konfiguration der SAP-Basis eingegangen.

Mandanten für den Betrieb festlegen

Zunächst muss ein Mandant für den Betrieb des SAP-ERP-Systems festgelegt werden. Als Mandant (engl. Client) wird in einem SAP-ERP-System eine technische Unterteilung verstanden und darf nicht mit dem Mandantenbegriff im Sinne von Kunde verwechselt werden. Nach der Installation dürfen die existierenden Standardmandanten mit den Nummern 000 (SAP Referenzmandant), 001 (Produktionsvorbereitungsmandant) und 066 (Earlywatch-Mandant) nicht genutzt werden. Nachdem die für den Betrieb erforderlichen Mandanten aufgebaut worden sind, sollten vor regulärer Inbetriebnahme des Systems die Mandanten 001 und 066 gelöscht werden (siehe SAP-Hinweis 1749142 - Entfernen ungenutzter Mandanten wie Mandant 001 und 066 [SECNOTE]).

Ein SAP-ERP-System kann mehrere Mandanten mit unterschiedlichen Verwendungszwecken enthalten. Alle Mandanten eines SAP-ERP-Systems hängen jedoch über den SAP-Referenzmandanten zusammen, in dem Konfigurationen erfolgen, die global für das gesamte SAP-ERP-System gelten.

Mandanten mit sehr unterschiedlichen Sicherheitsanforderungen sollten nicht zusammen in einem SAP-ERP-System betrieben werden. So darf etwa ein Produktivmandant nie zusammen mit einem Entwicklungsmandanten in einem SAP-ERP-System ausgeführt werden.

Sicherheitsrelevante IMG-Aktivitäten durchführen (Customizing)

Der SAP Implementation Guide (IMG, SAP Reference IMG) ist eine von SAP vordefinierte, systeminterne Liste mit Konfigurationsschritten für ein SAP-ERP-System. Sie ist hierarchisch aufgebaut und jeweils auf die verwendete Systemversion und die installierten Komponenten abgestimmt. Daneben ist es möglich, eigene IMGs zu erstellen (Projekt IMGs), in denen nur die im Rahmen der Systemverwendung notwendigen Konfigurationsschritte aus dem SAP Reference IMG enthalten sind. IMGs bieten zudem die Möglichkeit festzuhalten, welche Konfigurationen bereits durchgeführt wurden. Folgende Aktivitäten sind im IMG durchzuführen:

- Aktivierung oder Deaktivierung der HTTP-Services, falls diese für den späteren Einsatz nicht benötigt werden (Transaktion: SICF, siehe APP.4.2.M24 *Aktivierung und Absicherung des Internet Communication Frameworks (ICF)*)
- Vergeben von Berechtigungen für RFC-Schnittstellen (Transaktion PFCG, siehe APP.4.2.M8 *Absicherung der SAP RFC-Schnittstelle*)
- Content-Server-Administration (Transaktion: CSADMIN, siehe APP.4.2.M24 *Aktivierung und Absicherung des Internet Communication Frameworks (ICF)*)
- SAP Web Dispatcher konfigurieren (siehe dazu auch APP.4.2.M25 *Sichere Konfiguration des SAP Web Dispatchers*)

Alle Aktivitäten unter dem Stichwort "Systemadministration" sind durchzuführen.

Profilparameter anpassen

Profilparameter sollen das SAP-ERP-System vor Angriffen von außen schützen. Informationen zur Einstellung der Profilparameter sind in den folgenden Abschnitten beschrieben:

- Profilparameter zur Einstellung der Passwortsicherheit (siehe APP.4.2.M13 *SAP-Passwortsicherheit*)
- Profilparameter zur Absicherung der:
- Web Dispatcher (siehe APP.4.2.M25 *Sichere Konfiguration des SAP Web Dispatchers*)
- RFC-Schnittstelle (siehe APP.4.2.M8 *Absicherung der SAP RFC-Schnittstelle*)
- Message-Server (siehe APP.4.2.M9 *Absicherung und Überwachung des Message-Servers*)
- Konfiguration des Security Audit Logs (siehe APP.4.2.OPS.1.1.5.M3 *Konfiguration der Protokollierung auf System- und Netzebenen*)

Parameter mit dem Präfix auth/, login/, snc/ oder ssf sollten aus Sicherheitsperspektive immer besonders genau betrachtet werden. Sie lassen sich über die Transaktion RZ10 verwalten und über die Transaktion RSPFPAR anzeigen.

Systemänderbarkeit konfigurieren

Für Produktivsysteme wird empfohlen, die Systemänderbarkeit global auf nicht änderbar zu setzen. Damit können Änderungen nur noch über das Transportsystem eingespielt werden und somit nur über definierte Prozeduren und Abläufe erfolgen. Wichtig ist jedoch, einen geordneten Änderungsmanagementprozess zu definieren und einzuhalten.

Für Test- und Qualitätssicherungssysteme sollten die gleichen Einstellungen wie im Produktivsystem verwendet werden, also ebenfalls global nicht änderbar. Änderungen sind im Entwicklungssystem vorzunehmen und nach dem erfolgreichen Qualitätssicherungsprozess in das Produktivsystem zu transportieren.

Für Entwicklungssysteme sollten die Komponenten, die durch die Entwicklung nicht betroffen sind, ebenfalls auf nicht änderbar gesetzt werden. Die Komponenten, in denen entwickelt wird, müssen hingegen auf änderbar gesetzt werden.

Mandanten-Konfiguration durchführen

Es können auch einzelne Mandanten davor geschützt werden, dass sich ihre Eigenschaften verändern lassen. Diese Einstellung ist für alle produktiven Mandanten zu benutzen. Dadurch wird auch beeinflusst, ob Mandanten-Veränderungen automatisch aufgezeichnet werden, sodass Einstellungsveränderungen nach der Prüfung als Transportauftrag verfügbar sind und in andere Mandanten transportiert werden können, die mit den gleichen Einstellungen betrieben werden sollen. Die Einstellungen erfolgen über die Transaktion SCC4. Für die eigenen Produktivmandanten sind folgende Einstellungen empfohlen:

(Hinweis: Die angegebenen Bezeichnungen der Einstellungswerte finden sich so in der abgekürzten Schreibweise im SAP-ERP-System.)

- Rolle des Mandanten: Produktiv
- Änderungen und Transporte für mandantenabhängige Objekte: keine Änderung erlauben
- Änderungen an mandantenübergreifenden Objekten: keine Änderungen von Repository- und mand.unabh. Cust.-Obj.
- Schutz bezüglich Mandantenkopierer und Vergleichstool: Schutzstufe 2: kein Überschreiben, keine ext. Verfügbarkeit

Entsprechende Einstellungen sollten im Test- und Qualitätssicherungssystem gelten. Für andere Mandanten (Entwicklung, Schulung, Demo) sind die Einstellungen geeignet zu definieren.

Ausführbare Betriebssystemkommandos absichern

Die Kommandos werden mit den Betriebssystemrechten des technischen Betriebssystembenutzers ausgeführt, unter dem das SAP-ERP-System abläuft. Das sind in der Regel weitreichende Administratorrechte. Der Zugriff auf diese Funktion muss daher abgesichert werden. Insbesondere darf es nicht möglich sein, dass Kommandos angelegt oder verändert werden. Daher sollten folgende Hinweise umgesetzt werden:

- Die Berechtigungen, externe Betriebssystemkommandos auszuführen (Berechtigung S_LOG_COM) oder zu pflegen, (Berechtigung S_RZL_ADM mit ACTVT=01) sind restriktiv zu vergeben.
- Der Zugriff auf die Transaktion SM49 "Externe Betriebssystemkommandos ausführen" ist auf die berechtigten Administratoren einzuschränken.
- Der Zugriff auf die Transaktion SM69 "Externe Betriebssystemkommandos pflegen" ist auf die berechtigten Administratoren einzuschränken.
- Für Betriebssystemkommandos können Parameterwerte vorgegeben werden. Das verhindert, dass sich zusätzliche Parameter an die Kommandos anhängen lassen. Davon sollte Gebrauch gemacht werden. Dies trifft insbesondere für selbst definierte Kommandos zu.

Single-Sign-On sicher konfigurieren

Weitere Informationen zu diesem Thema finden sich in APP.4.2.M31 *Konfiguration von SAP Single-Sign-On*.

APP.4.2.M2 Sichere Konfiguration des SAP-JAVA-Stacks (B)

Mit dem Java-Stack eines SAP-ERP-Systems ist es möglich, Java-basierte Anwendungen einzusetzen. Der Java-Stack wird durch einen Applikationsserver gebildet, der die J2EE (Java 2 Enterprise Edition)-Spezifikation umsetzt. Im Vergleich zum ABAP-Stack gibt es unterschiedliche Sicherheitsmechanismen und -konzepte.

Im Folgenden werden die aus Sicherheitssicht wichtigsten Schritte aufgezeigt, die bei der initialen Konfiguration des Java-Stacks durchzuführen sind. Die Darstellung beschränkt sich auf die Konfiguration des Applikationsservers und geht damit nicht auf sonstige installierte Applikationen ein.

Java-Stack Installation

Die Installation des Java-Stacks auf einem SAP-ERP-System sollte nur durchgeführt werden, wenn Java-basierte Produkte oder Applikationen eingesetzt werden. Falls der Java-Stack nicht separat installiert werden kann und nicht genutzt wird , muss er so konfiguriert werden, dass darauf nicht zugegriffen werden kann. Dazu sollten alle Dienste des Java-Stacks deaktiviert werden.

Schulung zum Java-Stack

Administratoren des Java-Stacks müssen Kenntnisse in der Architektur und den Sicherheitskonzepten der J2EE-Architektur besitzen. Hier sind insbesondere Kenntnisse bezüglich der statischen Konfiguration der Sicherheit für J2EE-konforme Objekte notwendig, die über das Administrationswerkzeug durch den Administrator durchgeführt wird. Es kommt dabei ein rollenbasiertes Sicherheitskonzept zum Einsatz.

Zu beachten ist, dass SAP den J2EE Java Authentication and Authorization Service (JAAS) um die SAP-spezifischen User-Management- Engine- (UME)- Funktionen erweitert hat. Damit wurde die statische Konfiguration der Sicherheitseinstellungen um eine dynamische Konfigurationsmöglichkeit durch den Programmcode ergänzt, die über die UME gesteuert werden kann. In der UME können daher beispielsweise erlaubte Aktionen in den Programmen zu Rollen zusammengefasst werden. Benutzern kann dann diese Rolle zugeordnet werden, so dass sie damit die benötigten Berechtigungen erhalten.

Administratoren muss zudem bewusst sein, dass der Java-Stack mit einer separaten Benutzer- und Berechtigungsverwaltung ausgestattet ist, so dass hier immer administrative Aufgaben durchgeführt werden müssen. Dazu sollten sie die UME benutzen.

Unnötige Dienste abschalten

Der Java-Stack bietet viele Dienste an, die nicht alle in jedem Szenario benötigt werden. Daher sind aus Sicherheitsgründen alle nicht benötigten Dienste zu deaktivieren. Problematisch dabei ist, dass Dienste voneinander abhängig sein können. Es kann zudem zwischen Systemdiensten und Nicht-Systemdiensten unterschieden werden.

Die Administration, Konfiguration und das Monitoring der J2EE-Instanz erfolgt über den NetWeaver Administrator (NWA), den Nachfolger des Visual-Administrator-Tools. Durch Filter ist es möglich, Dienste im configtool abzuschalten. Dazu müssen folgende Schritte durchgeführt werden:

- Starten des configtool für die Datei:
  <SAP_install_dir>/<system_name>/<instance_name>/j2ee/configtool directory
- Expertenmodus wählen
- Konfigurationsvorlage oder eine relevante Instanz zum Hinzufügen der Filter wählen
- Filter wählen
- Es kann ausgewählt werden zwischen Start, Stopp oder Abschalten
- Komponente wählen (Service, Library, Applikation oder alle)
- Lieferanten der Komponente eingeben
- Namen der Komponente auswählen
- Durch Hinzufügen werden die benutzerdefinierten Regeln der Tabelle hinzugefügt
- In der Tabelle mit den benutzerdefinierten Aktionen Set auswählen und die Änderungen anwenden.

Systeminterne Schlüssel setzen oder neu erzeugen

Für den Betrieb von vertrauenswürdigen Umgebungen und SSL/TLS-Kommunikationen sollten die Systemschlüssel neu generiert werden.

APP.4.2.M3 Netzsicherheit (B)

Die Anwendungs- und Datenbankserver der SAP-Backendsysteme befinden sich in der Regel in der gleichen Netzzone, die vom internen Client-Netz getrennt sein sollte. Nur die erforderlichen Ports sollten zwischen dem Client-Netz und dem Applikationsservernetz geöffnet werden. Die folgenden Einstellungen sollten zur Absicherung des Netzes umgesetzt werden:

Isolierung des Netzes

Das SAP-Servernetz (High Security Area) muss vom Client-Netz (Internal Workstation Network) und von der demilitarisierten Zone (DMZ) über Firewalls getrennt werden. Nur für die erforderliche Konnektivität darf es erlaubt sein, die Firewall zu passieren. Vor allem die Zugriffe auf Datenbanken und auf Betriebssystemebenen müssen blockiert werden. Wenn der direkte Zugriff auf den Datenbankport von SAP-HANA-Systemen wegen Entwickler- oder Administriationstätigkeiten über das HANA Studio erfolgen muss (für Entwickler und Administratoren sollte vordringlich auf die SAP HANA WebIDE verwiesen werden), dann sollte dies nur über ein abgesichertes Administrationsnetz oder einen Terminalserver erfolgen.

Datenverschlüsselung

Die gesamte Kommunikation von nicht vertrauenswürdigen Netzen muss authentisiert und verschlüsselt werden. Das interne Netz (Internal Workstation Network) muss als nicht vertrauenswürdig angesehen werden, sofern nicht andere ausreichende Sicherheitsmechanismen vorhanden sind, die es als ein vertrauenswürdiges Netz kennzeichnen.

DMZ Authentisierung

Wenn der Zugang aus dem Internet erfolgt, muss dieser in der DMZ authentisiert und überprüft werden, bevor weitere Verbindungen zu oder Interaktionen mit den inneren Netzen möglich sind.

Absicherung des SAP-Routers

Alle SAP-Router müssen sicher konfiguriert und betrieben werden. Das schließt vor allem folgende Punkte ein:

- Alle anwendbaren Sicherheitshinweise für SAP-Router müssen implementiert werden und anstehende Sicherheitskorrekturen müssen regelmäßig aktualisiert und umgesetzt werden.
- Die SAP-Router-Routingtabelle muss eingerichtet und gewartet werden, damit der Zugriff beschränkt wird.
- Auf Betriebssystemebene müssen die ausführbaren Programme des SAP-Routers und auch die SAP-Router-Konfigurationsdaten (vor allem die Routing-Tabelle) vor unberechtigten und unerwünschten Änderungen geschützt werden.

Weitere Maßnahmen dazu sind in APP.4.2.M15 *Sichere Konfiguration des SAP-Routers beschrieben*.

Absicherung des Web Dispatchers

Alle SAP Web Dispatcher müssen sicher konfiguriert und betrieben werden. Eine ausführliche Beschreibung dazu ist in der APP.4.2.M25 *Sichere Konfiguration des SAP Web Dispatchers* beschrieben.

Administrativer Zugang

Der administrative Zugang ist für alle Arbeitsstationen einzuschränken, für die ein solcher Zugang geplant ist. Die Firewalls zwischen den Netzsegmenten müssen entsprechend konfiguriert werden. Alle administrativen Zugänge dürfen nur über eine authentisierte und verschlüsselte Verbindung erfolgen. Der Zugang darf nur auf Anfrage erfolgen, wenn die Verbindung nicht auf einer täglichen oder regelmäßigen Basis erforderlich ist.

APP.4.2.M4 Absicherung der ausgelieferten SAP-Standardbenutzer-Kennungen (B)

Es müssen alle Passwörter der ausgelieferten SAP-Standardbenutzer-Kennungen in jedem Mandanten geändert werden. Welche Einstellungen für die jeweiligen Standardbenutzer zu berücksichtigen sind, wird im Folgenden beschrieben:

SAP*

- Bevor der Benutzer SAP* abgesichert wird, sollte ein Notfallbenutzer eingerichtet werden.
- Der Benutzer muss in allen Mandanten über einen Benutzerstammsatz verfügen. Dieser muss gesperrt sein und die Berechtigungen müssen entzogen werden.
- Der Benutzer darf nicht gelöscht werden.
- Der Benutzer ist der Benutzergruppe SUPER zuzuordnen und das Passwort muss geändert werden.
- Protokollierung des Benutzers im Security Audit Log.
- Profilparameter login/no_automatic_user_sapstar muss auf 1 gesetzt werden.

DDIC

- Der Benutzer sollte in allen Mandanten, außer Mandant 000, abgegrenzt und gesperrt sein.
- Der Benutzer benötigt die Zuweisung des Profils SAP_ALL und ist grundsätzlich als hochprivilegierter User mit kritischen Berechtigungen zu betrachten.
- Benutzer der Benutzergruppe SUPER zuordnen und als Systembenutzer einstellen.
- Das Passwort muss geändert werden.
- Protokollierung des Benutzers im Security Audit Log.
- Mithilfe des Notallbenutzers kann DDIC auf einen Dialogbenutzer umgestellt werden.

TMSADM

- Das Passwort des Benutzers muss in allen Mandanten gleichzeitig geändert werden. Der Report TMS_UPDATE_PWD_OF_TMSADM kann auf dem Mandanten 000 ausgeführt werden.
- Benutzer der Benutzergruppe SUPER zuordnen.
- Der Benutzer TMSADM benötigt exakt die Berechtigungen des Profils S_A.TMSADM.
- Zum Ändern des Passwortes für TMSADM siehe auch SAP-Hinweis 1414256 - Ändern des TMSADM Kennwortes ist zu komplex (siehe [SECNOTE]).
- Der Benutzer sollte nur im Mandanten 000 angelegt sein. Wenn er über Mandantenkopien oder andere Verfahren in andere Mandanten gebracht wurde, sollte er dort gelöscht werden.

WF-BATCH

- Nach der automatischen Generierung des Benutzers ist das Passwort zu ändern und die Benutzergruppe SUPER zu wählen.

Standarduser im SAP Solution Manager

Der SAP Solution Manager wird für den Betrieb einer ERP-Landschaft benötigt, um diese warten zu können. Dazu wird der Solution Manager mit der ERP-Landschaft verbunden. Hierbei werden Benutzer generiert und teilweise mit bekannten Standardpasswörtern versehen. Daher sollte

- die Solution-Manager-Installation auf solche eventuell vorhandenen Konten geprüft werden (SMD_*, SMDAGENT_*, SOLMAN_*, SAPSUPPORT) und
- die Passwörter der generierten User sollten geändert werden.

CONTENTSERV

Falls am ERP-System ein Content-Server genutzt wird, sollte das Passwort dieses generierten Standardusers geändert werden.

EARLYWATCH

Dieser Benutzer ist veraltet und wird vom SAP-Support nicht mehr verwendet. Sofern er vorhanden ist, sollte

- zunächst geprüft werden, ob er gelöscht werden kann. Dasselbe gilt für den Mandanten 066 (siehe auch SAP-Hinweise 1897372- EarlyWatch Mandant 066 - Can Client 066 be deleted? und 1749142 - Entfernen ungenutzter Mandanten wie Mandant 001 und 066, [SECNOTE]).
- Falls der Benutzer noch verwendet wird, sollte beachten werden:
    - Benutzer der Benutzergruppe SUPER zuordnen und Passwort ändern.
    - Protokollierung des Benutzers im Security Audit Log.

SAPCPIC

Dieser Benutzer ist veraltet und wird überwiegend in SAP-ERP-Systemen nicht mehr verwendet. Sofern er vorhanden ist, sollte zunächst geprüft werden, ob er gelöscht werden kann.

Falls der Benutzer noch verwendet wird:

- Der Benutzer muss gesperrt werden, das Passwort ist zu ändern und es ist die Benutzergruppe SUPER zu wählen.
- Protokollierung des Benutzers im Security Audit Log.
- siehe auch SAP-Hinweis 29276 - An welchen Stellen sind Passwörter sichtbar (siehe [SECNOTE]).

Prüfung auf Passwortänderung

Der Report RSUSR003 (Ausführbar über die Transaktion SE38) enthält Informationen über die Standardbenutzer in allen Mandanten. Er überprüft die Standardbenutzer auf Existenz, Sperrstatus und Passwortänderungen. Weitere Hinweise dazu finden sich in APP.4.2.M13 *SAP-Passwortsicherheit*. Der SAP-Service Early Watch Alert kann ebenfalls die Informationen geben, ob das Standardpasswort geändert wurde oder nicht.

APP.4.2.M5 Konfiguration und Absicherung der SAP-Benutzerverwaltung (B)

Mit der Benutzerverwaltung im SAP-ERP-System werden die Benutzerstammsätze der Mitarbeiter angelegt. Für den Mitarbeiter werden z. B. Anmeldenamen, Passwort und Berechtigungsrollen definiert und zugeordnet. Mithilfe der Berechtigungsrollen kann der Mitarbeiter Aktivitäten im SAP-ERP-System durchführen. Für die Administration der SAP-Benutzerverwaltung ist der Benutzeradministrator verantwortlich. Benutzerstammsätze sind mandantenabhängig und müssten in jedem Mandanten separat gepflegt werden. Es gibt jedoch verschiedene Möglichkeiten eine Benutzerverwaltung im SAP-ERP-System zu nutzen. Diese werden im Folgenden kurz vorgestellt.

Zentrale Benutzerverwaltung (ZBV)

Die Benutzerstammsätze werden über ein zentrales System (Zentralsystem) gepflegt und Änderungen automatisch an die angeschlossenen Tochtersysteme übertragen. Daten werden als asynchrone Kommunikation über eine Application-Link-Enabling-Landschaft (ALE-Landschaft) verteilt. Werkzeuge dafür sind die Transaktionen: PFCG, SM59, SU01, SCUA, SCUM, SCUG, SUGR, SCUL, SUIM.

Benutzerverwaltung ohne ZBV

Aufgrund der Mandantenabhängigkeit muss jedes System separat gepflegt werden. Der Transport von Benutzerstammsätzen ist nicht möglich, aber sie können mit dem Mandantenkopierer kopiert werden. Werkzeuge dafür sind die Transaktionen: SU01, SU10, SUIM.

Benutzerverwaltung des Application Server Java (AS Java)

Die Benutzerverwaltung im AS Java wird als Service über die integrierte User Management Engine (UME) bereitgestellt. Abhängig von der Konfiguration werden folgende Benutzerspeicher unterstützt: Datenbank, LDAP Directory und AS ABAP.

Benutzerverwaltung mit SAP NetWeaver Identity Management (SAP IdM)

Benutzerstammsätze und Berechtigungen werden zentral und automatisch über das IdM verwaltet und gesteuert. SAP IdM basiert auf der AS Java Plattform und ist ein eigenständiges Produkt. Im Zusammenspiel mit SAP Access Control (SAP AC) erfolgt die Benutzeradministration und Zuweisung durch Prüfung von SAP-Berechtigungen gemäß bestehenden Compliance-Anforderungen.

Benutzerverwaltung in der SAP HANA

Die Datenbankmanagementsystem-(DBMS)-Benutzer auf SAP HANA werden über einen Mandaten des AS ABAP verwaltet.

Benutzertypen im SAP-ERP-System AS ABAP

Wenn ein neuer Benutzer im SAP-ERP-System angelegt wird, kann zwischen verschiedenen Benutzertypen ausgewählt werden. Der Benutzertyp wirkt sich auf das Anmeldeverhalten und die hinterlegten Passwortregeln aus. SAP definiert fünf verschiedene Benutzertypen:

- **Dialogbenutzer**: Der Dialogbenutzer meldet sich direkt in der SAP GUI des SAP-ERP-Systems mittels Benutzername und Kennwort an (Dialoganmeldung). Setzt der Benutzeradministrator das Passwort, hat es den Status Initial und der Benutzer setzt es durch die Passwortänderung bei Anmeldung auf Produktiv. Mehrfachanmeldungen sind nur mit bestimmten Konfigurationen möglich.
- **Systembenutzer**: Eine Dialoganmeldung ist beim Systembenutzer nicht möglich. Die Anmeldung erfolgt anonym und über den RFC-Aufruf. Systembenutzer werden für technische Abläufe, wie die Hintergrundverarbeitung und Kommunikation, innerhalb eines Systems verwendet. Lediglich der Benutzeradministrator ändert das Passwort und es hat immer den Status "Produktiv". Mehrfachanmeldungen sind immer möglich.
- **Kommunikationsbenutzer**: Kommunikationsbenutzer werden von verschiedenen Benutzern verwendet, um sich von außen über den RFC-Aufruf im SAP-ERP-System anzumelden. Der Benutzeradministrator ändert das Passwort (Status Initial), aber der Benutzer muss es beim RFC-Aufruf nicht ändern. Mehrfachanmeldungen sind immer möglich.
- **Servicebenutzer**: Servicebenutzer des Benutzertyps Service sind mehreren Personen zugeordnet. Dieser wird für anonyme Systemzugänge verwendet, z. B. für Webservices. Die Passwortregeln prüft das System nicht, aber Mehrfachanmeldungen sind immer möglich. Nur der Benutzeradministrator kann das Passwort ändern, das immer den Status "Produktiv" hat.
- **Referenzbenutzer**: Der Referenzbenutzer kann sich nicht am SAP-ERP-System anmelden. Er wird einem Dialogbenutzer zugewiesen und vererbt seine zusätzlichen Berechtigungen an ihn. So wird es ermöglicht, bestimmte Berechtigungsprüfungen durchzuführen. Das Passwort ist immer deaktiviert.

Maßnahmen für eine sichere Administration der Benutzer-IDs im SAP-ERP-System

Systemzugriffe sind nur autorisierten Personen gestattet, die sich im SAP-ERP-System mit einer Benutzer-ID und einem gültigen Passwort authentisieren müssen. Unberechtigte Systemzugriffe können durch bestimmte Sicherheitsmechanismen verhindert werden. Benutzeradministratoren sollten sich an folgende Empfehlung halten:

- Jede Benutzer-ID ist einer realen Person zugeordnet.
- Es sollten keine Sammelkonten angelegt werden.
- Aufgrund der Mandantenabhängigkeit von Benutzerstammsätzen sollte in jedem System die selbe Benutzer-ID vergeben werden.

- Benutzer-IDs müssen eindeutig sein. Es ist eine Namenskonvention zu definieren. Oftmals besitzen Mitarbeiter eine eindeutige Identifikationsnummer, diese kann auch als Benutzer-ID übernommen werden.
- Benutzer sollten einer bestimmten Benutzergruppe wie Internen, Externen, Partnern oder technischen Benutzern zugeordnet werden (siehe SAP-Hinweis 1663177 - SU01: Benutzergruppe als Pflichtfeld, [SECNOTE]).
- Einschränkung des Zeichenvorrats für den Benutzernamen, damit ein Name nicht nur aus "alternativen" Leerzeichen besteht (siehe SAP-Hinweis 1731549 - Einschränkungen des Zeichenvorrates für Benutzernamen, [SECNOTE]).
- Die Zuordnung der Berechtigungsprofile SAP_ALL und SAP_NEW muss vermieden werden. SAP_ALL sollte außer Notfallbenutzerkonten keine Benutzer zugewiesen bekommen. Diese Konten sollten dann ausreichend kontrolliert und überwacht werden. SAP_NEW sollte beispielsweise nur für den technischen Teil des Release-Upgrades genutzt werden.

Vorteile numerischer Benutzer-IDs

Es ist sinnvoll numerische Benutzer-IDs zu verwenden, da sie folgende Vorteile haben:

- Groß- und Kleinschreibung werden nicht verwechselt, wenn Benutzer-IDs nur aus numerischen Zeichen bestehen.
- Numerische Benutzer-IDs reflektieren den Realnamen einer Person nicht und können auch nicht direkt zugeordnet werden.
- Keine Änderung der numerischen Benutzer-ID bei Namensänderungen.
- Anhand der Nummernkreise für Benutzerkennungen werden grobe Zuordnungen durchgeführt.

Weitere Maßnahmen in der Benutzerverwaltung

Inaktive Benutzer im SAP-ERP-System sollten gesperrt oder ungültig gesetzt werden. Mit dem Report RSUSR_LOCK_USER können Administratoren inaktive Benutzer automatisch sperren lassen. Auch sollte regelmäßig ein Benutzerabgleich durchgeführt werden. Damit wird verhindert, dass die Zuordnung der Profile zu den Benutzern veraltet ist. Das kann entweder mit der Transaktion PFUD durchgeführt werden oder mit dem Report RHAUTUPD_NEW, der den Hintergrundjob PFCG_TIME_DEPENDENCY einplant. Benutzer, die über einen längeren Zeitraum auf dem SAP-ERP-System nicht aktiv waren, sollten automatisch abgemeldet werden. Dazu muss der Profilparameter rdisp/gui_auto_logout in der Transaktion RZ10 mit der entsprechenden Zeit eingestellt werden (in Sekunden).

APP.4.2.M6 Erstellung und Umsetzung eines Benutzer- und Berechtigungskonzeptes (B)

Die Funktionen eines SAP-ERP-Systems werden über Transaktionen aufgerufen, die dabei unterschiedliche Operationen oder Aktivitäten auf Daten ausführen können. Die über Transaktionen gestarteten Applikationen prüfen, ob der aufrufende Benutzer über die notwendigen Berechtigungen verfügt, die angeforderte Operation auf den durch die Applikation angesprochenen Daten auszuführen.

Prinzipien

Im ersten Schritt werden die grundlegenden Prinzipien vorgestellt, die für ein SAP-Berechtigungskonzept relevant sind:

Identitätsprinzip

Natürliche Personen, die im SAP-ERP-System einen Benutzer erhalten, müssen eindeutig zugeordnet werden. Handelt es sich um einen technischen Benutzer im SAP-ERP-System, muss nachvollziehbar sein, welche natürliche Person ihn verwendet hat. Es gilt zu vermeiden, dass eine natürliche Person im

SAP-ERP-System viele unterschiedliche SAP-Benutzer erhält. Zur Vermeidung von systemübergreifenden Zugriffsrisiken sollte ein systemübergreifendes Benutzer-Mapping erstellt werden. Mit dem Identity-Management-Konzept kann im SAP-ERP-System umgesetzt werden, dass eine SAP-Benutzer-ID systemübergreifend verteilt wird.

Minimalprinzip

Es werden nur die Transaktionen und Zugriffe für einen Benutzer berechtigt, die für den Benutzer zur Erfüllung seiner Tätigkeiten wirklich notwendig sind. Das Minimalprinzip muss in Bezug auf Datenqualität (z. B. Name, Wohnsitz, E-Mail Adressen, Kontodaten, Ware) dem organisatorischen Bezug (z .B. zuständige Landesorganisation) und den zeitlichen Bezug (z. B. Bestellzeitpunkt, Jahr der Bestellung) eingehalten werden. Beispielsweise benötigen Mitarbeiter im Versand nur die Informationen über die Bestellungen und nicht Informationen über Kontodaten.

Stellenprinzip

Alle natürlichen Personen, die einen Benutzer im SAP-ERP-System erhalten, müssen einer definierten Funktion in der Organisation zugeordnet sein. Zum einen dient die Form einer Aufbauorganisation, da sich grundsätzlich alle Aufgaben in Stellen definieren lassen. Das ist aber nicht zwingend Voraussetzung für das Stellenprinzip (Zuordnung über Organisationsmanagement).

Belegprinzip der Buchhaltung

Alle zahlungsrelevanten und bilanzwirksamen Vorgänge müssen gemäß dem Prinzip der Buchhaltung (in Deutschland: GoB) nachvollziehbar sein und für jedes Berechtigungsprinzip sichergestellt werden. Es muss ersichtlich sein, wer der Erfasser und Änderer des Beleges ist. Alle Zugriffe auf die Datenbank, die einen Beleg erzeugen, und jede dazugehörige Aktion (z. B. erfassen, ändern, löschen) umfassen das Belegprinzip.

Belegprinzip der Berechtigungsverwaltung

Alle relevanten Daten von Benutzern müssen gemäß der definierten Aufbewahrungsfrist gesichert und aufbewahrt werden. Folgende Informationen müssen aufbewahrt werden: die Zuordnung des Benutzers zu einer natürlichen Person, die Zuweisung von Berechtigungen, Art, Umfang, Änderungen und Änderer der Berechtigungen.

Funktionstrennungsprinzip

Mit dem Funktionstrennungsprinzip, auch Segration of Duties (SoD) genannt, wird gewährleistet, dass Benutzer nicht alle Prozesse in einem SAP-ERP-System allein ausführen können. Das Prinzip der Funktionstrennung muss beispielsweise in der Benutzer- und Berechtigungsadministration eingehalten werden. Administratoren, die in der Benutzerverwaltung zuständig sind, sollten nicht SAP-Berechtigungsrollen erstellen. Bei kleineren Institutionen kann ein Funktionstrennungsprinzip teilweise nicht durchgeführt werden. In dem Fall sollten kompensierende Kontrollen (auch mitigation controls) eingesetzt werden. Diese Kontrollen müssen in regelmäßigen Abständen geprüft werden.

Genehmigungsprinzip

Mit dem Genehmigungsprinzip wird veranlasst, dass Berechtigungen genehmigt werden müssen, bevor die Berechtigungsrollen erstellt oder sie einem Benutzer zugeordnet werden.

Bevor Berechtigungen an Benutzer vergeben werden, müssen diese nachvollziehbar genehmigt werden. Die Genehmigung sollte durch eine definierte Stelle durchgeführt werden. Es kann zwischen einer implizierten und explizierten Genehmigung unterschieden werden. Eine implizierte Genehmigung ist die indirekte Zuordnung von Berechtigungen, d. h. Berechtigungen werden ausschließlich über ein technisch definiertes Stellenkonzept vergeben. Die explizierte Genehmigung ist die direkte Vergabe einer Berechtigung an einen Benutzer.

Die Genehmigung eines Rollenantrags für einen SAP-Dialogbenutzer sollte nach dem Vier-Augen-Prinzip erfolgen. Wer welche Genehmigung für welchen Prozess durchführt, muss von der Institution definiert werden. Im ersten Schritt kann es der Vorgesetzte des SAP-Dialogbenutzers sein und im zweiten Schritt kann es der Prozessinhaber der angeforderten Rolle sein.

Genehmiger von Rollenzuordnungen

Die Genehmiger von Rollenzuordnungen sind für die Vergabe von Benutzerrechten verantwortlich. Sie genehmigen die Freigabe und den Entzug von Benutzerrollen für einzelne Benutzer im SAP-ERP-System. Die Genehmiger sollten die folgenden Kenntnisse im SAP-ERP-System besitzen:

- Kenntnis der betroffenen SAP-Prozesse,
- Kenntnis der organisatorischen Aufbau- und Ablauforganisation,
- Kenntnis der Aufgaben und Organisationsstruktur der jeweiligen Anwender,
- Kenntnis des Inhaltes der bestehenden Benutzerrollen in ihrem Verantwortungsbereich.

Der Genehmiger legt für die Rollen seines Verantwortungsbereiches fest, welche Benutzer, einschließlich der Geschäftspartner, welche Aufgaben im SAP-ERP-System durchführen dürfen. Die eingetragenen Benutzerstämme sollten im Produktivsystem regelmäßig (z. B. einmal im Quartal) auf ihre Aktualität geprüft werden. Die Prüfunterlagen sind zehn Jahre lang aufbewahrungspflichtig.

Standardprinzip

Zur Vereinfachung des Berechtigungskonzeptes ist notwendig, dass technische Standards eingehalten werden. Lösungen und Risiken werden anhand des Standards definiert. Wird vom Standard abgewichen, kann das weitreichende Folgen für die Sicherheit des Berechtigungskonzeptes haben. Alle Änderungen die vom Standard abweichen, müssen immer dokumentiert werden.

Schriftformprinzip

In der Institution muss das genehmigte Berechtigungskonzept schriftlich vorliegen. Des Weiteren muss das Konzept für Externe nachvollziehbar und verständlich sein. Es sollte Auskunft über die technische Realisierung, die betriebswirtschaftliche Nutzung der Berechtigungen, und der Umsetzung der normativen Grundlagen geben.

Kontrollprinzip

Die Umsetzung des Berechtigungskonzeptes muss durch Kontrollen innerhalb der Berechtigungsadministration sowie durch neutrale Prüfer überprüft werden. Die folgenden Punkte sollten mit dem Berechtigungskonzept kompatibel sein:

- technische Standards im System
- Ausprägungen der Berechtigungen
- Zuordnung der Benutzer
- Passwortregeln
- Anzahl der inaktiven Benutzer
- Anzahl der gesperrten Benutzer
- Unbekannt-Sperrungen aufgrund von Falschanmeldungen

Rahmenbedingungen

Über diese Prinzipien hinaus sollten beim Aufbau eines Berechtigungskonzeptes die folgenden Rahmenbedingungen berücksichtigt werden:

- datenschutzrechtliche Bestimmungen,
- Gesetzliche Rahmenbedingungen wie die Grundsätze ordnungsmäßiger Buchführung (GoB), das Handelsgesetzbuch (HGB), International Financial Reporting Standard (IFRS) oder Sarbanes Oxley Act (SOX),
- Konzernvorgaben,
- Anforderungen der internen Qualitätsmanagementsysteme.

Grundbegriffe

Die wichtigsten Begriffe im Zusammenhang mit dem SAP-Berechtigungskonzept sind:

- **PFCG Einzelrolle**: Die Erstellung und Änderung der Rollen erfolgt mit dem Profilgenerator (Transaktion PFCG). Mit dem Profilgenerator wird ein Berechtigungsprofil automatisch generiert.
- **Businessrolle**: Beschreibt den Arbeitsplatz eines Benutzers und beinhaltet alle dafür notwendigen (Sammel-)rollen in den Systemen, in denen der Benutzer Berechtigungen für den Arbeitsplatz benötigt.
- **Berechtigungsobjektklasse**: Logische Zusammenfassung von Berechtigungsobjekten, z. B. alle Berechtigungsobjekte der Finanzbuchhaltung beginnend mit "F_" werden zur Objektklasse FI gezählt.
- **Berechtigungsobjekt**: Im Programmcode wird zur Berechtigungsprüfung das technische Objekt aufgerufen und gegen den Benutzerpuffer geprüft. Das Berechtigungsobjekt fasst 1 bis 10 Berechtigungsfelder zusammen, die in Kombination als UND-Verknüpfung geprüft werden.
- **Berechtigungsfeld**: Ist ein Bestandteil des Berechtigungsobjekts und die kleinste Einheit mit Werten wie Lesen, Ändern, Anlegen.
- **Berechtigungsprofil**: Sobald eine Rolle generiert wurde, wird automatisch das dazugehörige Berechtigungsprofil erstellt, das die Ausprägung der einzelnen Berechtigungsobjekte (Werte) enthält.
- **Benutzer**: Meldet sich im SAP-ERP-System an und erhält über die Zuordnung der Berechtigungsprofile Zugriff auf Funktionen und Objekte.
- **Benutzertyp**: Der klassische Endanwender ist ein Dialog-Benutzer. Im SAP-ERP-System gibt es z. B. noch Servicebenutzer, Systembenutzer und Kommunikationsbenutzer.

Umsetzung

Wenn ein Berechtigungskonzept entwickelt wird, gibt es dabei viele Herausforderungen, die von den SAP-Berechtigungsadministratoren zu lösen sind. So steigt beispielsweise die Anzahl der Rollen mit der Anforderung nach organisatorischer Trennung, aber auf der anderen Seite wird in den Geschäftsanforderungen die Abgrenzung in reine Organisationseinheiten gefordert. Gleiches gilt für die Rollen der Mitarbeiter. Es gibt viele unterschiedliche Rollen für die gleichen Arbeitsplätze aufgrund der individuellen Aufgaben der Mitarbeiter, was wieder zu einer hohen Rollenanzahl im SAP-ERP-System führt.

SAP hat daher einen Best-Practice-Ansatz für ein SAP-Berechtigungskonzept entwickelt. Die folgenden Schritte unterstützen Benutzer- und Berechtigungsadministratoren bei der Erstellung des Konzeptes:

1. Erstellen eines Projektplans
2. Erstellen eines Berechtigungsrahmenkonzepts
3. Definition der Namenskonventionen
4. Definition der Einzelrollen
5. Identifizierung kritischer Berechtigungen oder Berechtigungskombinationen
6. Definition der Orglevel-Sets
7. Definition der Sammelrollen
8. Rollen-Konsolidierung
9. Definition der Rollenverantwortlichen
10. Implementierung und Test
11. Zuordnung zu Benutzern

Grundsätzlich muss die Trennung der Verantwortlichkeiten im Berechtigungswesen eingehalten werden. Es muss einen Benutzeradministrator, einen Berechtigungsadministrator und eventuell einen Profiladministrator geben. Die Administratoren sollten Benutzergruppen zugeordnet werden, die von ihnen selbst nicht verändert werden können (Vier-Augen-Prinzip), d. h. in den Rollen der Administratoren sollte die Pflegeberechtigung für diese Gruppen nicht enthalten sein.

Folgende Punkte müssen für die Umsetzung eines Benutzer- und Berechtigungskonzepts noch beachtet werden:

Profilgenerator

Mit dem Profilgenerator (Transaktion PFCG) werden die SAP-Rollen und deren Berechtigungsdaten gepflegt. Der Profilgenerator wird als Standardwerkzeug zur Rollenpflege eingesetzt. Die Funktionen des Profilgenerators erleichtern die Pflege der SAP-Rollen, indem sie verschiedene Prozesse automatisieren und der Umsetzung des Berechtigungskonzepts mehr Flexibilität verleihen. Es wird empfohlen, im Profilgenerator jede Änderung an einer SAP-Rolle im Feld Langtext der Beschreibungskarte zu dokumentieren.

Berechtigungsprüfung der Berechtigungsobjekte

Die Prüfung der Berechtigungsobjekte erfolgt im ABAP-Code über die Anweisung AUTHORITY-CHECK. Es wird überprüft, ob der Benutzer in seinem Benutzerstammsatz über die entsprechenden Berechtigungen verfügt, die im AUTHORITY-CHECK als Bedingung hinterlegt sind. Kundeneigene Berechtigungsobjekte müssen in der Transaktion SU21 und Berechtigungsfelder in der Transaktion SU20 angelegt werden. Diese kundeneigenen Berechtigungsobjekte können bis zu zehn Felder enthalten.

SU24 - Vorschlagswerte Profilgenerator

Für die Pflege der SAP-Berechtigungsrollen wird die Anwendung der Transaktion SU24 empfohlen. Innerhalb von SU24 werden Vorschlagswerte und Prüfkennzeichen (inklusive dem globalen Deaktivieren von Berechtigungsprüfungen) gepflegt. In einem Konzept muss ausführlich beschrieben werden, wie SU24 genutzt werden soll. Die Transaktion SU24 bedeutet initial zusätzlichen Aufwand, allerdings ist es dadurch deutlich einfacher, die SAP-Berechtigungsrollen zu pflegen. Weitere Vorteile sind:

- vermeidet wiederholende Berechtigungsfehler,
- SAP-Standard,
- dokumentiert benötigte Berechtigungen,
- unterstützt den Rollenentwicklungsprozess,
- erleichtert die Anpassung des Berechtigungskonzepts während eines Upgrades erheblich sowie
- Vorschlagswerte werden auch in der Risikodefinition von Access Control verwendet.

In der Transaktion SU24 werden nicht nur die Transaktionen gepflegt, sondern unter anderem auch RFC-Bausteine oder Web-Dynpro-Anwendungen. Die Vorschlagswerte können auch über Traceauswertungen bezogen werden, entweder mit dem Systemtrace oder dem Langzeittrace.

Systemtrace (ST01, STAUTHTRACE) und Langzeittraces (STUSOBTRACE, STUSERTRACE)

Mit dem Systemtrace werden alle Berechtigungsprüfungen, z. B. während eine Transaktion ausgeführt wird, mitgeschrieben und alle fehlgeschlagenen Berechtigungsprüfungen werden analysiert und angepasst. Folgendes ist zu beachten:

- Der Trace wird im Kernel aufgezeichnet und beeinflusst daher die Performance des ganzen SAP-ERP-Systems. Der Trace sollte nur für ausgewählte Benutzer oder über einen kurzen Zeitraum laufen.
- Der Trace darf nicht ohne Wissen der aufzuzeichnenden Benutzers eingeschaltet werden: Leistungs- und Verhaltenskontrolle.

- Der Trace ist applikationsserverspezifisch und muss daher auf allen Servern eingeschaltet werden.

Um Berechtigungserfordernisse zu ermitteln, die sich nicht direkt aus unmittelbaren Tests von ausführenden Dialogusern ergeben, ist der Systemtrace wenig effizient. In solchen Fällen sollten alternativ Langzeittraces verwendet werden. Folgendes ist zu beachten:

- Die Langzeittraces werden nicht, wie der Systemtrace, auf Dateisystemebene geschrieben, sondern in die Datenbank. Das beeinträchtigt die Performance mehr als der Systemtrace. Daher sollten Langzeittraces nur mit Filter eingeschaltet werden.
- STUSOBTRACE: Systemweit, mandantenübergreifend, benutzerunabhängig, jede Berechtigungsprüfung einer Programmstelle wird nur einmal erfasst. Es erfolgt also keine Erfassung von Benutzern mit Zeitstempeln.
- STUSERTRACE: Systemweit, mandanten- und benutzerabhängig, jede Berechtigungsprüfung einer Programmstelle wird pro Benutzer einmal mit dem ersten Zeitstempel erfasst.

Organisationsebenen

Die Organisationsebenen bilden die Unternehmensstruktur im SAP-ERP-System ab. Dabei bilden sie die Aufbauorganisation (z. B. Buchungskreis), die Ablauforganisation (z. B. Kontenplan) oder die technisch-organisatorischen Trennungen ab. In den Berechtigungsobjekten bilden Organisationsebenen spezielle Felder ab, die eine besondere Pflege ermöglichen. Es gibt Standard-Organisationsebenen und es ist möglich, kundeneigene Organisationsebenen zu definieren. Organisationsebenen sind komponentenspezifisch und stehen in Relation zueinander. Sie stellen Unterscheidungsmerkmale dar, nach denen Berechtigungen differenziert werden können.

Synchronisation mit dem Rollenkatalog im Fiori-Gateway und mit nativen HANA-Berechtigungen

Bei modernen S/4HANA-Systemen werden neben den Detailberechtigungen im ABAP-Backend auch Rollen für den Anwendungskatalog im Fiori-Gateway (Frontendsystem) benötigt. Diese müssen mit den Backendrollen abgestimmt sein, damit die Navigation auf dem Frontend zu den Berechtigungen auf die Businessdaten passt. In der PFCG gibt es hierzu Synchronisationsprozesse, die zu beachten sind. Darüber hinaus müssen bei der Einbettung nativer HANA-Applikationen entsprechend auch Benutzer und Berechtigungen passend zum Gesamtberechtigungskonzept auf der HANA-Datenbank erarbeitet und mit den Berechtigungen auf den Frontend- und Backendsystemen abgestimmt und synchron gehalten werden.

Prozesse der Berechtigungsadministration

Die folgenden Prozesse müssen im Rahmen der Berechtigungsadministration definiert werden: Rollen anlegen, Rollen ändern, Rollen löschen, Rollen transportieren und SU24-Vorschlagswerte transportieren. SAP-Berechtigungsrollen sollten nur im Entwicklungssystem angelegt und gepflegt werden. Sie werden mithilfe des Transport-Management-Systems (TMS) durch die verschiedenen Systemstufen transportiert.

Rollen und Profile können zusammen transportiert werden. Jedoch sind diese mandantenabhängig und müssen über Transportaufträge in die anderen Mandanten verteilt werden. Nach einem Transport muss der Benutzerstammsatz aktualisiert werden (Massenabgleich). Rollen können auch heruntergeladen und lokal gespeichert werden oder in einem anderen System wieder hochgeladen werden. SU24-Vorschlagswerte können mit allen Änderungen der USOBX_C und USOBT_C transportiert werden.

Definition der Arbeitsplatzrollen

Es werden Arbeitsplätze definiert und hierfür Mitarbeiter zugeordnet. Ein Ansatz ist es, für jeden Arbeitsplatz Businessrollen zu entwickeln, die alle für den Arbeitsplatz notwendigen Einzelrollen sowie Sammelrollen umfassen. Die Businessrolle wird allen Mitarbeitern eines Arbeitsplatzes zugeordnet. Kritische Funktionen, die nur von einigen Mitarbeitern eines Arbeitsplatzes ausgeführt werden sollen, sind in zusätzlichen Add-on-Sammelrollen enthalten. Beispiele für Businessrollen sind Lagermitarbeiter, Sachbearbeiter Vertrieb oder Einkaufsleiter.

Einhaltung der Funktionstrennung

Die Einhaltung der Funktionstrennung sollte mit der Berechtigungsvergabe nach dem Vier-Augen-Prinzip durchgeführt werden. Ein Benutzer darf immer nur einen Teilprozessschritt im Rahmen eines geschäftskritischen Prozesses ausführen. Um Betrug zu vermeiden, werden die Berechtigungen über verschiedene Benutzer verteilt.

Grundsätzlich sind Berechtigungen auf Stamm- und Bewegungsdaten voneinander zu trennen, z. B. Bestellungen aufgeben und Lieferantendaten ändern. Die Funktionstrennung definiert sich z. B. über Vorgaben von SOX (nicht verbindlich für Organisationen, die an der NASDAQ gelistet sind). SOX fordert die Definition von Risiken und die Auswertung und Kompensation von Konflikten. Ein kontinuierliches Monitoring auf die SoD-Konfliktfreiheit von Rollen und die Vergabe von kritischen Berechtigungen an Anwender sollte mit geeigneten Werkzeugen durchgeführt werden, um Abweichungen frühzeitig erkennen zu können. Mit dem Tool SAP Access Control können SAP-spezifische Risikoanalysen von Benutzer- und Rollenzuordnungen durchgeführt, geprüft und dokumentiert werden.

Definition von Berechtigungen für technische Benutzer

Neben der Berechtigung von Endanwendern werden in SAP-ERP-Systemen auch Berechtigungen für spezielle technische Konten, etwa für den Hintergrund- oder Schnittstellenbetrieb benötigt. Dabei sollte darauf geachtet werden, solche Konten jeweils szenarienbezogen auszugestalten und (nach Minimalprinzip) zu berechtigen. Es sollte vermieden werden, einen einzigen technischen Benutzer für viele Schnittstellen und Hintergrundjobs zu verwenden, da ein solcher Benutzer zu umfangreiche Berechtigungen hat und das Risiko einer Beeinträchtigung der Verfügbarkeit erheblich erhöht ist.

Aktivierung schaltbarer Berechtigungsprüfungen

Ausgewählte Berechtigungsprüfungen (insbesondere im Schnittstellenumfeld) werden von SAP als optional zuschaltbar ausgeliefert (SACF). Im Berechtigungskonzept muss bestimmt werden, welche Prüfungen aktiv geschaltet werden müssen und welche inaktiv verbleiben sollen.

Zusammenfassung der SAP-Berechtigungsrichtlinien:

- Positives Berechtigungskonzept: Alle Zugriffe und Aktionen müssen explizit erlaubt werden.
- Minimalprinzip: Es werden nur so viele Transaktionen und Zugriffe für einen Anwender berechtigt, wie er auch wirklich benötigt.
- Rollenbasiertes Berechtigungskonzept: Berechtigungen werden in den PFCG-Rollen angelegt, gespeichert und dem Benutzer zugeordnet.
- Funktionstrennung: Es sollten keine Funktionstrennungskonflikte in einzelnen Rollen vorhanden sein.
- Das Rollenkonzept orientiert sich an der Organisationsstruktur der Institution.
- Rollen werden nach Anzeige- und Änderungsberechtigung unterschieden.
- Alle Mitarbeiter der Institution, die innerhalb der Organisation dieselben Aufgaben haben, sollen auch mit denselben Berechtigungen arbeiten.
- Die Rollen unterscheiden sich nur in der Ausprägung der jeweiligen Organisationsebenen.
- Trennung der Verantwortlichkeiten. Es muss einen extra Berechtigungsadministrator geben.
- Es muss ein Notfallkonzept erstellt werden, falls im Produktivsystem Berechtigungsprobleme auftreten oder im Customizing Änderungen durchgeführt werden müssen (siehe APP.4.2.M28 *Erstellung eines Notfallkonzeptes* und APP.4.2.M29 *Einrichten eines Notfallbenutzers*).
- Vollständigkeit: Das Rollen- und Berechtigungsdesign muss auch den Betrieb technischer Konten abdecken, also auch die Berechtigung von Hintergrund- und Schnittstellenbenutzern. Auch für diese ist das Minimalprinzip zu gewährleisten.

APP.4.2.M7 Absicherung der SAP-Datenbanken (B)

Auf Datenbanken kann mittels SAP-Tools und Software von Drittherstellern zugegriffen werden. Generell wird empfohlen, dafür SAP-Tools zu benutzen.

Es ist notwendig, die Passwörter für die Standardbenutzer der Datenbank zu ändern, da SAP diese im Klartext ausliefert. Das Standardpasswort für die Benutzer SAPR3 oder SAP<SID> muss immer geändert werden. Zum Schutz der Standardbenutzer müssen folgende Maßnahmen umgesetzt werden:

- Standardpasswörter sollten nicht übernommen werden.
- Sichere Passwörter sollten verwendet werden.
- Wird das DBM-Benutzerkonto vorübergehend genutzt, ist ein zweites temporäres Passwort für den DBR-Benutzer zuzuweisen.
- Um Passwörter für SAP MaxDB Standardbenutzer zu ändern, sollte das Datenbankwerkzeug Database Manager CLI oder das Computing Center Management System (CCMS) genutzt werden.

Des Weiteren muss der Zugriff auf die folgenden Tabellen für andere Datenbankbenutzer unterbunden werden:

- USR* Tabellen
- T000 Tabelle (keine Schreibrechte)
- Allgemeine Tabellen (wie SAPUSER oder RFCDES) oder anwendungsspezifische Tabellen (wie PA* oder HCL*)

Wird auf Daten in der Datenbank mittels Software von Drittherstellern zugegriffen, müssen bestimmte Sicherheitsmaßnahmen durchgeführt werden. Die Benutzer SAPR3 oder SAP<SID> sind nicht zur Verbindung zur Datenbank zu nutzen. Dafür sollten andere Benutzer erstellt werden, die besonders zu pflegen sind:

- die Zugriffsrechte auf die erforderlichen Tabellen sind einzuschränken,
- nur lesender Zugriff sowie
- kein Benutzer sollte die Berechtigung erhalten, alle Tabellen pflegen zu können.

Ebenfalls ist darauf zu achten, dass bei Nutzung von Software von Drittherstellern keine Schäden in Bezug auf die Sicherheit der Konsistenz oder Berechtigung der Datenbank erfolgt.

Authentisierung und Verschlüsselung der Datenbanken

Nach der Installation müssen die Systemschlüssel auf individuelle Werte geändert werden (SAP HANA: Master Encryption Key ändern). Um den Authentisierungsprozess sowie die Kommunikation abzusichern, gibt es die folgenden Methoden:

- Es ist der Verschlüsselungsmechanismus zu verwenden, der von den proprietären Datenbanktreibern zur Verfügung gestellt wird.
- Es sind Betriebssystemmethoden oder Anwendungsmethoden wie zum Beispiel SSH oder SSL-Tunnel zu verwenden.
- Applikations- und Datenbankserver sollten in einem separaten Sicherheitsnetzsegment abgelegt werden. Die Überwachung des Netzverkehrs sollte erschwert werden.
- Die Verschlüsselung in solch einem Netzsegment ist nicht zwingend erforderlich, wird aber empfohlen.
- Es sollte SSF für die ABAP-Technologie verwendet werden.

SAP MaxDB Sicherheit

Die verantwortlichen Datenbankadministratoren sollten für die Absicherung der SAP MaxDB folgende Einstellungen vornehmen:

- Die Passwörter der Datenbankbenutzer müssen entsprechend den Passwortrichtlinien der Institution gepflegt sein. Das betrifft vor allem die Standardpasswörter der Benutzer DBADMIN, DBA und DBM. Das Standardpasswort muss geändert werden.
- Es ist ein Benutzer- und Berechtigungskonzept für die Datenbankbenutzer zu definieren und zu implementieren.
- Software und Funktionen sind auf das erforderliche Minimum zu begrenzen:
- Es ist nur Software zu installieren, die wirklich benötigt wird.
- Die Global Listener und SAP MaxDB Server sind für die lokale Kommunikation abzuschalten.
- Der SAP MaxDB X Server ist ohne NI Support (Unix und Linux) zu starten.
- Demo Daten sind zu entfernen.
- Trace- und Logdateien:
- Tracedateien sind nur zur Suche von Fehlern zu benutzen. Alle Tracedateien sind zu entfernen und das Schreiben des Traces ist zu deaktivieren, nachdem die Auswertung beendet wurde.
- Der Zugriff auf Logdateien ist zu beschränken.
- Der Zugriff auf Betriebssystembefehle und -funktionen ist zu beschränken.
- Die Serverberechtigungen zum Lesen von Datenbankdateien sind bei allen DBM-Betreibern zu entziehen, um den Zugriff auf Logdateien zu unterbinden.
- Im Datenbankmanager CLI sind die DBFileRead Serverberechtigungen zu entziehen.

Oracle DB Sicherheit

Zur Absicherung einer Oracle-Datenbank müssen die Passwörter nach den Richtlinien der Passwortsicherheit geändert werden. Das betrifft vor allem die Passwörter der Benutzer SAP<SID> oder SAPR3. Deshalb muss ein Berechtigungskonzept für die Datenbankbenutzer definiert und umgesetzt werden.

Der Benutzer OPS$ ist für die Windowsbenutzer zu definieren, die für den Betrieb des SAP-ERP-Systems notwendig sind. Normalerweise sind das die Benutzer SAPService<sid> und <sid>adm. Der Name kann ebenfalls geändert werden. Im SAP-Hinweis 50088 - Anlegen der OPS$ Benutzer unter Windows /Oracle (siehe [SECNOTE]) sind weitere Informationen zum Erstellen des OPS$-Benutzers auf Windows beschrieben.

Sofern es technisch umsetzbar ist, sollte die OPS$-Remoteverbindung durch die "Secure Storage in File System"-(SSFS)-Methode ersetzt werden. Der Zugriff auf die Datenbank ist durch die erforderlichen IP-Adressen einzuschränken.

APP.4.2.M8 Absicherung der SAP-RFC-Schnittstelle (B)

Für die sichere Konfiguration der RFC-Schnittstelle müssen vor allem die Einstellungen der RFC-Verbindungen, der RFC-Berechtigungen und die Absicherung der RFC-Gateways betrachtet werden.

RFC-Verbindungen

RFC-Verbindungen sollten nach bestimmten Richtlinien verwaltet werden. RFC-Verbindungen können zwischen verschiedenen Systemen der gleichen Sicherheitsklassifizierung (z. B. von einem Produktivsystem zu einem anderen) oder von einem System der höheren Sicherheitsklassifizierung zu einem System mit niedrigerer (z. B. von einem Produktivsystem zu einem Testsystem) angelegt werden.

Es ist nicht erlaubt, Benutzerdaten oder eine Trusted-Systemanmeldung von einem System mit einer niedrigen Sicherheitsklassifizierung zu einem System mit einer höheren Sicherheitsklassifizierung zu

nutzen. Diese Verbindungen sind nur erlaubt, um technische Verbindungskonfigurationen zu speichern und Benutzer für jeden Zugriff zu authentisieren.

Folgende Empfehlungen und Umsetzungen sind für RFC-Verbindungen zu beachten:

- Alle RFC-Verbindungen müssen einem für die Verbindungen verantwortlichen Benutzer hinzugefügt werden. Der Verantwortliche kann Informationen zur Notwendigkeit und Verwendung der RFC-Verbindungen zur Verfügung stellen. RFC-Verbindungen, die nicht länger benötigt werden, sind zu löschen.
- RFC-Verbindungen mit gespeicherten Benutzerdaten oder solche, die eine Trusted-Systemanmeldung benutzen, müssen mit der gleichen Sicherheitsklassifizierung oder von einer höheren zu einer niedrigen Sicherheitsklassifizierung genutzt werden.
- Beim Betrieb des SAP-ERP-Systems werden von den von außen aufrufbaren Funktionsbausteinen (remote enabled) typischerweise weniger als zehn Prozent wirklich benötigt. Bei allen anderen Funktionsbausteinen sollte die Remote-Fähigkeit abgeschaltet werden. Ab Release 740 steht hierfür eine Standardfunktion zur Verfügung, mit der die RFC-Funktionsbausteinnutzung gemessen und ungenutzte Bausteine für den Remote-Zugriff deaktiviert werden können (UCON). Dies sollte umgesetzt werden.

RFC-Berechtigungen

Der Zugriff auf Trusting-Systeme wird durch das Berechtigungsobjekt S_RFCACL gesteuert und muss streng kontrolliert werden. Des Weiteren muss die Vergabe von Wildcard-Berechtigungen (*) für das Objekt vermieden werden. Es muss sichergestellt werden, dass der Profilparameter auth/rfc_authority_check aktiviert ist. Alle RFC-Verbindungen mit gespeicherten Anmeldeinformationen sollten dokumentiert werden. Ebenfalls muss sichergestellt werden, dass diesen RFC-Benutzerkonten auf dem Zielsystem nur die Mindestberechtigungen (vor allem nicht SAP_ALL) und die Benutzergruppe SYSTEM zugewiesen werden. Innerhalb des SAP Solution Manager hat SAP dafür eine Diagnosefunktion implementiert.

Zusammenfassend sind die folgenden Maßnahmen umzusetzen:

- Die RFC-Berechtigungsprüfung wird mit dem Profilparameter auth/rfc_authority_check = 1 aktiviert.
- Der Benutzertyp für die RFC-Verbindungen ist SYSTEM.
- Eine Namenskonvention für die RFC-Serverbenutzer sollte entwickelt werden.
- Die Berechtigungen auf dem Zielsystem sind stark einzuschränken. Kein SAP_ALL!
- Keine Wildcard-Berechtigung für das Berechtigungsobjekt S_RFCACL.

Absicherung des RFC-Gateways

RFC-Gateways sind Teil jeder ABAP-Instanz, sie sollten aber unabhängig von dieser Instanz installiert werden. Ein Gateway-Betrieb ist zum Beispiel für bestimmte Java-Anwendungen notwendig. In beiden Fällen werden die gleichen Profiparameter eingestellt. Die RFC-Gateways sind für jede Art der Kommunikation erforderlich, die RFC- oder CPI-C- Protokolle verwenden und müssen deshalb die neuste verfügbare RFC-Bibliothek nutzen. Als Applikationsserver-Schnittstelle zu anderen Systemen (z. B. zu anderen SAP-ERP-Systemen, zu externen Programmen) müssen angemessene Sicherheitsbedingungen geschaffen werden. Speziell für externe Programme, die über die Gateways gestartet werden, müssen die folgenden Sicherheitseinstellungen benutzt werden:

- Es ist eine sichere Verbindung zwischen Gateway und verschiedenen SAP-ERP-Systemen herzustellen. Das kann mit der Einrichtung von SNC oder der Verwendung des SAP-Routers zwischen den Gateways durchgeführt werden.
- Die Protokollierung des Gateways ist zu aktivieren. Das Gateway muss so konfiguriert werden, dass vom Gateway ausgeführte Aktionen und erhaltene Anfragen in die Protokolldatei

aufgenommen werden, um die Sicherheitseinstellungen für ein externes Programm zu definieren.

- Jeder unberechtigte Start eines externen Programmes muss durch die Instandhaltung der Datei secinfo im Datenverzeichnis der Gatewayinstanz (gw/sec_info) verhindert werden. Eine allgemeine Freigabe mit * auf allen Nutzungsspezifikationen ist nicht erlaubt.
- Die nicht autorisierte Registrierung von Programmen muss verhindert werden, indem die Datei reginfo in das Datenverzeichnis der Gatewaysinstanz (gw/reg_info) aufgenommen wird. Eine allgemeine Freigabe mit * auf allen Nutzungsspezifikationen ist nicht erlaubt.

Für das RFC-Gateway gibt es vier verschiedene Anwendungsfälle. Jeder einzelne muss im Kontext der Sicherheit analysiert werden:

1. Anwendungsfall: Überwachung – gwmon

Die Serverapplikation gwmon kann ohne Berechtigungen remote aufgerufen werden. Die folgenden Aktionen können unter anderem ausgeführt werden:

- Anzeige von Profilparametern
- Änderung der Gatewayparameter
- Anzeige von secinfo und erneutes Lesen von reginfo (reread)
- Anzeige der Verbindungstabellen
- hartes Herunterfahren des Gatewayservers

Zur Konformität muss der Parameter gw/monitor auf 1 gesetzt werden. Der Parameter definiert, ob das Gateway lokal (=0) und/oder remote (=1) mit einem Monitor kommuniziert.

2. Anwendungsfall: RFC-Verbindung zu einem ABAP-Stack → fehlt – wird noch nachgeliefert

Dieser Anwendungsfall ist nur mit einem integrierten RFC-Gateway möglich. Funktionsbausteine werden innerhalb des AS ABAP auf diesen Weg aufgerufen und mit Hilfe des AS ABAP wird die Authentifizierung und Autorisierung durchgeführt. Die folgenden Aktionen dürfen von Clients ausgeführt werden:

- Aufruf eines beliebigen Funktionsbausteines innerhalb der AS ABAP Berechtigungen.
- Das Berechtigungsobjekt S_RFC wird für den Funktionsaufruf benötigt. Aus diesem Grund muss dieses Berechtigungsobjekt nur dem Benutzer zugeordnet werden, der dieses benötigt und die erforderlichen Funktionsbausteine müssen im Berechtigungsobjekt gepflegt werden.

Für Remote Aufrufe wird zusätzlich das Berechtigungsobjekt S-RFC benötigt. Des Weiteren sind Berechtigungsprüfungen für Remote Aufrufe die gleichen wie für interne Aufrufe.

Zur Gewährleistung einer starken Authentifizierung und Verschlüsselung zum AS ABAP und einer Ende-zu-Ende-Verschlüsselung sollte SNC verwendet werden. Der Parameter snc/permit_insecure_com definiert, ob vom RFC-Gateway Verbindungen akzeptiert werden, die nicht über SNC abgesichert sind. Ein weiterer Parameter snc/permit_insecure_start definiert, ob Programm (z. B. AS ABAP) Verbindungen ohne SNC herstellen dürfen.

3. Anwendungsfall: Starten von RFC-Serverprogrammen

Das Programm ist auf dem Server selbst ausführbar, ohne die Sicherheitsmechanismen des AS ABAP zu nutzen. Die primäre Authentisierung wird durch das RFC-Gateway selbst ausgeführt. Dazu wird die Datei secinfo, die einen ACL enthält, verwendet. Die folgenden Aktionen können vom RFC-Client ausgeführt werden:

- Starten des Serverprogramms auf dem Server

Die Datei secinfo ist mit den entsprechenden ACL für die RFC-Clients zu verwalten. Empfohlen wird Secure Network Communication (SNC) einzusetzen, um eine starke Authentisierung zum RFC-Gateway und eine Ende-zu-Ende-Verschlüsselung zu erreichen. Der Profilparameter

snc/permit_insecure_com definiert, ob das RFC-Gateway Verbindungen akzeptiert, die nicht SNC geschützt sind.

4. Anwendungsfall: Registrierung von RFC-Serverprogrammen

Das externe RFC-Serverprogramm registriert sich selbst durch Benutzung der Programm-ID, ohne die Sicherheitsmechanismen des AS ABAP zu nutzen. Das RFC-Serverprogramm akzeptiert alle Aufrufe der RFC-Clients durch Nutzung des RFC-Gateways (ähnlich wie Anwendungsfall 3). Die folgenden Aktionen können vom RFC-Server ausgeführt werden:

- Ein beliebiges RFC-Serverprogramm kann sich durch Verwendung der Programm-ID registrieren.
- Ein beliebiger RFC-Client kann jedes der registrierten Serverprogramme aufrufen.
- Berechtigungen, die ACLs für ihre IP-Adressen oder Hostnamen nutzen.
- Verwalte die Datei reginfo mit angemessenen ACLs für die registrierten RFC-Serverprogramme.
- Verwalte die Datei secinfo mit angemessenen ACLs für die RFC-Clients.

Protokollierung am Gateway

Es gibt bestimmte Systemvoraussetzungen, um die Protokollierung am Gateway mit der Transaktion SMGW zu nutzen. Die Protokollierung ist für die Kernel-Releases größer 640 zu implementieren. Zur Protokollierung der Gateway-Ereignisse sollte die folgende Parametereinstellung gesetzt werden (siehe auch SAP-Hinweis 910919 – Gateway-Logging einrichten, [SECNOTE]):

- Empfohlene Einstellung des Profilparameters mit Aktionen: gw/logging: ACTION=SPXMZR

Härtung des RFC-Gateways

Für die Systemsicherheit ist es notwendig, dass die Zugriffssteuerungslisten (ACLs) des Gateways erstellt und gewartet werden. Dazu sollten die folgenden Schritte durchgeführt werden.

1. Mit der Transaktion RZ11 wird der Parameter gw/reg_no_conn_info geprüft. Die SAP-Empfehlung ist, dass alle Sicherheitsbits gesetzt werden. Der Parameter sollte demnach auf 255 stehen. Falls das noch nicht umgesetzt wurde, muss DEFAULT.PFL auf Betriebssystemebene eingestellt oder mit der Transaktion RZ10 den Parameter gw/reg_no_conn_inf auf 255 gesetzt werden.
2. Der Inhalt der ACL-Dateien soll für alle Einträge geprüft werden, die als Variable ein * haben (z. B. TP=* USER=* HOST=*). Dazu die Transaktion SMGW aufrufen, Menüpunkt Springen wählen, unter Expertenfunktionen Externe Sicherheit und Anzeige ACL wählen.
3. Ist das der Fall, müssen die ACLs zentral verwaltet und überwacht werden.

Zusammenfassung der Gatewayeinstellungen

Die RFC-Gateway Sicherheitsdateien secinfo, reginfo und pxyinfo müssen bearbeitet und aktiviert werden. secinfo verhindert, dass externe Programme unberechtigt gestartet werden. reginfo stellt sicher, dass sich externe Programme am Gateway registrieren.

Der Profilparameter gw/reg_no_conn_info muss gemäß SAP-Hinweis 1444282 - gw/reg_no_conn_info Einstellungen (siehe [SECNOTE]) – gw/reg_no_conn_info Einstellung eingespielt werden. In jedem Fall sollte der Parameter auf 255 gesetzt werden. Für den Profilparameter muss ein ungerader Wert gesetzt werden.

Der Profilparameter gw/acl_mode definiert, wie sich das Gateway verhält, falls eine ACL-Datei (gw/sec_info oder gw/reg_info) nicht existiert. Die empfohlene Standardeinstellung für den Parameter ist gw/acl_mode = 1. Externe und registrierte Server werden so nur innerhalb des Systems erlaubt.

Der Profilparameter gw/monitor definiert, ob das Gateway lokal und/oder remote mit einem Monitor kommuniziert. Die empfohlene Einstellung ist gw/monitor = 1.

APP.4.2.M9 Absicherung und Überwachung des Message-Servers (B)

Der Message-Server wird pro SAP-ERP-System nur einmal konfiguriert. Seine Aufgaben sind:

- Zentraler Kommunikationskanal zwischen den einzelnen Applikationsservern (Instanzen) des Systems.
- Lastverteilung bei Anmeldungen über SAP GUI und RFC mit Logongruppen (Transaktion SMLG).
- Informationsstelle für den Web Dispatcher und die Applikationsserver. Jeder Applikationsserver des Systems meldet sich zuerst beim Message-Server an.

Die Sicherheitseinstellungen für den Message-Server sind über Profilparameter durchzuführen. Die empfohlenen Werte zur Einstellung der Profiparameter sind in der folgenden Tabelle aufgeführt:

Profilparameter	**Beschreibung**	**Wert**
ms/monitor	Nur der Applikationsserver darf den internen Speicher des Message-Servers ändern und die Monitorfunktion ausführen. Das externe Überwachungstool msmom hat nur noch eingeschränkten Zugriff. Wert 1 bedeutet, dass auch externe Überwachungsprogramme den internen Speicher des Message-Servers überwachen dürfen.	0 Die externe Überwachung des Message-Servers wird unterbunden.
ms/acl_info	Bestimmung einer Datei mit Zugriffsberechtigungen auf die Zugriffskontrollliste (ACL) für den Message-Server.	<Dateiname>
rdisp/msserv_internal	Die Message-Server Ports müssen in interne Ports (Kommunikation mit dem Applikationsserver) und externe (Kommunikation mit Client/Server) Ports getrennt werden. Für den internen Port kann der Profiparameter rdisp/msserv_internal genutzt werden. Der Parameter bestimmt einen Port, der vom Applikationsserver zur internen Kommunikation genutzt wird. Der Wert 0 bedeutet, dass kein eigener Port für die interne Kommunikation verwendet wird.	<Interne Port Nummer> Sollte sich vom externen Message Port unterscheiden.
ms/admin_port	Der Parameter spezifiziert einen Port, der für die remote-Administration des Message-Servers genutzt werden kann. Ist der Wert auf 0 gesetzt, ist die remote-Administration deaktiviert.	0
icm/http_admin	Der interne Kommunikationsmanager kann remote als Web-Interfacemkonfiguriert werden.	Sollte nicht verwendet werden.

Zum verbesserten Schutz des Message-Servers und zum Genehmigen von Ports müssen die folgenden Einstellungen festgelegt werden:

1. Ist es externen Überwachungsprogrammen wie dem Überwachungstool msmon erlaubt, sich mit dem Message-Server zu verbinden?
2. Wird die interne von der externen Kommunikation getrennt?
3. Werden ACLs (Zugriffskontrollliste) für den Message-Server genutzt?

Überwachung des Message-Servers

Fällt der Message-Server auf dem SAP-ERP-System aus, muss dieser schnellstmöglich neu gestartet werden. Wird eine Instanz gestartet, kontaktiert der Dispatcher-Prozess den Message-Server und stellt die verfügbaren Dienste dem Message-Server vor (DIA, BTC, SPO, UPD etc.). Kann der Verbindungsaufbau zum Message-Server nicht hergestellt werden, werden diese Daten im Systemprotokoll (Syslog) eingetragen. Es gibt verschiedene Möglichkeiten, den Message-Server zu überwachen und zu testen:

- Überwachung des Message-Servers im SAP-ERP-System: Mit der Transaktion SMMS – Message-Server-Monitor können alle Einstellungen im SAP-ERP-System geprüft und geändert werden sowie Trace-Dateien erzeugt und angeschaut und Statistiken gelesen werden.
- Überwachung des Message-Servers über den Browser: Damit Details über Server und Logon-Gruppen im Web-Browser angezeigt werden, muss in der URL der Host des Message-Servers und der http-Port des Message-Servers angeben werden. Dazu muss der Profilparameter ms/server_port_<xx> gesetzt werden.
- Überwachung und Test des Message-Servers auf Betriebssystemebene: Dafür stehen die folgenden Programme zur Verfügung:
- msmon – hat die gleichen Funktionen wie die Transaktion SMMS.
- msprot – übermittelt einen kontinuierlichen Status über die Applikationsserver, die an den Message-Server angeschlossenen sind.

Zum Testen stehen die folgenden Programme zur Verfügung:

- Im Executable-Verzeichnis das Programm /usr/sap/<SID>/SYS/exe/run.
- igtst, zur Prüfung der Verbindung zum Message-Server und zum Anzeigen der aktiven Instanzen und Logon-Gruppen.

APP.4.2.M10 ENTFALLEN (B)

Die zugehörige Anforderung ist entfallen.

APP.4.2.M11 Sichere Installation eines SAP-ERP-Systems (S)

Bevor ein SAP-ERP-System sicher konfiguriert wird, müssen bestimmte Schritte während der Installation durchgeführt werden. Im folgenden Kapitel werden einige der wichtigsten Punkte zur sicheren Installation eines SAP-ERP-Systems (ABAP) beschrieben.

Aktuelle SAP-Sicherheitsleitfäden und SAP-Dokumentationen berücksichtigen

SAP stellt zahlreiche Dokumente und Informationen zur Verfügung. Diese sollten die Administratoren kennen und sie sollten regelmäßig prüfen, ob Aktualisierungen vorliegen. Details zu Sicherheitseinstellungen können dem SAP-Hinweis 2253549 - The SAP Security Baseline Template entnommen (siehe [SECNOTE]) werden. Dieser SAP-Hinweis beinhaltet Informationen und Dokumente zu den Themen:

- **SAP Security Baseline Template**
- **SAP Security White Papers** [SAPSWP]
- **Security Optimization Services** [SAPSOS]
- **Security Guides zu SAP-Lösungen** [SAPSG]
- **SAP HANA Security Checklists and Recommendations** [SAPHSCR]

Absicherung der Betriebssysteme

Die Komponenten eines SAP-ERP-Systems werden als Programme auf einem IT-System installiert und in Form von Prozessen ausgeführt. Damit ist die Sicherheit des genutzten Betriebssystems auch wichtig für das SAP-ERP-System. Folgende Maßnahmen sind hierbei zu beachten:

- APP.4.2.M16 *Umsetzung von Sicherheitsanforderungen für das Betriebssystem Windows*
- APP.4.2.M17 *Umsetzung von Sicherheitsanforderungen für das Betriebssystems Unix*

Mithilfe geeigneter Schutzmaßnahmen sollte der Applikationsserver Betriebssystemkommandos und Dateizugriffe so selten wie möglich und immer nur kontrolliert ausführen können. Hierzu sollten entsprechende Berechtigungen gesetzt und die Dateischnittstelle geschützt werden (Transaktionen FILE und SFILE, Tabelle SPTH).

Nur benötigte Komponenten installieren

Ein SAP-ERP-System besteht potenziell aus vielen unterschiedlichen Komponenten. Ungenutzte Komponenten bergen jedoch Sicherheitsrisiken, da diese oft vergessen werden und daher ohne angepasste Konfiguration betrieben werden. Aus diesem Grund sollten nur Komponenten installiert werden, die tatsächlich benötigt werden.

Für ein SAP-ERP-System muss insbesondere entschieden werden, ob nur ein oder beide Stacks nötig sind, sofern die eingesetzte Systemversion die separate Installation noch unterstützt. Ist das nicht der Fall, muss der nicht benötigte Stack so abgesichert werden, dass dessen Funktionen nicht unberechtigt genutzt werden können.

Wahl von sicheren Passwörtern

Während der Installation müssen wichtige Authentisierungsdaten eingegeben werden. Dies sind beispielsweise Passwörter für technische Benutzer, die von den SAP-ERP-Systemkomponenten zur Authentisierung bei internen Kommunikationsverbindungen genutzt werden. Weitere Informationen sind in der Maßnahme APP.4.2.M13 *SAP-Passwortsicherheit* beschrieben.

Installationsquellen absichern

In der Regel werden SAP-ERP-Systeme nicht direkt von CD oder DVD installiert. Vielmehr wird eine Verzeichnisstruktur lokal oder im Netz genutzt, um die Daten anzubieten, die zur Installation benötigten werden. Die Daten der CD- bzw. DVD-Medien werden dann dorthin kopiert. Es wird empfohlen, die Daten nicht lokal auf dem Rechner zu halten, auf dem das SAP-ERP-System installiert wird, sondern auf einem Server. Auf die Daten kann dann über das Netz zugegriffen werden. In großen Institutionen kann dieses Verzeichnis genutzt werden, um zusätzliche SAP-ERP-Systeme zu installieren. Werden die Systeme nicht in einem separaten und abgeschirmten Netzsegment installiert, sollte der Installationsrechner vom Netz genommen werden, solange er nicht benötigt wird.

Es wird empfohlen, den Zugriff auf die Installationsquellen mit Mitteln des Betriebssystems abzusichern, sodass nur berechtigte Administratoren darauf zugreifen können. Unberechtigte Benutzer dürfen insbesondere keine schreibenden Rechte auf die Installationsquellen besitzen, damit die enthaltenen Daten nicht verändert werden können.

Werden die Installationsquellen lokal auf den Rechnern des SAP-ERP-Systems vorgehalten, sollten sie nach der Installation gelöscht werden.

SAP-Hinweise für die Installation umsetzen

Die Installationsanleitung eines SAP-ERP-Systems enthält in der Regel viele Verweise auf SAP-Hinweise, in denen wichtige Informationen für eine reibungslose Installation oder zur Problemlösung enthalten sind. Häufig verweisen die SAP-Hinweise auch wieder auf weitere SAP-Hinweise, sodass eine beträchtliche Informationsmenge zusammenkommen kann. Die Hinweise sind vor der Installation zu besorgen. Es ist aber zunächst ausreichend, die in der Installationsdokumentation angegebenen Hinweise zu lesen und einen weiteren Iterationsschritt durchzuführen. Oft wird bei Referenzen auf weitere Informationen explizit angegeben, ob diese verpflichtend abzuarbeiten sind oder nur unter bestimmten Bedingungen angewandt werden sollen.

Es wird dringend empfohlen, alle relevanten Informationen abzuarbeiten, da es sonst leicht zu Fehlern kommen kann. Fehlermeldungen dürfen nur dann ignoriert werden, wenn dies explizit durch die Installationsanleitung oder SAP-Hinweise angegeben wird. Weitere Informationen sind in der Maßnahme APP.4.2.M30 *Implementierung eines kontinuierlichen Monitorings der Sicherheitseinstellungen* beschrieben.

Sichere Installation und Konfiguration der Datenbank

Die SAP-Datenbank ist eine kritische Komponente, die vor unberechtigtem Zugriff geschützt werden muss. Neben den allgemeinen Aspekten einer sicheren Datenbank-Installation sind die spezifischen Empfehlungen in der Maßnahme APP.4.2.M7 *Absicherung der SAP-Datenbanken* zusammengefasst. Die Sicherheit von Datenbanken wird auch im Baustein APP.4.3 *Relationale Datenbanksysteme* behandelt.

APP.4.2.M12 SAP-Berechtigungsentwicklung (S)

Die klassische SAP-ERP-Systemlandschaft besteht aus drei Stufen: Entwicklung, Qualitätssicherung/Test und Produktion (D-Q-P). In SAP-ERP-Systemen werden Entwicklungen durchgeführt und Änderungen vorgenommen. Die Entwicklungen werden nach einem festgelegten Zyklus freigegeben und entsprechend ausgerollt. Berechtigungsrollen, die neu entwickelt oder geändert wurden, sollten mithilfe des SAP-Transportsystems durch die SAP-Transportstufen D-Q-P transportiert werden.

Entwicklungssysteme

Berechtigungen in Entwicklungssystemen sind grundsätzlich nicht so stark eingeschränkt wie in einem Qualitätssicherungs- und Produktivsystem. Dennoch sollten Berechtigungen in den folgenden Funktionsbereichen gewissen Einschränkungen unterliegen: Berechtigungsadministration, Benutzeradministration, Systemadministration, Customizing, Transportverwaltung und Entwicklung. Im Entwicklungssystem können neue Funktionen erstellt und geändert werden sowie weitere Rollenanpassungen vorgenommen werden. Schaltbare Berechtigungsprüfungen (SACF) werden im Entwicklungssystem aufgenommen und in den Loggingmodus oder aktiv gesetzt und danach in die Folgesysteme transportiert.

Qualitätssicherung/Test

Die SAP-ERP-Systeme für die Qualitätssicherung sowie Tests unterliegen den gleichen Berechtigungseinschränkungen wie Produktivsysteme. Die Qualitätssicherungssysteme für Tests und Trainings simulieren eine reale Systemumgebung. Tests werden auf dem Qualitätssicherungssystem von sogenannten Key-Usern durchgeführt. Dadurch wird vermieden, dass sich Endanwender auf dem System befinden.

Produktivsysteme

Die Berechtigungsvergabe unterliegt im Produktivsystem bestimmten Einschränkungen, die in einem Berechtigungskonzept definiert werden sollten. Berechtigungen für das Replacing im Debugging (elektronisches Radieren) und die Berechtigung für das Editieren von Änderungsbelegen sollten im Produktivsystem ausschließlich Notfallbenutzer erhalten. Berechtigungen, mit denen sich Massenpflegeaktivitäten (z. B. über CATT, SAPGUI-Skripting usw.) durchführen lassen, sollten in Produktivsystemen sehr restriktiv vergeben werden. Das Notfallkonzept regelt die Ausnahmefälle kritischer Berechtigungen im Produktivsystem.

APP.4.2.M13 SAP-Passwortsicherheit (S)

SAP liefert viele Profilparameter mit Standard-Passwort- und -Anmelderegeln aus. Es müssen jedoch nicht nur diese Standardeinstellungen geändert werden, sondern auch Passwortrichtlinien definiert, interne oder externe Vorgaben umgesetzt und Sicherheitsrichtlinien für Benutzer erstellt werden.

SAP-ABAP-Stack

Passwortregeln im SAP-ERP-System können durch Profilparameter (RZ10), Customizing-Schalter (Tabelle PRGN_CUST), Pflegen verbotener Passwörter (Tabelle USR40) oder durch erstellte Sicherheitsrichtlinien (SECPOL) definiert werden.

Einstellungen der Passwortregeln über Profilparameter (Login-Parameter)

Die Login-Parameter definieren die Mindestanforderungen für Passwörter. SAP liefert eine Reihe von Standardwerten aus. Alle Standardregeln der Profilparameter für Passwort- und Anmelderegeln sind auf der SAP-Help Webseite unter [SAPLOPA] detailliert beschrieben.

Die Einstellungen der Profilparameter in der folgenden Tabelle werden empfohlen, um eine höhere Absicherung zu erreichen (die Pflege der Profilparameter erfolgt über die Transaktion RZ10):

Profilparameter	Empfohlener Wert	Standard-wert	Beschreibung
login/min_password_lng	8	6	Minimallänge des Passworts
Mindestens zwei der fünf Zeichenkategorieparameter sollten gesetzt werden:			
login/min_password_digits	1	0	minimale Anzahl von Ziffern
login/min_password_letters	1	0	minimale Anzahl von Buchstaben
login/min_password_lowercase	1	0	minimale Anzahl von Kleinbuchstaben
login/min_password_uppercase	1	0	minimale Anzahl von Großbuchstaben
login/min_password_specials	1	0	minimale Anzahl von Sonderzeichen
login/password_max_idle_initial	3	0	Gültigkeit des ungenutzten Initialpasswortes
login/password_downwards _compatibility	0	1	Grad der Abwärtskompatibilität

Hinweis: Schutz vor Passwort-Attacken

Es wird empfohlen, das SAP-ERP-System vor Passwort-Attacken zu schützen, indem nach einer bestimmten Anzahl erfolgloser Anmeldeversuche die Verbindung unterbrochen wird. Die Anzahl wird durch den Profilparameter login/fails_to_session_end konfiguriert.

Generierung von Passwörtern

Werden Kennwörter neu angelegt oder zurückgesetzt, sollten die neuen Kennwörter vom SAP-ERP-System generiert und nicht manuell gesetzt werden. So wird vermieden, dass dieselben Initialpasswörter an verschiedene Benutzer ausgeliefert werden.

Customizing-Schalter für die Generierung von Passwörtern

Mithilfe der Customizing-Schalter wird die Obergrenze der Werte definiert. Die Mindestanforderungen werden durch Profilparameter gesetzt. In der folgenden Tabelle sind die korrespondieren Customizing-Schalter und Profilparameter dargestellt.

Customizing-Schalter	Profilparameter (Login-Parameter)	Empfohl-ener Wert	Beschreibung
GEN_PSW_MAX_LETTERS	login/min_password_letters	40	maximale Anzahl an Buchstaben im generierten Kennwort
GEN_PSW_MAX_DIGITS	login/min_password_digits	2	maximale Anzahl an Zahlen im generierten Kennwort
GEN_PSW_MAX_SPECIALS	login/min_password_specials	1	maximale Anzahl an Sonderzeichen im generierten Kennwort
GEN_PSW_MAX_LENGTH	login/min_password_lng	10	maximale Länge des generierten Kennworts

Ist der Wert des Customizing-Schalters nicht mit dem Wert des Profilparameters identisch, wird der Standardwert des Profilparameters gezogen. Die Pflege erfolgt über die Tabelle PRGN_CUST mit der Transaktion SM30.

Komplexitätsregeln und verbotene Passwörter

Passwörter können über Komplexitätsregeln oder mittels einer Liste verbotener Passwörter definiert werden. Die Komplexität der Passwörter lässt sich durch die folgenden Profilparameter definieren:

- login/min_password_specials
- login/min_password_uppercase
- login/min_password_lowercase

Durch die Pflege der Tabelle USR40 (Transaktion SM30/SM31) ist es möglich, bestimmte Passwörter auszuschließen. Es können ebenfalls generische Werte (mit der Wildcard *) und Platzhalter (wie ?) als Einzelwerte oder Muster verboten werden.

Definieren von Sicherheitsrichtlinien

Falls die Anforderung besteht, dass die Passwortregeln und Anmeldebestimmungen nicht für jeden Benutzer gleich sind, müssen Sicherheitsrichtlinien definiert werden (siehe dazu APP.4.2.M19 *Definition der Sicherheitsrichtlinien für Benutzer*).

Passwörter mit dem Hash-Algorithmus schützen

Passwörter in einem SAP-ERP-System werden verschlüsselt und als Hash-Wert abgelegt. Dieser Wert wird verwendet, wenn das Passwort übertragen wird. Deshalb muss der eingesetzte Hash-Algorithmus den aktuellen Sicherheitsstandards entsprechen.

Es muss zudem darauf geachtet werden, dass der neueste Hash-Algorithmus auch aktiviert wird (Codeversion). In der nachfolgenden Tabelle sind die entsprechenden Codeversionen für die einzelnen Releases mit den empfohlenen Profilparametern aufgeführt.

Release	Empfohlener Profilparameter	Codeversion
Bis 4.5	Keine bestimmten Profilparameter werden benötigt	B
4.6 – 6.40	login/password_charset = 2	E
7.00 – 7.01	login/password_downwards_ compatibility = 0	F
7.02 und höher	login/password_downwards_ compatibility = 0	H

Zur Sicherung des Passwortes muss die Berechtigungsgruppe von Tabellen, in denen Hash-Werte abgelegt sind, auf SPWD geändert werden. Das betrifft die Tabellen: USR02, USH02, USRPWDHISTORY, VUSR001, USH02_ARC_TMP und VUSR02_PW. Kein Benutzer darf auf die Berechtigungsgruppe SPWD über die Berechtigungsobjekte S_TABU_DIS zugreifen. Dedizierte Benutzer könnten die Berechtigung über die Tabelle USR02 durch das Berechtigungsobjekt S_TABU_NAM erhalten.

Der Report CLEANUP_PASSWORD_HASH_VALUES unterstützt dabei redundante, alte und abwärtskompatible Passwörtern zu entfernen (über die Transaktion SA38). Alte Passwort-Hashes können auch über die Tabelle USR02 (über die Transaktion SE16) in den Spalten BCODE und PASSCODE angezeigt werden.

Hinweis: Wird die zentrale Benutzerverwaltung (ZBV) eingesetzt, müssen die Basisrelease der angebundenen Systeme (Tochtersysteme) gleich oder ein Release höher sein.

Weitere Empfehlungen für die sichere Einstellung des Passwort-Hashes im ABSP-System sind in den SAP-Hinweisen 1458262 - ABAP: Empfohlene Einstellung für Kennwort-Hash-Algorithmen und 1484692 - Lesezugriff für Tabellen können mit Kennwort-Hash-Werten geschützt werden [SECNOTE] beschrieben.

Hinweis: Benutzer-IDs und Passwörter werden während der Anmeldung unverschlüsselt am Client des Anwendungsservers übertragen. Deshalb müssen weitere Sicherheitsmaßnahmen ergriffen werden, z. B. verschlüsselte Kommunikation (siehe APP.4.2.M18 *Abschaltung von unsicherer Kommunikation*).

SAP-JAVA-Stack

Mit den folgenden Parametern sollten die Sicherheitsrichtlinien für Anmelde-IDs und Passwörter definiert werden.

Hinweis: Wird die ABAP-Benutzerverwaltung als Datenquelle verwendet, wird das System diese Werte in den meisten Fällen ignorieren.

UME-Parameter	**Wert**	**Beschreibung**
ume.logon.security_policy.auto_unlock_time	Defaultwert = 600 = deaktiviert diese Option.	Sperre eines Benutzers in Minuten nach mehrfachen fehlerhaften Loginversuchen.
ume.logon.security_policy.enforce_policy_at_logon	Defaultwert = FALSE	Das Passwort wird während der Anmeldung gegen die Sicherheitsliste überprüft. Falls diese nicht mehr reicht, muss der Benutzer ein neues Passwort setzen.
ume.logon.security_policy.lock_after_invalid_attempts	Defaultwert = 6Mögliche Werte = 0 bis 99990 = erlaubt eine unbegrenzte Anzahl an fehlgeschlagener Anmeldeversuche.	Anzahl fehlerhafter Login-Versuche, bevor der Benutzer gesperrt wird.
ume.logon.security_policy.log_client_hostaddress	Defaultwert = TRUE	Die IP-Adresse des Benutzers wird mitprotokolliert.
ume.logon.security_policy.log_client_hostname	Defaultwert = FALSE	Der Benutzername wird mitprotokolliert.
ume.logon.security_policy.oldpass_in_newpass_allowed	Defaultwert = FALSE	Definiert, ob das neue Passwort Bestandteile des alten Passworts enthalten darf.
ume.logon.security_policy.password_alpha_numeric_required	Defaultwert = 1	Mindestanzahl von Buchstaben und Zahlen (Beispielsweise muss das Passwort mindestens 3 Buchstaben und 3 Zahlen enthalten, wenn der Wert = 3)
ume.logon.security_policy.password_change_allowed	Defaultwert = TRUE	Definiert, ob Benutzerpasswörter geändert werden können.
ume.logon.security_policy.password_expire_days	Defaultwert = 90	Gültigkeit des Passworts in Tagen.

UME-Parameter	Wert	Beschreibung
ume.logon.security_policy.password_history	Default value = 0	Verhindert dass Benutzer alte Passwörter wiederverwenden (Größe der Passworthistorie).
ume.logon.security_policy.password_impermissible		Eine Liste, die durch Kommata getrennt ist, mit Ausdrücken und Zeichen, die nicht als Passwort verwendet werden dürfen. Variablen sind Stern (*) = eine Reihe von Zeichen (aaa*= alle Passwörter, die mit „aaa“ beginnen, werden abgelehnt) und Fragezeichen (?) = ein Einzelausdruck.
ume.logon.security_policy.password_last_change_date_default	Datum im Format = MM/DD/YYYYDefaultwert = 12/31/9999	Das Datum wird als Datum der letzten Änderung gezählt, wenn der Benutzer sein Passwort niemals verändert hat. Siehe auch: ume.logon.security_policy.password_expire_days
ume.logon.security_policy.password_max_idle_time	Defaultwert = 0Weitere mögliche Werte: 0 bis 2147483647; Wert = 0 deaktiviert	Tage bis zur Sperrung des Passwortes seit dem letzten Login.
ume.logon.security_policy.password_max_length	Defaultwert = 14	Maximale Passwortlänge
ume.logon.security_policy.password_min_length	Defaultwert = 1	Minimale Passwortlänge
ume.logon.security_policy.password_mix_case_required	Defaultwert = 0	Minimale Anzahl von Groß- und Kleinbuchstaben in einem Passwort.
ume.logon.security_policy.password_special_char_required	Defaultwert = 0	Minimale Anzahl an Sonderzeichen in einem Passwort.

UME-Parameter	Wert	Beschreibung
ume.logon.security_policy.password_successful_check_date_default	Datum im Format = MM/DD/YYYYDefaultwert = 12/31/9999	Definiert das Standarddatum für die letzte erfolgreiche Anmeldung mit Benutzer-ID und Passwort, wenn ein Benutzer keine erfolgreiche Anmeldung mit Benutzer-ID und Passwort aufgezeichnet hat oder die letzte Anmeldung vor dem Standarddatum stattgefunden hat.
ume.logon.security_policy.userid_digits	Defaultwert = 0Wert < 0 => Zahlen sind nicht erlaubtWert = 0 => Zahlen sind erlaubtWert > 0 = > Zahlen sind erforderlich	Minimale Anzahl an Zahlen in einer Benutzer-Login-ID.
ume.logon.security_policy.userid_in_password_allowed	Defaultwert = FALSE	Definiert, ob das Passwort Teile der Benutzer-ID enthalten darf.
ume.logon.security_policy.userid_lowercase	Veraltet.	
ume.logon.security_policy.userid_special_char_required	Defaultwert = 0Wert < 0 => Sonderzeichen sind verbotenWert = 0 => Sonderzeichen sind erlaubtWert > 0 => Sonderzeichen sind erforderlich	Minimale Anzahl an Sonderzeichen in einer Benutzer-Login-ID.
ume.logon.security_policy.useridmaxlength	Defaultwert = 20	Maximale Länge der Benutzer-ID.Dieser Wert wird automatisch auf 12 gesetzt, wenn die Kombination AS Java und AS fürABAP installiert ist. Wenn eine Datenbank als Quelle für Benutzerdaten verwendet wird, muss dieser Wert kleiner bzw. gleich 200 sein.

UME-Parameter	Wert	Beschreibung
ume.logon.security_policy.useridminlength	Defaultwert = 5	Minimale Länge der Benutzer-ID.

APP.4.2.M14 Identifizierung kritischer SAP-Berechtigungen (S)

Kritische Berechtigungen sollten nur restriktiv vergeben werden und auch nur dann, wenn organisatorische und technische Sicherheitsmaßnahmen dafür definiert wurden. Mithilfe von Tools, wie SAP Access Control Emergency Access Management, können kritische Berechtigungen vergeben und überwacht werden.

Kritische Berechtigungen werden meistens Notfallbenutzern zugeordnet. Tritt ein Notfall ein, meldet sich der Benutzer mit dem Notfallbenutzer an und seine Tätigkeiten werden protokolliert.

Was sind kritische Berechtigungen?

Vereinfacht kann eine kritische Berechtigung damit beschrieben werden, dass sie auf Konfigurationen im SAP-ERP-System zugreifen kann, die sicherheitskritische Aktivitäten beinhalten. Dazu zählen die SAP-Basisberechtigungen oder auch der Zugriff auf personenbezogene Daten. SAP gibt keine generellen Anweisungen für den Umgang mit kritischen Berechtigungen vor, da jede Institution andere Sicherheitsbestimmungen und individuelle Vorgaben im Umgang mit kritischen Berechtigungen hat.

Kritische Berechtigungen identifizieren

Mithilfe eines Berechtigungsreviews oder mit Tools wie SAP Access Control Access Risk Analysis lassen sich kritische Berechtigungen in Benutzerrollen analysieren. Nachdem sie in den Rollen identifiziert wurden, müssen die Berechtigungsadministratoren diese Objekte im Detail betrachten:

- Sind diese wirklich für die Institution kritisch?
- Ist die Transaktion allein kritisch oder vor allem die Ausprägung der Werte des Berechtigungsobjektes?
- Welche Maßnahmen können durchgeführt werden?
- Kann die Institution das Risiko tragen oder müssen Kontrollen zur Minderung eingesetzt werden?

Die Liste der kritischen Berechtigungen und Kombinationen wäre insgesamt jedoch sehr lang und könnte nicht vollständig abgebildet werden. Deshalb werden allgemeine Beschreibungen für kritische Berechtigungen definiert und im Folgenden nur einige Beispiele vorgestellt.

Allgemein können die Berechtigungen der SAP-ERP-Systemadministration als kritisch eingestuft werden. Die Berechtigungsobjekte beginnen mit dem Präfix S_ wie beispielsweise:

- uneingeschränkte Tabellenpflege = S_TABU_DIS oder S_TABU_NAM mit * und ACTVT <> 3
- Entwicklungsobjekte anlegen, ändern oder löschen: S_DEVLOP mit ACTVT = 01, 02 oder 06
- Security Audit Log löschen = S_ADMI_FCD mit A_ADMI_FCD = AUDA
- Benutzer pflegen = S_USER_GRP mit ACTVT = 01, 02, 05 oder 06
- In diesem Zusammenhang gelten insbesondere die Berechtigungen zum Debugging mit Replace (S_DEVELOP|OBJ_TYPE = DEBUG; ACTVT = 02) und zur Löschung von Änderungsbelegen (S_SCD0, S_SCD0_OBJ jeweils mit ACTVT=06) als hochkritisch.

Kritische Rollen und kritische Profile

Neben den kritischen Berechtigungen gibt es auch kritische Rollen und Profile. Kritische Profile lassen sich durch die Endung _ALL identifizieren und kritische Rollen durch die Zeichenkette ADM.

Kritische Berechtigungen durch Analyse identifizieren und bewerten

Folgende Instrumente sind für eine Analyse verfügbar:

- Report RSUSR008_009_NEW: Der Report wird über die Transaktion SA38 aufgerufen oder über das Benutzerinformationssystem SUIM ("Benutzer" und dann "mit kritischen Berechtigungen (Neue Version)" wählen). Mit dem Report können Benutzer mit kritische Berechtigungen und Benutzer mit kritischen Berechtigungskombinationen analysiert werden. Es empfiehlt sich zunächst die Hauptgeschäftsprozesse und -funktionen zu definieren, damit Risiken besser zugeordnet werden können. Kritische Berechtigungen werden unter dem Punkt kritische Berechtigungen gepflegt. Die ID der Berechtigung ist frei wählbar. Es sollte jedoch eine Namenskonvention dafür definiert werden. Nachdem die ID definiert wurde, kann unter dem Punkt Berechtigungsdaten das Berechtigungsobjekt mit den Werten erstellt werden. Danach muss noch eine Variante erstellt werden, die dann zur Analyse genutzt wird. Im Einstiegsbild des Reports kann die Analyse durchgeführt werden (Variante für kritische Kombinationen oder für kritische Berechtigungen). Es können noch weitere Kriterien gewählt werden, z. B. Benutzer, Benutzergruppe, Rollen. Der Report kann insgesamt jedoch keine ausführliche Risikoanalyse ersetzen und dient als Übersicht des SAP-ERP-Systems.
- SAP Access Control: Mit dem Tool SAP Access Control ist es möglich, SAP-spezifische Analysen auf Benutzer-, Rollen- und Profilebene durchzuführen sowie für HR-Objekte. Es kann für eine schnelle und umfassende Erstbereinigung eingesetzt werden. Auch lassen sich bestehende Zugriffs- und Berechtigungsrisiken identifizieren und elimenieren.

APP.4.2.M15 Sichere Konfiguration des SAP-Routers (S)

Der SAP-Router ist ein SAP-Programm und schützt das SAP-Netz. Er ergänzt eine bestehende Firewall-Architektur und sollte immer zusammen mit einer Firewall-Architektur eingesetzt werden. Der SAP-Router sollte als Gateway für eine klassische ABAP-Verbindung benutzt werden.

Es sollten folgende Punkte berücksichtigt werden:

- Der SAP-Router muss die Verbindungen zu den SAP-ERP-Systemen überwachen und protokollieren.
- Es muss eine indirekte Verbindung aufgesetzt werden, falls eine direkte Verbindung aufgrund der Netzkonfiguration nicht möglich ist.
- Verbesserung der Netzsicherheit durch Umsetzung der folgenden Einstellungen:
- SAP-Router Passwörter setzen
- genehmigt Zugang nur zu bestimmten Hosts,
- genehmigt Zugang nur zu bestimmten Dienstleistungen und Hosts,
- akzeptiert nur SNC gesicherte Verbindungen und
- Benutzung eines SAP-Routers als SNC-Tunnel.

Darüber hinaus kann es erforderlich sein, die Leistung und Stabilität des lokalen Netzes zu steigern, um die Last des SAP-ERP-Systems zu kompensieren.

Es muss geprüft werden, dass die Richtlinien für den SAP-Router eingehalten werden. Vor allem die SAP-Router Routetabelle (bestehend aus Verbindungseinträgen) und die SAP-Router excecutable müssen durch folgende Maßnahmen geschützt werden:

- Die Routetabelle darf nicht unberechtigt geändert werden. Hierfür bietet das Betriebssystem unterstützende Einstellungen an. Der Standardname der Routetabelle ist saprouttab.
- Der SAP-Router muss für spezielle Verbindungen mit einem Passwort geschützt werden.
- Das Passwort wird in der Routetabelle eingetragen und wird unverschlüsselt gespeichert. Deshalb ist es zwingend erforderlich, ein Passwort zu benutzen, das in keinem persönlichen Bezug steht.

- Verbindungen, die ein Passwort für die SAP-Router-Verbindung verwenden, müssen verschlüsselt werden. SNC-Einträge fangen immer mit dem Buchstaben K (wie key) an. Verbindungen, die nicht SNC verwenden, sind in dem Fall zu blockieren.
- Es dürfen keine Wildcard-Verbindungen konfiguriert sein, also Verbindungen bei denen Quelle und Ziel nur mit * spezifiziert sind.
- Sofern kein nativer TCP/IP-Zugriff gewünscht ist, sondern SAP-Kommunikation (DIAG/SAPGUI, RFC, eventuell mit SNC) eingesetzt wird, sollten Verbindungseinträge statt mit D mit S erlaubt werden.

Die ausführbare Datei des SAP-Routers muss geschützt werden (SAP-Router auf Unix/Linux oder saprouter.exe unter Windows).

APP.4.2.M16 Umsetzung von Sicherheitsanforderungen für das Betriebssystem Windows (S)

Die SAP-spezifischen kritischen Benutzer <sid>adm, SAPService<sid> müssen jedoch genauso sicher wie andere administrative Benutzer verwaltet werden. Zudem muss der Zugriff auf die Ressourcen und die Administrationsrechte auf die erforderlichen Benutzer beschränkt werden.

Der Benutzer SAPService<sid> führt die für das SAP-ERP-System benötigten Windowsdienste aus. Dafür sind auf dem lokalen Rechner entsprechende Berechtigungen notwendig. Allerdings sollte eine interaktive Anmeldung nicht erlaubt sein. Darüber hinaus muss der Benutzer nicht in der lokalen Windowsadministratorengruppe enthalten sein. In Bezug auf diese Berechtigungen müssen die dazugehörigen Systemressourcen des SAP-ERP-Systems geschützt werden. Das beinhaltet Dateien, Prozesse und gemeinsam genutzten Speicher zu schützen.

Windowsgruppen und -Benutzer in einer SAP-ERP-Systemumgebung

Windows unterscheidet zwischen Domaingruppen und lokalen Gruppen. In der Windowsdomain gibt es lokale, globale und allgemeine Domains. Domaingruppen sind innerhalb einer Windowsdomain gültig und nicht nur auf einem Server. Es ist notwendig, die Domainbenutzer, abhängig von ihren Aufgaben, in unterschiedlichen Aktivitätsgruppen zu bündeln. Der Domainadministrator kann die Aktivitätsgruppen auf andere Bereiche exportieren, sodass der jeweilige Benutzer auf alle Ressourcen zugreifen kann, die er benötigt, um das SAP-ERP-System zu verwalten. Der Name der globalen Standarddomaingruppe für SAP-ERP-Systemadministratoren ist definiert als SAP_<SID>_GlobalAdmin.

Lokale Benutzergruppen sowie lokale Benutzer existieren auf einem Server nur lokal. Während der Installation eines SAP-ERP-Systems werden die Benutzerrechte an lokale Benutzer zugewiesen. Zum Beispiel erhält der Benutzer <sid>adm die Benutzerberechtigung, sich direkt als Dienst anzumelden. Allerdings sollten für eine einfachere Benutzeradministration und für eine bessere Ressourcennutzung des Servers die Benutzerberechtigungen lokalen Gruppen zugeordnet werden. Danach werden diese den entsprechenden Domainbenutzern und Domaingruppen der lokalen Gruppe zugewiesen.

Hinweis: Wenn lokale Benutzergruppen oder ein einzelner lokaler Benutzer auf einem Domaincontroller definiert wurden, ist die Gruppe oder der Benutzer auf allen Domaincontrollern innerhalb der Domain bekannt. Deshalb muss es vermieden werden, SAP-ERP-Systeme auf Domaincontrollern zu installieren.

Die folgenden drei Beziehungen können zwischen dem Benutzer, der lokalen Gruppe und der Domaingruppe bestehen:

- Ein lokaler Benutzer kann nur ein Mitglied einer lokalen Gruppe sein.
- Ein Domainbenutzer kann Mitglied einer lokalen Gruppe und einer Domaingruppe sein.
- Eine Domaingruppe kann in eine lokale Gruppe eingeschlossen werden. Es können auch Domaingruppen zu anderen Windowsdomains exportiert werden.

SAP-ERP-Systeme in einem Windowsdomainkonzept

Es sollten zwei getrennte Domains erstellt werden: Eine Domain für die Institution und eine für das SAP-ERP-System. Zwischen den beiden Domains sollte eine vertrauensvolle Beziehung (trusted relationship) eingerichtet werden, damit ein Single-Sign-On (SSO) möglich ist. In der Institutionsdomain sind die Domainbenutzer (einschließlich der SAP-ERP-Systembenutzer) und die Domainadministratoren einzurichten. In der SAP-Domain sind die SAP-ERP-Systemserver, Dienste und Administratoren einzurichten, einschließlich:

- SAP-ERP-Systemapplikation und Datenbankserver,
- SAP-ERP-System und Datenbankdienste,
- SAP-ERP-Systemadministratoren,
- Windowsadministratoren sowie
- SAP-Domainadministratoren.

Es wird empfohlen, auch separate Domains für die Institutionsdaten und das SAP-ERP-System zu etablieren. Des Weiteren sollte das vertrauenswürdige Windowsdomainkonzept für bestimmte SAP-spezifische Funktionen und spezielle Windowsdienste verwendet werden, die für eine vertrauenswürdige Beziehung zwischen den Domains nötig sind.

Sicherung der relevanten Daten in einem SAP-ERP-System

Unabhängig davon, ob das SAP-ERP-System zentral installiert ist oder als verteiltes System besteht, sollte eine Domain eingerichtet werden, die die SAP-ERP-System-Applikation und den Datenbankserver enthält. Der SAP-ERP-System-Server sollte in einer Windowsdomain installiert werden. Für kurzfristige Testinstallationen oder Demonstrationszwecke könnte das zentrale SAP-ERP-System installiert werden, das sich nicht in einer Windowsdomain befindet. Das ist jedoch nur für ein begrenztes Szenario zu empfehlen. Es ist schwierig, ein Domainkonzept auf einem System einzuführen, das bereits genutzt wird. In der zentralen Installation auf dem Server in einer Domain sind alle SAP-ERP-Systemadministratoren Mitglieder der lokalen Gruppe SAP_<SAPSID>_LocalAdmin. Bei einer verteilten Installation mit mehreren Servern in der Domain ist die globale Gruppe für das SAP-ERP-System einzurichten (SAP_<SAPSID>_GlobalAdmin). Diese Gruppe ist Mitglied der lokalen Gruppen des Servers und beinhaltet die SAP-ERP-Systemadministratoren. Das vereinfacht die Administration der Client- oder Serverumgebung, da neue Benutzer, die SAP-ERP-Systemadministrationsrechte benötigen, nur Mitglieder der lokalen Gruppe werden.

APP.4.2.M17 Umsetzung von Sicherheitsanforderungen für das Betriebssystem Unix (S)

Es sollten Sicherheitsmaßnahmen realisiert werden, wenn die folgenden Objekte, Dateien oder Services genutzt werden:

- **SUID/SGID-Programme:** Es sollten nur die SENDMAIL-Versionen genutzt werden, in dem bekannte Fehler korrigiert wurden (oder ähnliche SUID-Programme).
- **Passwortdatei (passwd):** Es ist nur eine Shadow-Passwortdatei zu verwenden, die nur dem Benutzer Root-Zugriff auf die Passwortinformationen genehmigt.
- **Network Information System (NIS)**: Es sollten sichere Alternativen wie LDAP (mit SSL/TLS) oder Kerberos genutzt werden.
- **Network File System (NFS):** Es bestehen Sicherheitsrisiken, wenn dieser Service verwendet wird. Es sollten daher keine Verzeichnisse exportiert werden, die SAP-Daten zu beliebigen Empfängern enthalten und NFS nutzen. Es sollte nur zu bekannten und vertrauenswürdigen Systemen exportiert werden. Schreibberechtigungen müssen für NFS-Pfade sehr sorgfältig zugewiesen werden und es sollte vermieden werden, dass die Home-Verzeichnisse der Benutzer über NFS verteilt werden.

Insgesamt müssen folgende Punkte berücksichtigt werden:

- Alle nicht genutzten Dienste müssen deaktiviert werden.
- Es sollte keine direkte Anmeldung mit der Administrator-UserID root erlaubt sein. Alle Benutzeranmeldungen sollten personalisiert erfolgen. Tätigkeiten mit root-Rechten sollten über sudo entsprechend protokolliert werden.
- Es dürfen keine Verzeichnisse, die SAP-Daten an beliebige Empfänger mit NFS enthalten, exportiert werden. Der Transport sollte nur an vertrauenswürdige Systeme erfolgen.
- Schutz der folgenden Benutzer: root, <sid>adm, <db><sid> und DAAADM. Diese Benutzer sollten die einzigen Benutzer sein, die auf dem Applikationsserver und auf der Hauptinstanz existieren. Nach der Installation ist der Benutzer <db><sid> auf dem Applikationsserver zu sperren.
- Für kritische Benutzer ist die .rhosts-Datei zu leeren und die Berechtigung 000 zuzuweisen.
- Entweder ist die Datei /etc/hosts.equiv zu löschen oder es ist sicherzustellen, dass sie leer ist.
- Das Betriebssystem muss mit den entsprechenden sicherheitsrelevanten Patches auf dem aktuellen Stand gehalten werden.

Unter Unix/Linux müssen die Zugriffsberechtigungen für SAP-ERP-Systemverzeichnisse festgelegt werden. Es wird empfohlen, die Datei- und Verzeichniszugriffsrechte entsprechend der folgenden Tabelle zu setzen:

SAP-Verzeichnis oder Dateien	Zugriffsrechte in Oktalform	Eigentümer	Gruppe
/<sapmnt>/<SAPSID>/exe	755	<sapsid>adm	sapsys
/<sapmnt>/<SAPSID>/exe/saposcol	755	root	sapsys
/<sapmnt>/<SAPSID>/global	700	<sapsid>adm	sapsys
/<sapmnt>/<SAPSID>/profile	755	<sapsid>adm	sapsys
/usr/sap/<SAPSID>	751	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/<instance ID>	755	<sapsid>adm	sapsys
/usr/sap/<SAPSID>	750	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/<instance ID>/sec	700	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/SYS	755	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/SYS/*	755	<sapsid>adm	sapsys
/usr/sap/trans	775	<sapsid>adm	sapsys
/usr/sap/trans/*	770	<sapsid>adm	sapsys
/usr/sap/trans/.sapconf	775	<sapsid>adm	sapsys
<home directory of <sapsid>adm>	700	<sapsid>adm	sapsys
<home directory of <sapsid>adm>/*	700	<sapsid>adm	sapsys

APP.4.2.M18 Abschaltung von unsicherer Kommunikation (S)

Jede Information, die als vertraulich klassifiziert ist, sollte verschlüsselt übertragen werden. Hierzu zählen beispielsweise Passwörter, die grundsätzlich nie unverschlüsselt über unsichere Netze übertragen werden dürfen. Die sichere Datenübertragung erfolgt über eine verschlüsselte Kommunikation, z. B. über aktuelle Implementierungen von SSL/TLS oder SNC.

Secure Network Communication (SNC)

SNC schützt die Datenkommunikationspfade zwischen verschiedenen Clients- und Serverkomponenten des SAP-ERP-Systems, die das SAP-Protokoll RFC oder DIAG verwenden. SNC bietet durch eine Ende-zu-Ende-Verschlüsselung Sicherheit auf der Anwendungsebene. Die gesamte Kommunikation zwischen zwei mit SNC geschützten Komponenten wird gesichert, z. B. zwischen dem SAP GUI for Windows und dem Anwendungsserver. SNC bietet drei Schutzstufen an:

- Authentisierung (geringer Schutz): Das System verifiziert die Identität der Kommunikationspartner

- Integrität (mittlerer Schutz): Das System bemerkt, wenn Daten geändert oder manipuliert wurden.
- Vertraulichkeit (hoher Schutz): Die übertragenen Daten werden vom System verschlüsselt.

Das Sicherheitsprodukt von SNC ist die SAP Cryptographic Library, die SNC-Verbindungen zwischen Systemkomponenten (RFC-Verbindungen) schützt.

Secure-Sockets-Layer (SSL)

Mit SSL erfolgt die Absicherung der HTTP-Verbindungen zum und vom AS ABAP. Die Daten zwischen den beiden Partnern (Client und Server) werden verschlüsselt übertragen und sie können sich gegenseitig authentisieren. Die SSL-Informationen werden über diese Funktionen gepflegt:

- Profilparameterpflege (Transaktion RZ10)
- Trust-Manager (Transaktion STRUST)
- Pflege der RFC-Destinationen (Transaktion SM59)
- ICM Monitor (Transaktion SMICM)

Das SSL-Protokoll verwendet das Public-Key-Verfahren. Daher muss der Server ein Public-Key-Schlüsselpaar sowie ein entsprechendes Public-Key-Zertifikat besitzen. Ein Schlüsselpaar und ein Zertifikat benötigt er, um sich als Serverkomponente auszuweisen. Das weitere Schlüsselpaar und Zertifikat wird gebraucht, um sich gegebenenfalls als Client-Komponente auszuweisen. Diese Schlüsselpaare und Zertifikate sind in den eigenen persönlichen Sicherheitsumgebungen (Personal Security Environments; PSEs) des Servers abgelegt, in der SSL-Server-PSE bzw. der SSL-Client-PSE.

Transport Layer Security (TLS)

TLS sichert die Transportschicht von Verbindungen zwischen den SAP-NetWeaver-Systemkomponenten ab. Mithilfe von TLS wird die Datenübertragung verschlüsselt und die Kommunikationspartner können sich gegenseitig authentisieren. Bei Verbindungen, die Internetprotokolle wie HTTP verwenden, wird das SSL-Protokoll benutzt. Bei SAP-Protokollen wie RFC oder Dialog wird SNC eingesetzt. TLS bietet drei Schutzstufen an:

- Authentisierung: Die Kommunikationspartner können authentisiert werden. Bei SSL können die Verbindungen so eingerichtet werden, dass nur die Serverkomponente der Verbindung authentisiert wird oder dass beide Partner authentisiert werden. Bei SNC werden immer beide Partner authentisiert
- Datenintegrität: Die zwischen dem Client und dem Server übertragenen Daten sind geschützt, sodass jede Manipulation der Daten aufgedeckt wird.
- Vertraulichkeit der Daten: Die zwischen dem Client und dem Server übertragenen Daten sind auch verschlüsselt, wodurch der Schutz der Vertraulichkeit erreicht wird.

APP.4.2.M19 Definition der Sicherheitsrichtlinien für Benutzer (S)

Für unterschiedliche Benutzer können spezifische Sicherheitsrichtlinien für Passworte und Anmelderestriktionen eingestellt werden. Zum Beispiel sind für technische Benutzer im Gegensatz zu Dialogbenutzern abwärtskompatible Passwörter erforderlich und Benutzer mit kritischen Berechtigungen müssen durch starke Passwortregeln höher abgesichert werden. Die Zuordnung der Sicherheitsrichtlinien kann benutzer- und mandantenspezifisch erfolgen.

Die Sicherheitsrichtlinien lösen die Steuerung der Passwortregeln, Passwortänderungen und Anmelderestriktionen durch Profilparameter ab. Wird einem Benutzer keine Sicherheitsrichtlinie explizit zugeordnet, gelten für ihn die Richtlinien nach den gesetzten Profilparametern. Jedoch können auch nicht alle Profilparameter als Sicherheitsrichtlinie abgebildet werden.

Die Sicherheitsrichtlinien können mit SAP NetWeaver 7.31 umgesetzt werden. Weitere Informationen dazu finden sich im SAP-Hinweis 2018918 – Benutzerspezifische Einstellungen zu Kennwortregeln, Kennwortänderungen und Anmelderestriktionen (siehe [SECNOTE]).

Sicherheitsrichtlinien definieren

Sicherheitsrichtlinienattribute und die zugehörigen Vorschlagswerte sind in den Sicherheitsrichtlinien definiert und können wie folgt angepasst werden.

Vorgehen über SECPOL:

- Transaktion SECPOL ausführen.
- Bearbeitungsmodus aktivieren und neue Einträge wählen.
- Im Feld Sicherheitsrichtlinie einen Namen definieren und im Feld Kurztext eine Beschreibung eintragen.
- Für die neue Sicherheitsrichtlinie müssen Attribute definiert werden: Neue Einträge wählen.
- In der Tabelle werden die Richtlinienattribute und Attributwerte gepflegt.
- Button Effektiv: Alle tatsächlich aktiven Attribute werden angezeigt.
- Button Verzichtbare Einträge: Anzeige der Attributwerte, die sich nicht von den globalen Einträgen unterscheiden.
- Eine Übersicht der Sicherheitsrichtlinienattribute für die Steuerung der Kennwortregeln, Kennwortänderungen und Anmelderestriktionen findet sich im SAP Help Portal [SAPSECPO].

Sicherheitsrichtlinien Benutzern zuordnen

Die Zuordnung der definierten Sicherheitsrichtlinien zu Benutzern erfolgt über die Benutzerpflege (SU01) oder die Massenbenutzerpflege (SU10).

Vorgehen über die SU01:

- Transaktion SU01 ausführen.
- Ausgewählten Benutzer im Änderungsmodus öffnen.
- Registerkarte Logondaten auswählen.
- Im Feld Sich.-Richtlinie eine definierte Sicherheitsrichtlinie für den Benutzer auswählen.
- Eingaben sichern.

Vorgehen über die SU10:

- Transaktion SU10 ausführen.
- Alle Benutzer in der Spalte Benutzer eintragen.
- (Alle) Benutzer ändern wählen.
- Im Feld Sich.-Richtlinie eine definierte Sicherheitsrichtlinie für alle Benutzer auswählen.
- Eingabe sichern.

Verwendungsnachweis von Sicherheitsrichtlinien

Mit dem Report RSUSR_SECPOL_USAGE (über SA38) werden die Benutzer und ihre zugeordneten Sicherheitsrichtlinien dargestellt. Der Report lässt sich ebenfalls über das Benutzerinformationssystem (SUIM) öffnen. Hier muss die Struktur unter Benutzerinformationssystem bis Benutzer nach komplexen Selektionskriterien geöffnet werden. Weitere Informationen dazu finden sich im SAP-Hinweis 1611173 – SUIM| Auswertung von Sicherheitsrichtlinien für Benutzer (siehe [SECNOTE]).

APP.4.2.M20 Sichere SAP-GUI-Einstellungen (S)

Folgenden Maßnahmen müssen eingestellt werden, um die Sicherheit der SAP-GUI-Nutzung zu erhöhen:

- Es ist immer die neueste verfügbare SAP-GUI-Version auf allen Endbenutzer-Arbeitsstationen einzusetzen.
- Die SAP-GUI-Sicherheitseinstellungen sind als customized und Standardaktionen als ask einzustellen.

Es wird empfohlen, die dazugehörigen Administratorregeln beizubehalten und zu verteilen. So ist es möglich, homogene Sicherheitseinstellungen auf allen Arbeitsstationen zu erreichen und den Benutzer von unnötigen Pop-ups zu befreien. Des Weiteren sollten die folgenden Einstellungen umgesetzt und implementiert werden:

- kein Zugriff auf die Registry
- eingeschränkte Konfigurationsoptionen der lokalen SAP-GUI-Installation wie über diese SAP-Hinweise (siehe [SECNOTE]):
- SAP-Hinweis 762661 - SAP Logon: Registerkarten/Bearb.funktion anzeigen/ausblenden
- SAP-Hinweis 867260 - Scripting: Plattenzugriff über Registry-Schlüssel deaktiv.
- SAP-Hinweis 1669256 - SAP GUI 7.30: Registry-Werte und Optionsdialog schreibgeschützt

APP.4.2.A21 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

APP.4.2.M22 Schutz des Spools im SAP-ERP-System (S)

Der Spool-Administrator ermöglicht einen reibungslosen Betrieb der SAP-Ausgabe-Landschaft. Zu den Aufgaben des Spool-Administrators gehören:

- administrieren von Ausgabegeräten,
- definieren einer ausfallsicheren Spool-Server-Landschaft,
- überwachen des korrekten Ausgabebetriebes.

Die Spool-Administration der Ausgabegeräte erfolgt mit der Transaktion SPAD. Schützenswerte Spool-Einträge sind zum Beispiel Einträge aus dem Bereich Finanzwesen.

Vergabe von Spool-Berechtigungen

Will ein Benutzer im SAP-ERP-System etwas ausdrucken, braucht er dazu die entsprechenden Berechtigungen. Diese werden über das Berechtigungsobjekt S_SPO_DEV gesteuert. Wird S_SPO_DEV mit den Gesamtberechtigungen (*) erteilt, hat der Benutzer Zugriff auf alle Drucker im SAP-ERP-System. Weitere Einstellungen von Spool-Berechtigungen erfolgen über die Aktivitäten und Wertezuweisungen der Berechtigungsobjekte S_ADMI_FCF und S_SPO_ACT. Auszuführende Aktionen werden mit dem Berechtigungsfeld SPOACTION festgelegt. Das Berechtigungsfeld SPOAUTH ordnet die Spool-Einträge zu. Eine Übersicht über benutzereigenen Spool-Aufträge kann jeder Benutzer mit der Transaktion SP02 aufrufen.

Es ist zu vermeiden, dass Benutzer dazu berechtigt sind, (geschützte) Spool-Aufträge von anderen Benutzern aufzurufen (Transaktion SP01 oder SP01O). Die folgenden Beispiele für Spool-Berechtigungen sollten im Regelbetrieb nur dem Spool-Administrator zugeordnet werden.

Berechtigungen zur Änderung des Inhabers einer Spool-Anfrage:

- Berechtigungsobjekt 1: S_TCODE mit TCD = SP01
- Berechtigungsobjekt 2: S_ADMI_FCD mit S_ADMI_FCD = SP01 or SP0R
- Berechtigungsobjekt 3: S_SPO_ACT mit SPOACTION = USER

Berechtigungen zum Umleiten des Druckauftrages zu einem anderen Drucker:

- Berechtigungsobjekt 1: S_TCODE mit TCD = SP01

- Berechtigungsobjekt 2: S_ADMI_FCD mit S_ADMI_FCD = SP01or SP0R
- Berechtigungsobjekt 3: S_SPO_ACT mit SPOACTION = REDI

Berechtigungen zum Exportieren eines Druckauftrages:

- Berechtigungsobjekt 1: S_TCODE mit TCD = SP01
- Berechtigungsobjekt 2: S_ADMI_FCD mit S_ADMI_FCD = SP01oder SP0R
- Berechtigungsobjekt 3: S_SPO_ACT mit SPOACTION = DOWN

Schritte zur benutzerübergreifenden Vergabe von Spool-Berechtigungen

Für den Fall, dass Benutzer in Spool-Aufträgen auf andere Benutzer zugreifen sollen, müssen bestimmte Einstellungen in der SP01 durch den Spool-Administrator durchgeführt werden. Voraussetzung dafür ist, dass dem Benutzer, der die Spoolaufträge eines anderen Benutzers bearbeiten soll, drei Berechtigungsobjekte mit der entsprechenden Ausprägung zugewiesen werden:

1. Das Berechtigungsobjekt S_ADMI_FCD mit dem Wert SPOR (= Benutzerübergreifende Verwaltung von Spool-Aufträgen).
2. Das Berechtigungsobjekt S_SPO_ACT für die Aktion mit BASE mit dem entsprechenden Wert, z. B. Name des anderen Benutzers.
3. Das Berechtigungsobjekt S_SPO_ACT mit der Ausprägung, die der Benutzer erhalten soll: DISP (Anzeigen des Inhaltes), DELE (Löschen des Spoolauftrages), PRNT (einmaliges Drucken eines bisher nicht gedruckten Auftrages), PEPR (Nachdrucken eines Auftrages)

Der Benutzer kann somit alle Druckaufträge des anderen Benutzers bearbeiten. Der andere Benutzer kann die Druckaufträge jedoch schützen, indem das Feld Berechtigung in der SP01 mit dem Wert GEHEIM gepflegt wird. Das geht nicht, wenn der andere Benutzer über die Berechtigung GEHEIM verfügt.

Schutz des TemSe-Inhaltes

Die Datenablage TemSe wird vom SAP-Spoolsystem genutzt, um Datenausgaben und Zwischenergebnisse von Hintergrundjobs zwischenzuspeichern. Die folgenden Berechtigungen sollten geprüft und entsprechend zugewiesen werden, damit unbefugte Benutzer nicht zu viele Berechtigungen haben.

Berechtigungen zur Anzeige von TemSe-Inhalten:

- Berechtigungsobjekt 1: S_TCODE mit TCD = SP11 oder TCD = SP12
- Berechtigungsobjekt 2: S_TMS_ACT mit STMSACTION = REA und (STMSOWNER = GRP oder OCL) und STMSOBJECT = SPOOL*

Das Druckerkonzept sollte durch eine Namenskonvention vereinheitlich werden.

APP.4.2.M23 Schutz der SAP-Hintergrundverarbeitung (S)

Für die Verwaltung der Batch-Jobs (Hintergrundjobs) ist der Batch-Job-Administrator verantwortlich. Hintergrundjobs können über die Transaktionen SM36, SA38 und über weitere Anwendungstransaktionen eingeplant werden. Batch-Jobs können nach folgenden Kriterien eingeteilt werden:

- Art des Jobs (technisch, funktional),
- periodische Nutzung (stündlich, täglich, wöchentlich, monatlich),
- sporadische Nutzung (ja/nein),
- Kurzbeschreibung des Jobs,
- Zuordnung zu Rolle, Benutzer oder Position.

Benutzer benötigen keine speziellen Berechtigungen, um ihre eigenen Hintergrundjobs anlegen oder ändern zu können. Die Freigabe von eigenen oder anderen Hintergrundjobs wird über ein spezielles Berechtigungsobjekt (S_BTCH_JOB) geschützt. Der generelle Zugriff auf Hintergrundjobs von anderen Benutzern benötigt ebenfalls spezielle Berechtigungen. Die drei wichtigsten Berechtigungsobjekte für Hintergrundjobs sind:

- **S_BTCH_JOB** Steuerung der Zugriffsrechte von Hintergrundjobs für den eigenen und für andere Benutzer. Alle kritischen Operationen für die Verwaltung der Hintergrundverarbeitung werden über dieses Objekt geprüft. Mit dem Objekt können keine Hintergrundjobs eingeplant werden. Spezielle Berechtigungen:
- Freigabe von eigenen Hintergrundjobs oder von anderen Benutzern:
  Berechtigung: S_BTCH_JOB mit JOBACTION = RELE
- Ändern der Hintergrundjobs von anderen Benutzern:
  Berechtigung: S_BTCH_JOB mit JOBACTION = MODI
- Löschen der Hintergrundjobs von anderen Benutzern:
  Berechtigung: S_BTCH_JOB mit JOBACTION = DELE
- Anzeigen der Hintergrundjobdefinitionen von anderen Benutzern:
  Berechtigung: S_BTCH_JOB mit JOBACTION = SHOW
- **S_BTCH_NAM** Das Berechtigungsobjekt berechtigt dazu, einen Hintergrundjob im Namen eines anderen Benutzers zu vergeben. Diese Benutzer müssen in den Berechtigungen (Feld BTCUNAME) eingetragen werden. Batch-Administratoren können somit die Hintergrundjobs unter einem technischen Benutzer laufen lassen. Spezielle Berechtigung:
- Job-Steps unter einem anderen Benutzer einplanen:
  Berechtigung: S_BTCH_ADM mit BTCUNAME = <Benutzererkennung>
- **S_BTCH__ADM** Umfassende Berechtigungen für den Batch-Job-Administrator. Das ermöglicht unter anderem die systemweite Übersicht aller Hintergrundjobs, das Durchführen aller Funktionen für Hintergrundjobs und den Zugriff auf Hintergrundjobs in allen Mandanten. Spezielle Berechtigung:
- Administratorberechtigung: S_BTCH_ADM mit BTCADMIN = Y

Einplanen von Hintergrundjobs

Alle Schritte für zeitgesteuerte wiederkehrende Hintergrundjobs sind an Hintergrundbenutzer zu binden. Hintergrundjobs sollten durch Systembenutzer (Typ System) nach ihren Funktionsbereichen eingeplant werden. Die verwendete Benutzer-ID wird als Benutzertyp SYSTEM angelegt. Hintergrundbenutzer sind durch die Namenskonvention von anderen Benutzern zu unterscheiden.

Der Benutzer, der Jobs für einen Systembenutzer einplant, muss diese Berechtigungen erhalten: Berechtigungsobjekt S_BTCH_NAM und im Feld BTCUNNAME = Name des auszuführenden Benutzers (z. B. Systembenutzers). Ein Risiko für kontinuierlichen und störungsfreien Betrieb besteht, wenn Hintergrundbenutzer versehentlich gesperrt werden oder die Kennwörter ablaufen.

Empfehlungen:

- Die Berechtigungsobjekte S_BATCH_ADM und S_BATCH_JOB mit dem Wert RELE sollten beim Endbenutzer nicht mehr berechtigt werden.
- Batch-Administratoren sind berechtigungstechnisch auf die entsprechenden Systemuser einzuschränken. Das geschieht über das oben beschriebene Berechtigungsobjekt S_BTCH_NAM, in das der Batch-Benutzername hinterlegt werden kann.
- Technische Benutzer sollten nicht das SAP-Profil SAP_ALL zugewiesen bekommen.
- Eine Anzeigeberechtigung für die Transaktion SM37 "Übersicht über Hintergrundjobs" ohne Jobfreigabe ist bei den entsprechenden Benutzern als nicht kritisch anzusehen.

APP.4.2.M24 Aktivierung und Absicherung des Internet Communication Frameworks (S)

Mit dem Internet Communication Framework (ICF) ist es möglich, von einem SAP-ERP-System über http, https und SMTP-Anfragen mit anderen Systemen zu kommunizieren. Auf die webbasierten Anwendungen eines ABAP-Systems kann vom Webbrowser aus zugegriffen werden. Dieser Inhalt wird durch die Dienste des ICFs gepflegt und kann über die Transaktion SICF verwaltet werden. Die Dienste sind in einer dateisystemähnlichen Baumstruktur hierarchisch angeordnet.

Um unautorisierte Zugriffe zu vermeiden, müssen die folgenden Einstellungen für ICF-Dienste umgesetzt werden:

- Es sind nur die ICF-Dienste zu aktivieren, die für die Geschäftsprozesse wirklich notwendig sind. Vor allem auf produktiven SAP-ERP-Systemen sollten nicht alle ICF-Dienste aktiviert werden.
- Alle ICF-Dienste müssen überprüft werden, für die keine Benutzerauthentisierung erforderlich ist. Einschließlich der ICF-Dienste /sap/public mit gespeicherten Anmeldedaten.

In der folgenden Tabelle sind alle ICF-Dienste aufgeführt, die zu deaktivieren sind, falls diese im aktuellen Release vorhanden sind und nicht für einen Geschäftsprozess verwendet werden:

ICF-Dienst	**SAP-Hinweis (siehe [SECNOTE])**
/sap/bc/soap/rfc	1394100 - Sicherheitshinweis:Zugriff auf RFC-fähige Bausteine via SOAP
/sap/bc/echo	626073 - Nicht freigegebene Internet Communication Framework Services
/sap/bc/FormToRfc	626073 - Nicht freigegebene Internet Communication Framework Services
/sap/bc/report	626073 - Nicht freigegebene Internet Communication Framework Services
/sap/bc/xrfc	626073 - Nicht freigegebene Internet Communication Framework Services
/sap/bc/xrfc_test	626073 - Nicht freigegebene Internet Communication Framework Services
/sap/bc/error	626073 - Nicht freigegebene Internet Communication Framework Services 517484 - Inaktive Services im Internet Communication Framework
/sap/public/bc/its/mobile/rfid	219753 - Sicherheitsschwachstellen in einem zu SAP ITS Mobile gehörigen ICF-Service
/sap/bc/webrfc	865853 - WebReporting/WebRFC ab NW2004s veraltet
/sap/bc/bsp/sap/bsp_model	887164 - BSP-Testanwendungen in Produktivsystemen
/sap/bc/bsp/sap/certreq	1417568 - Unautorisierte Änderung von Inhalten in CERTREQ und CERTMAP
/sap/bc/bsp/sap/certmap	1417568 - Unautorisierte Änderung von Inhalten in CERTREQ und CERTMAP
/sap/bc/gui/sap/its/CERTREQ	1417568- Unautorisierte Änderung von Inhalten in CERTREQ und CERTMAP
/sap/bc/gui/sap/its/CERTMAP	1417568- Unautorisierte Änderung von Inhalten in CERTREQ und CERTMAP
/sap/bc/bsp/sap/bsp_veri	1422273 Unautorisierte Modifikation von angezeigtem Inhalt in BSP
/sap/bc/bsp/sap/bsp_verificatio	517484 - Inaktive Services im Internet Communication Framework
/sap/bc/bsp/sap/icf	1422273 - Unautorisierte Modifikation von angezeigtem Inhalt in BSP

ICF-Dienst	SAP-Hinweis (siehe [SECNOTE])
/sap/bc/bsp/sap/it0*	887164 - BSP-Testanwendungen in Produktivsystemen 517484 - Inaktive Services im Internet Communication Framework
/sap/bc/bsp/sap/htmlb_samples	887164- BSP-Testanwendungen in Produktivsystemen 517484 - Inaktive Services im Internet Communication Framework
/sap/bc/bsp/sap/itmvc2	887164 - BSP-Testanwendungen in Produktivsystemen
/sap/bc/bsp/sap/itsm	887164 - BSP-Testanwendungen in Produktivsystemen
/sap/bc/bsp/sap/sbspext_phtmlb	887164 - BSP-Testanwendungen in Produktivsystemen 517484 - Inaktive Services im Internet Communication Framework
/sap/bc/bsp/sap/sbspext_htmlb	887164 - BSP-Testanwendungen in Produktivsystemen 517484 - Inaktive Services im Internet Communication Framework
/sap/bc/bsp/sap/sbspext_table	887164 - BSP-Testanwendungen in Produktivsystemen
/sap/bc/bsp/sap/sbspext_xhtmlb	887164 - BSP-Testanwendungen in Produktivsystemen
/sap/bc/bsp/sap/system_private	887164 - BSP-Testanwendungen in Produktivsystemen
/sap/bc/bsp/sap/system_public	887164 - BSP-Testanwendungen in Produktivsystemen
/sap/bc/IDoc_XML	1487606 - IDoceingang via HTTP/SOAP
/sap/bc/srt/IDoc	1487606 - IDoceingang via HTTP/SOAP

ICF-Kommunikation über SSL

Es wird empfohlen für die ICF-Kommunikation SSL für alle ICF-Dienste zu verwenden. SSL kann auch nur für einzelne ICF-Dienste konfiguriert werden (siehe APP.4.2.M18 Abschaltung von unsicherer Kommunikation).

ICF-Berechtigungen

Wenn Berechtigungen für ICF-Dienste vergeben werden, muss dabei auf die Funktionstrennung geachtet werden. Benutzer, die auf ICF-Dienste Zugriff haben, sollten nicht über die Dialogschnittstelle (SAPGUI) auf das SAP-ERP-System zugreifen können. Für das Berechtigungsobjekt S_ICF sollten die folgenden Werte gesetzt sein:

- Feld: ICF_Field = SERVICE
- Feld: ICF_VALUE = muss die Zeichenkette genutzt werden, die im betroffenen ICF-Dienst unter Service-Daten/Service Optionen/SAP-Berechtigung eingetragen ist.

Berechtigungen für die Transaktion SICF können über das Berechtigungsobjekt S_ADMI_FCD mit dem Feldwert S_ADMI_FCD = ICFA gesteuert werden. Über die Transaktion SICF kann der Administrator die Funktionen für SICF aktivieren oder deaktivieren:

- Recording-Funktion nicht erlauben,
- Trace-Funktion nicht erlauben,
- Debugging-Funktion nicht erlauben,
- Laufzeitanalyse-Funktion nicht erlauben.

Folgenden Sicherheitsmaßnahmen sind zusammenfassend für die Aktivierung der ICF-Dienste zu beachten:

- Nur die ICF-Dienste aktivieren, die wirklich benötigt werden.
- Authentisierungsmethoden und Anmeldefolgen für Benutzer von Services definieren.
- Für die ICF-Kommunikation ist SSL zu verwenden.
- ICF-Berechtigungen sind nur restriktiv zu vergeben.

- Fehlerseiten sollten für ICF-Dienste so konfiguriert werden, dass keine internen Informationen ersichtlich sind.

Session Management

Das Secure-Session-Management (Transaktion SICF_SESSIONS) muss für alle Mandanten aktiviert werden. Als Fallback sollte der Parameter icf/user_recheck=1 gesetzt werden. Allerdings wird dann bei jeder neuen http(s)-Anfrage eine neue Anmeldung (eventuell per SAP-Logon-Ticket) durchgeführt, was zu Leistungseinbußen führen kann. icf/user_recheck=1 ist aber unwirksam, solange das Secure-Session-Management aktiv ist.

APP.4.2.M25 Sichere Konfiguration des SAP Web Dispatchers (S)

Der SAP Web Dispatcher sollte nicht der erste Einstiegspunkt aus dem Internet sein. Außerdem sollten folgende Einstellungen vorgenommen werden:

- Der Web Dispatcher muss immer auf dem aktuellen Stand sein (siehe SAP-Hinweis 538404 - Sammelhinweis SAP Web Dispatcher, siehe [SECNOTE]).
- Es sollte eine eigene Fehlerseite konfiguriert werden, damit Informationen (technischer Grund der Fehlermeldung) für potenzielle Angreifer nicht unnötig offengelegt werden. Dazu muss der Parameter icm/HTTP/error_templ_path = /usr/sap/<SID>/<Instance>/data/icmerror gesetzt werden. Alternativ kann auch der Parameter is/HTTP/show_detailed_errors to FALSE benutzt werden (an den Client werden keine Informationen weitergegeben).
- Der Web Dispatcher kann als URL-Filter mit Positivlisten verwendet werden. In jedem Fall müssen die folgenden URLs gefiltert werden, da sie Informationen über die Infrastruktur und Konfiguration zurückgeben:
    - D /sap/public/icman/*
    - D /SAP/public/ping
    - D /sap/public/icf_info/*

Der Zugriff auf Informationsseiten wird mit dem Parameter blockiert: D /sap/wdisp/info

Die Webadmin-Oberfläche wird mit den folgenden Parametern sicher konfiguriert:

- Die Verwendung des HTTPS-Ports verhindert es, dass Passwörter abgefangen werden. Die HTTPS-Port-Einstellungen sollten mit dem Parameter icm/server_port_<num> in der URL eingerichtet werden.
- Die Administration des Web Dispatchers sollte nur auf Ports erlaubt sein, die ein sicheres Protokoll (HTTPS) verwenden. In der URL ist ein HTTPS-Port zu benutzen. Für den Parameter icm/HTTP/admin_<num> muss die Option PORT gesetzt werden.
- Der Admin-Port konfiguriert einen Port, der nur im internen Netz erreichbar ist mittels des Parameters icm/HTTP/admin_<num> mit der Option PORT.
- Die Administration sollte nur unter einem bestimmten Hostnamen oder mit einer IP-Adresse aus dem internen Netz erlaubt werden. Dazu wird die Option HOST für den Parameter icm/HTTP/admin_<num> verwendet.
- Die Administration von Clients aus dem internen Netz muss eingeschränkt werden. Dazu wird die Option PORT für den Parameter icm/HTTP/admin_<num> benutzt.

Alle aktuellen Sicherheitseinstellungen für den SAP Web Dispatcher sind im SAP-Hinweis 87017 (siehe [SECNOTE]) zusammengefasst.

APP.4.2.M26 Schutz des kundeneigenen Codes im SAP-ERP-System (S)

SAP und andere Anbieter haben verschiedene Tools entwickelt, die kundeneigenen Code unter den Aspekten Qualität, Sicherheit und Quantität prüfen.

Die folgende Tabelle stellt die SAP-Prüftools für kundeneigenen Code vor:

Tools	Prüfung	Beschreibung
ABAP Test Cockpit (ATC)	Qualität des Codes	• neues Kontroll-Rahmenwerk, das statistische und dynamische Qualitätskontrollen des ABAP-Codes durchführt • ermöglicht Unit-Tests für ABAP-Programme • einzige Anlaufstelle zum Einstieg für alle statistischen Code-Kontroll-Tools • vollständige Integration mit der Entwicklungs-Workbench (z. B. SE80, SE24, SE38, SE11) und dem Transport-Management-Tool • korrigiert Bugs
Code Vulnerability Analyzer (CVA)	Sicherheit des Codes	• entwickelt vom Team, das auch die ABAP-Sprache entwickelt • stark in der Standard-Test-Infrastruktur integriert • identifiziert die bekannten Quellcoderisiken gemäß der Top 10 von OWASP • führt verschiedene Prüfungen durch, z. B. SQL Injection (Open SQL und ADBC), Code Injection (ABAP), OS Command Injection, Blackdoors & Authorizations
Usage & Procedure Logging (UPL)	Quantität des Codes	• auf dem Kernel basierte Protokollierungstechnik, um eine reale Nutzung des Systems zu erhalten • wird zum Aufrufen und Ausführen aller ABAP-Units verwenden • Grundlage zur Reduktion des kundeneigenen Codes (Deaktivierung und Reinigung)
SAP Solution Manager	Custom Code Lifecycle Management	• Die Ergebnisse aus der Prüfung des ATC und des UPL können für verschiedene Systeme im SAP Solution Manager zentral angezeigt werden. • ermöglicht einen Überblick über noch offene Ausnahmen von verschiedenen Konsolidierungssystemen • Eine unbestimmte Anzahl an SAP-ERP-Systemen kann über die gesamte Systemlandschaft abgebildet werden

Custom Code Lifecycle Management

Das Custom Code Lifecycle Management (CCLM) sowie ergänzende Tools sind seit dem SAP Solution Manager mit der Version 7.1 verfügbar. CCLM wurde entwickelt, um ABAP-Erweiterungen und Neuentwicklungen während des gesamten Lebenszyklus zu begleiten. Der Lebenszyklus startet, wenn ein Objekt (z. B. ein Programm, eine Transaktion oder eine Tabelle) entwickelt wird, geht über die Verwendung im Produktivsystem und erstreckt sich bis hin zur Nichtanwendung oder Neuausrichtung des Objektes. Der Kern des CCLM ist eine generische Bibliothek, die kundeneigene Codes klassifiziert und grundlegende Informationen enthält. Die generische Bibliothek mit allen Informationen ist über eine XML-Datei verfügbar (siehe SAP-Hinweis 1547237 – Technische Konfiguration des CCLM, [SECNOTE]). Der Datensammler erhält die Eigenschaften der kundeneigenen Codes automatisch von den angeschlossenen Systemen. Das kann über einen periodisch angelegten Hintergrundjob gesteuert werden.

Berechtigungen für das CCLM

Da der SAP Solution Manager die Informationen über die zu überwachenden Systeme in internen Tabellen speichert, kann auf sie schnell zugegriffen werden. Es sind jedoch bestimmte Berechtigungen

notwendig, um den SAP Solution Manager mit CCLM benutzen zu können. Falls SAP-Standardrollen für CCLM genutzt werden, müssen diese in den kundeneigenen Namensraum kopiert werden:

- SAP_CCLM_DIS: die SAP-Standardrolle enthält die Berechtigung CCLM im Anzeigemodus zu nutzen (keine Änderungen in der Konfiguration möglich).
- SAP_CCLM_ALL: die SAP-Standardrolle enthält das Berechtigungsobjekt SM_CC_AUTH mit dem Berechtigungsfeld SM_CC_LIB (Änderungen in der Konfiguration sind möglich).
- SAP_SMWORK_BASIC_CCLM: die SAP-Standardrolle enthält die Berechtigung auf das Workcenter zuzugreifen und die Basisberechtigung für das Berechtigungsobjekt CCLM.
- SAP_SMWORK_BASIC_CCLM: die SAP-Standardrolle enthält die Berechtigung auf das Workcenter Custom Code Lifecycle Management zuzugreifen.

Der kundeneigene Code sollte durch spezialisierte Prüfwerkzeuge auf Schwachstellen untersucht werden. Das Transportwesen sollte so konfiguriert werden, dass ungeprüfte Entwicklungen oder Programme mit identifizierten Schwachstellen nicht weitertransportiert werden.

APP.4.2.M27 Audit des SAP-ERP-Systems (S)

SAP-ERP-Systeme sollten regelmäßig auditiert werden. Die folgenden Empfehlungen sollten zur Vorbereitung für ein internes und externes Audit eingehalten werden:

- Es sollten aus den relevanten Vorschriften wie ITIL, BASEL II, SOX, FDA oder Datenschutz alle notwendigen Maßnahmen identifiziert werden.
- Die Revisionssicherheit der Systeme wird durch angemessene und effektive Sicherheitsmaßnahmen gewährleistet, insbesondere durch die Zuweisung von Berechtigungen. So sollten beispielsweise nicht uneingeschränkte Berechtigungen durch die Zuweisung des Profils SAP_ALL oder die Zuweisung von Debug- und Änderungsberechtigungen auf dem Produktivsystem vergeben werden.
- Protokolle und Traces sollten definiert und erfasst werden, z. B. die Prüfung der Datenschutzgesetze oder Einschränkungen der Produktionsumgebung. Das Protokollieren der Daten und der Zugriff auf Protokollierungsmöglichkeiten muss eingeschränkt werden.

Für das in der Institution bestehende Risikomanagementrahmenwerk muss ein Plan entwickelt werden, der allen relevanten regulatorischen Anforderungen entspricht. Demzufolge ist es für das Auditmanagement entscheidend, sich die Risikoinformationen anzeigen zu lassen, die von der Institution erfasst und dokumentiert wurden. Darüber hinaus müssen die folgenden Schritte durchgeführt werden:

- alle relevanten regulatorischen Anforderungen identifizieren,
- benötigte Protokolle und Traces definieren, den Security Audit Log (SAL) aktivieren und konfigurieren,
- Protokolle mit geeigneten Tools analysieren,
- Sicherheitsüberprüfungen wie Penetrationstests und Schwachstellenscans durchführen,
- Prüfung der verschiedenen Secure Operation Tracks:
- Infrastruktureinstellungen und Kommunikationsschnittstellen (Firewall, Dispatcher und Reserve-Proxy, Betriebssystem, RFC-Verbindungen, ALE, ICF, WS usw.),
- Benutzer und Berechtigungen überprüfen (Stichproben, SAP Access Control usw.).

Ist in einer Institution kein Rahmenwerk für das Risikomanagement definiert, muss das Auditmanagement seine eigene Bewertung über die Risikoeinträge anwenden und diese mit der Geschäftsleitung absprechen.

Der Leiter der internen Revision muss in der Lage sein, die risikobasierenden Pläne und die dafür erforderlichen Ressourcen zusammenzufassen. Der Vorstand und die leitenden Angestellten der Institution haben die Befugnis, die Arbeit der internen Revision zu überwachen.

APP.4.2.M28 Erstellung eines Notfallkonzeptes (S)

Die folgenden Schritte sind zur Vorbereitung und für den Einsatz des Notfallkonzepts für SAP-ERP-Systeme notwendig.

Vorbereitungen auf einen Zwischenfall

- Definition von Prozessen und Verantwortlichen,
- Durchführung von regelmäßigen Notfallübungen und Anpassung der Prozesse,
- Erstellen und Bearbeiten von Notfallbenutzern (siehe APP.4.2.M29 *Einrichten eines Notfallbenutzers*) für alle relevanten Systeme,
- Sammlung von notwendigen Protokollen und Daten,
- Definition von Regeln und Auslösern zur Identifizierung und Klassifizierung von Vorfällen,
- Vorbereitung für technische und nichttechnische (z. B. gesetzliche Vorschriften) Folgeaktivitäten und Verbesserungen.

Etablierung eines Datensicherungs- und Wiederherstellungskonzeptes

Ein wesentlicher Punkt der Notfallvorsorge ist die Datensicherung der SAP-ERP-Systeme. Demzufolge müssen Verantwortlichkeiten und Prozessabläufe in einem Konzept definiert werden. Das Datensicherungskonzept muss ständig verfügbar sein, damit es im Notfall auch schnell umgesetzt werden kann. Die folgenden Informationen und Maßnahmen sind in dem Konzept festzuhalten:

- Wann werden welche Komponenten und Daten gesichert?
- Wer besitzt die Berechtigung dazu?
- Wer besitzt die Berechtigung, Daten wiederherzustellen?
- Wer besitzt Zugriff auf die archivierten Backup-Daten?
- Wo werden die Backup-Daten sicher gelagert? Hier ist besonders darauf zu achten, dass Backup-Daten räumlich getrennt von Produktivdaten aufbewahrt werden.

Weiterhin müssen die Verfahren definiert werden, mit denen ein SAP-ERP-System wiederhergestellt werden soll. Da die Verfügbarkeit von SAP-ERP-Systemen und der damit verbundenen Prozesse, Anwendungen und Dienste die Voraussetzung für einen sicheren Betrieb sind, sollten Ausweichsysteme vorgehalten oder hochverfügbare Architekturen für Server benutzt werden (Cold-Stand-by, Hot-Stand-by, Cluster oder Cloud). Vor allem kleinere Unternehmen und Behörden betreiben oftmals eine Single-Server-Installation. In dem Fall wird empfohlen, auf einem Ausweichsystem (z. B. als Cold-Stand-by-System) die letzte Datensicherung einzuspielen.

Konzept der Notfall-Administration erstellen

Sollte mit den normalen Administrator-Benutzerkennungen nicht mehr auf ein SAP-ERP-System zugegriffen werden können, wird ein Notfall-Administrator-Konto benötigt. Der ABAP- und Java-Stack verfügt jeweils über eine Benutzerverwaltung und es muss in jedem Stack ein solches Konto definiert werden. Weitere Informationen zum Notfallbenutzer siehe APP.4.2.M5 *Konfiguration und Absicherung der SAP-Benutzerverwaltung*.

APP.4.2.M29 Einrichten eines Notfallbenutzers (S)

Aufgrund der weitreichenden Berechtigungen ist es notwendig, dass Notfallbenutzer stark kontrolliert werden:

- Notfallbenutzer-IDs unterscheiden sich von normalen Benutzer-IDs.

- Für Notfallbenutzer, die nicht im Einsatz sind, werden Gültigkeitseinschränkungen im System deaktiviert.
- Beim Einsatz der Notfallbenutzer ist der Security Audit Log zu aktivieren.
- Die Nutzung der Notfallbenutzer ist protokollarisch festzuhalten.
- Nach Beendigung des Notfalleinsatzes ist die ID wieder zu sperren und das Kennwort neu zu initialisieren.

Mit dem Produkt SAP Access Control (SAP AC) und der Komponente Emergency Access Management (EAM) lassen sich sogenannte FireFighter als Notfalladministratoren erstellen. Werden die FireFighter eingesetzt, wird das automatisch protokolliert. Das Prinzip des Firefighters besteht darin, dass ein Benutzer (z. B. ein Benutzeradministrator) sich mit der FireFighter-ID an dem jeweiligen SAP-ERP-System anmelden kann. Der Vorteil ist, dass die Notfallmaßnahmen außerhalb seiner eigentlichen Tätigkeit in einer kontrollierten und für den Audit transparenten Umgebung durchgeführt werden.

APP.4.2.M30 Implementierung eines kontinuierlichen Monitorings der Sicherheitseinstellungen (S)

Mit dem Solution Manager ab Version 7.1 ist es möglich, systematische und automatisierte Überwachungsprozesse einzurichten.

Konfigurationsvalidierung

Die Konfigurationsvalidierung dient dazu, die Sicherheitskonfiguration der SAP-ERP-Systeme und den Implementierungsstatus von SAP-Sicherheitshinweisen und Patches zu überwachen. Eine Option der Konfigurationsvalidierung ist es, die Ist-Werte der Konfigurationselemente mit definierten Sicherheitsstandards zu vergleichen. Des Weiteren können Benutzer auf kritische Berechtigungen analysiert werden. Die Konfigurationsvalidierung basiert auf der Änderungsauswertung und der Änderungsdatenbank (CCDB). Die CCDB speichert die Konfigurationsdaten der Systeme, die mit dem SAP Solution Manager verbunden sind.

Funktionen/Sichten der Konfigurationsvalidierung:

- Vorlagen für Auswertungen/Reports
- Es gibt verschiedene Auswertungsvorlagen, basierend auf Ad-hoc-Reports.
- Die Auswertungen sind nach Kategorien unterteilt: Operatorvalidierung, Konsistenzvalidierung, Konfigurations-Reporting und gewichtete Validierung
- Transport-Reporte
- Bietet schnellen Zugriff auf eine Reihe vordefinierter Reports, damit Transporte geprüft und validiert werden können.
- Lesezeichen
- Für den späteren Zugriff lässt sich die URL einer Reportvariante sichern.
- Zielsysteme
- Enthalten benutzerdefinierte Zielkonfigurationsdaten und sind virtuelle Systeme.
- Vergleichslisten
- Es können Vergleichslisten definiert werden, um ähnliche Systeme, die regelmäßig validiert werden sollen, zu Gruppen zusammenzufassen. Systeme müssen nicht jedes Mal beim Ausführen erneut ausgewählt werden.
- Trendanalyse

- Reports können regelmäßig in Tages- oder Wochenintervallen eingeplant werden, um Analysen über einen bestimmten Zeitraum zu erhalten. Daraus können dann Trendanalysen erstellt werden.

Weitere Informationen über die Konfigurationsvalidierung sind im SAP-Hinweis 1483508 (siehe [SECNOTE]) beschrieben.

System Recommendations (Systemempfehlungen)

Das Tool System Recommendations liefert passende Empfehlungen zu wichtigen SAP-Hinweisen und Patches für ABAP- und Java-basierte SAP-ERP-Systeme. Abhängig vom aktuellen Systemstatus und bereits implementierten Hinweisen empfiehlt das Tool weitere SAP-Hinweise bezüglich Sicherheit, Performance oder gesetzlichen Änderungen (Java-Patches, HotNews mit hoher Priorität oder allgemeine SAP-Hinweise).

Integration der System Recommendations:

- Im SAP-Support-Portal werden die Hinweise für die ausgewählten Systeme abgefragt und die Informationen werden zum SAP Solution Manager übertragen.
- System Recommendations werden als Änderungsanträge eingebunden.
- Die SAP-Hinweise werden dann heruntergeladen und könnten mit dem Note Assistant implementiert werden.

Funktionen der System Recommendations:

- Anzeigen und Herunterladen von Hinweisen, um sie anschließend zu implementieren.
- Darstellen der Ergebnisse nach Anwendungskomponente, Softwarekomponente oder als Liste. In der Listendarstellung können die Ergebnisse gefiltert und sortiert werden.
- Zuweisen eines Status zu einem Eintrag und Anzeigen von Hinweisinformationen eines bestimmten Status.
- Analysieren, wie sich die Implementierung eines Hinweises auf das System und die Geschäftsprozesse auswirkt.
- Anlegen eines Änderungsantrags oder Auswahl eines Java-Patches und Anlegen eines Wartungsvorgangs.
- Definieren eines Hintergrunddienstes zur automatischen Aktualisierung der Hinweisinformationen.

APP.4.2.M31 Konfiguration von SAP Single-Sign-On (S)

SAP Single-Sign-On (SSO) ermöglicht es, die Risiken von ungesicherten Login-Informationen zu senken und Help-Desk-Anrufe zu reduzieren. Folgende sicherheitsrelevante Aspekte sind zu bedenken, wenn SAP Single-Sign-On eingesetzt wird:

- Single-Sign-On sollte nur zwischen vertrauenswürdigen Systemen konfiguriert werden. Insbesondere SSO-Szenarien über Unternehmens- oder Behördengrenzen hinweg sind unter Sicherheitsgesichtspunkten zu vermeiden.
- Es empfiehlt sich, pro Szenario nur ein System für die zentrale Anmeldung einzusetzen, das SSO-Tickets ausstellt. Alle anderen Systeme sollten SSO-Tickets nur akzeptieren.
- Besonders wichtig ist, dass die Kommunikation zwischen dem Browser des Benutzers und dem SAP-ERP-System verschlüsselt wird. Ansonsten besteht die Gefahr, dass Angreifer das SSO-Ticket abhören und damit ohne Anmeldung auf das SAP-ERP-System zugreifen können.

Folgende Profilparameter regeln die SSO-Konfiguration für ein SAP-ERP-System:

- login/accept_sso2_ticket: System akzeptiert SSO-Tickets.
- login/create_sso2_ticket: System stellt SSO-Tickets aus.

- login/ticket_expiration_time: Gültigkeitsdauer der ausgestellten SSO-Tickets in Stunden.
- login/ticket_only_by_https: SSO-Tickets werden nur beim Zugriff über HTTPS ausgestellt.
- login/ticket_only_to_host: SSO Tickets werden nur bei Zugriffen auf das ausstellende System verwendet.

Für die Konfiguration von SAP SSO sind zusätzliche administrative Tätigkeiten durchzuführen, die über die Transaktionen SSO2, SSO2_ADMIN (SSO2_ACL) und STRUSTSSO2 gemanagt werden können. SAP empfiehlt, die Transaktion SSO2 zu nutzen.

Neben dem SAP-SSO-Mechanismus über Tickets können auch externe Systeme für SSO genutzt werden. Diese müssen dann jedoch über die SNC-Schnittstelle eingebunden sein.

Für Windows-Umgebungen wird darauf hingewiesen, Single-Sign-On über Kerberos zu nutzen. In diesem Fall erfolgt die Anmeldung nur am Windows-System. Beim Zugriff auf das SAP-ERP-System ist es dann nicht mehr notwendig, Benutzername und Passwort einzugeben. Der verwendete Windows-Kerberos-SNC-Provider ist standardmäßig und ohne Mehrkosten verfügbar. Es muss jedoch bedacht werden, dass der Windows-Kerberos-SNC-Provider die Kommunikation nicht verschlüsselt. Daher ist nur eine SNC-basierte Authentisierung verfügbar. Es ist es jedoch möglich, IPSec zwischen Rechnern einzusetzen und so die Kommunikation zu verschlüsseln. Ob das eine mögliche Variante ist, um Single-Sign-On in einer Institution umzusetzen, muss diese jeweils selbst entscheiden.

APP.4.2.M32 Echtzeiterfassung und Alarmierung von irregulären Vorgängen (H)

Mithilfe von Security-Information-and-Event-Management-(SIEM)-Systemen können Betrugs- und Sicherheitsvorfälle identifiziert werden. Die Systeme sammeln die Logdaten aus verschiedenen Quellen (Netzkomponenten, Servern und Datenbanken) und bringen sie mit vordefinierten Regelwerken in Beziehung. Ein Alarm wird ausgelöst, sobald ein Angriffsmuster erkannt wurde.

Für SAP-ERP-Systeme sind Standard SIEM-Produkte nur bedingt geeignet. Die Enterprise Threat Detection (ETD) ist eine Lösung von SAP, die SAP-Protokolle und Logdateien interpretieren und analysieren kann. Es gibt noch viele weitere Lösungen auf dem Markt, die für SAP-ERP-Systeme eingesetzt werden können. Diese Produkte müssen Angriffe aufzeigen, sobald Veränderungen am ABAP-Quellcode durchgeführt, unbefugte Sicherheitseinstellungen erkannt oder Berechtigungen manipuliert wurden.

2.2. Maßnahmen zum Baustein OPS.1.1.3 Patch- und Änderungsmanagement

APP.4.2.OPS.1.1.3.M15 Regelmäßige Aktualisierung von IT-Systemen und Software (B)

SAP hat den Prozess "Product Security Response Prozess" zur Verbesserung der Produktsicherheit definiert: Sobald eine Schwachstelle identifiziert wurde, gibt das Unternehmen einen SAP-Sicherheitshinweis heraus. Die Hinweise werden typischerweise an jedem zweiten Dienstag eines Monats veröffentlicht (SAP Security Patch Day) und in dringenden Fällen auch außerhalb des Patch-Day-Zyklus.

Die Sicherheitshinweise haben verschiedene Prioritätsstufen:

- HotNews (1)
- Korrekturen mit einer hohen Priorität (2)
- Korrekturen mit einer mittleren Priorität (3)
- Korrekturen mit einer niedrigen Priorität (4)
- Empfehlungen / zusätzliche Informationen (5)

Die erste und zweite Stufe müssen zeitnah eingespielt werden, während die dritte bis fünfte Stufe auch mit dem nächsten Support-Package eingespielt werden können. Die fünfte Stufe der SAP-Hinweise beinhaltet lediglich Informationen und keine Software-Patches. Der zentrale Zugangspunkt mit den neuen Informationen zu SAP-Hinweisen ist der SAP Service Marketplace (siehe [SECNOTE]).

SAP HotNews

In dem SAP HotNews ist beschrieben, wie Probleme behoben oder verhindert werden (z. B. wie das SAP-ERP-System heruntergefahren wird oder keine Daten verlorengehen). Es sollte ein Verfahren eingerichtet werden, mit dem regelmäßig die SAP HotNews geprüft werden. Dafür sollte ein Verantwortlicher benannt werden, der die Änderungsanforderung (Change Request) erstellen darf. Diese Änderungsanforderungen werden den verantwortlichen Personen des Prozesses weitergeleitet.

SAP Security Patch Day

Der SAP Security Patch Day findet jeden zweiten Dienstag im Monat statt. Eine aktuelle Liste der Sicherheitshinweise befindet sich unter [SECNOTE]. Darüber hinaus können in der Media Library (siehe [SAPSOS]) weiterführende Informationen zu verschiedenen Applikationen und Hinweisen nachgelesen werden, die im Folgenden kurz erläutert werden und in einem eigenen Abschnitt noch detaillierter beschrieben werden.

Mit der Applikation-Systemempfehlung (System Recommendations) wird geprüft, welche Sicherheitshinweise für die verschiedenen Systeme der SAP-Landschaft relevant sind. Dafür kann ein regelmäßiger Hintergrundjob eingeplant werden, der die Sicherheitshinweise für das System auswertet. Eine Änderungsanforderung (change request) kann direkt aus der Applikation gestartet werden.

Die Risikobewertung (Risk Assessment) gibt an, wie kritisch die Sicherheitslücke ist, aber auch wie hoch das Risiko für die produktiven Geschäftsprozesse durch das Einspielen ist. Entsprechend dieser Bewertung wird entschieden, welche Sicherheitshinweise im Rahmen eines monatlichen Patch-Zyklus angewandt werden und welche ein Teil des nächsten Wartungszyklus sind.

Die Applikation-Validierung der Konfiguration ("Configuration Validation") bietet die Möglichkeit, einen Report auszuführen, der prüft, welches System den Sicherheitsrichtlinien entspricht. Demzufolge werden alle zu installierenden Sicherheitshinweise für das Zielsystem der Validierung der Konfiguration (Configuration Validation) hinzugefügt.

Innerhalb des aktuellen Monats erfolgt die Anwendung der ausgewählten Sicherheitshinweise (Security Notes). Falls notwendig, wird ein Regressionstest durchgeführt, um sicherzustellen, dass die produktiven Geschäftsprozesse ordnungsgemäß funktionieren.

Im Rahmen des Wartungszyklus wird der Kernel aktualisiert. Das gilt für Java Patches und ABAP-Support-Packages. Dazu zählt ebenfalls, dass die Korrekturen der Sicherheitshinweise mitgeliefert werden. Ein Teil der Sicherheitshinweise beschreibt Konfigurationsänderungen, die sofort angewendet werden können. Während der Aktualisierung kann es sein, dass neue Sicherheitshinweise von neueren Patch-Days eintreffen. Diese sollten mit einbezogen werden. Am Ende der Aktualisierung ist ein vollständiger Test für alle Geschäftsprozesse durchzuführen.

SAP-Sicherheitshinweise mit der Transaktion SNOTE implementieren

Die Transaktion SNOTE wird dazu verwendet, die mit den SAP-Sicherheitshinweisen gelieferten Korrekturen einzuspielen. Es ist notwendig, alle dazugehörigen SAP-Hinweise und Beschreibungen sorgfältig zu lesen und diese nicht zu ignorieren.

SAP-Sicherheitshinweise transportieren

Das Einspielen eines SAP-Sicherheitshinweises sollte mit den dazugehörigen SAP-Sicherheitshinweisen in einem Transportauftrag angelegt werden. SAP-Sicherheitshinweise, die unabhängig voneinander sind, dürfen nicht in einen gemeinsamen Transportauftrag aufgenommen werden.

Java-Systeme

Neben Korrekturen, die über Java-Support-Packages ausgeliefert werden, sollte unbedingt beachtet werden, dass die verwendete JVM selbst ebenfalls Schwachstellen aufweisen kann und aktuell gehalten werden muss. Das gilt sowohl für die JVM von Oracle als auch die von SAP. Die regelmäßigen Updates zu den JVM enthalten oft wichtige Sicherheitskorrekturen, die mitunter nicht detailliert beschrieben sind. Daher sollten JVM-Updates auch ohne konkreten Sicherheitshinweis regelmäßig angewendet werden.

Grundsätzlich gilt, dass die SAP-Sicherheitshinweise der Priorität 1 (HotNews) und 2 (High) teilweise schwerwiegende Fehler in der Programmierung der SAP-Standardsoftware beheben und deswegen zeitnah bewertet und angewendet werden müssen. Hinweise mit geringerer Priorität können auch über Support-Packages implementiert werden. Da die ausgelieferten Korrekturen oft Abhängigkeiten zum Softwarestand haben und deswegen eine verspätete Umsetzung komplexer wird, sollte mindestens einmal im Jahr ein Support-Package eingespielt werden. SAP garantiert den Downport von Einzelkorrekturen nur für Releases und Support-Package-Stände der zurückliegenden 18 Monate.

2.3. Maßnahmen zum Baustein OPS.1.1.5 Protokollierung

APP.4.2.OPS.1.1.5.M3 Konfiguration der Protokollierung auf System- und Netzebenen (B)

Mit der Transaktion SM19 (Security-Audit: Audit-Profil verwalten) werden die Filter des Security Audit Logs (SAL) konfiguriert. Für jeden Filter lässt sich definieren, ob Mandanten und Benutzer aufgezeichnet werden (abhängig von der Kategorisierung und Auditklasse). Die Ergebnisse können nach den drei Kategorien unkritisch, schwerwiegend und kritisch eingestuft werden. Diese müssen den Auditklassen Dialoganmeldung, RFC-/CPIC-Anmeldung, RFC-Funktionsaufruf, Transaktionsstart, Reportstart, Benutzerstammänderung, System und sonstige Ereignisse zugeordnet werden.

Das Security Audit Log kann als statische oder dynamische Konfiguration eingestellt werden. Bei der statischen Konfiguration werden die Filtereinstellungen persistent in der Datenbank gespeichert und bei jedem Systemstart verwendet. Bei der dynamischen Konfiguration können dagegen die Filtereinstellungen im laufenden Betrieb geändert werden. Allerdings ist die Anzahl der vorhandenen Filter nicht änderbar. Die Einstellungen sind bei dieser Konfiguration nur bis zum nächsten Systemstart aktiv.

Damit die Ereignisse im System protokolliert werden, muss zusätzlich der Profilparameter für das Security Audit Log aktiviert werden (Transaktion RZ11). Das Security Audit Log wird durch die folgenden drei Einstellungen aktiviert:

- **rsau/enable = 1** Dieser Parameter bestimmt, ob das Log eingeschaltet ist oder nicht (1 = eingeschaltet, 0 = ausgeschaltet (Standardwert)).
- **rsau/selection_slots = 10** Dieser Parameter zeigt die Anzahl der Filter, die in der Transaktion SM19 konfiguriert und dann geprüft werden.
- **rsau/user_selection = 1** Dieser Parameter bestimmt, ob eine generische Selektion von Benutzern möglich ist (0 = generische Selektion ist nicht möglich, 1 = generische Selektion ist möglich (z. B. SAP_*))

Die folgende Tabelle zeigt weitere Profilparameter, die zu setzen sind:

Profilparameter	Standardwert	Empfohlener Wert	Beschreibung
DIR_AUDIT			Verzeichnis, in dem die SAL-Dateien angelegt werden
FN_AUDIT			definiert den Namen der SAL-Dateien

Profilparameter	Standardwert	Empfohlener Wert	Beschreibung
rsau/ip_only	0 = Terminal-Name wird protokolliert	1 = IP-Adresse wird protokolliert	Protokollierung des Terminal-Namens oder der IP-Adresse
rsau/max_diskspace/local		2 GB	maximale Größe der SAL-Dateien, Wertebereich von 100 MB bis 2 GB
rsau/max_diskspace/per_file		2 GB	maximale Größe der SAL-Dateien. Ist die maximale Größe der Datei erreicht, wird eine neue erstellt. Wertebereich von 1 GB bis 2 GB
rsaus/max_diskspace/per_day		1.024 GB	Bestimmt maximalen Speicherplatz für alle SAL-Dateien. Wertebereich von 3* bis 1.024 GB

Mindestens eine der folgenden Protokollierungen sollte definiert und aktiviert werden:

- Die Protokollierung aller Ereignisse für kritische Benutzer wie SAP* (Verwendung des Filters SAP#*), Notfallbenutzer (wie FF*) oder Supportbenutzer (wie SAPSUPPORT*).
- Die Protokollierung aller kritischen Ereignisse für Benutzer.

Hinweis: Das Security Audit Log wurde in den letzten Jahren erweitert. Im Folgenden wird ein Auszug der neuen Funktionen mittels SAP-Hinweisen vorgestellt (siehe [SECNOTE]):

- 1411741 - Auswertung von Debuggingereignissen im Audit Log
- 1465495 - ABAP Debugger: Sicherheitsprüf.prot. für Debugger-Aktivität. 1465495 - ABAP Debugger: Sicherheitsprüf.prot. für Debugger-Aktivität
- 1539105 - Protokollierung generischer Tabellenzugriffe per RFC
- 1810913 - Performanceverbesserung beim Auslesen des Security Audit Log
- 1963882 - SAL|Probleme bei der Auswertung von AuditLog-Dateien
- 1941568 - SAL|FAQ für Nutzung kundenindividueller Ereignisse
- 1819317 - Erweiterung des Security Audit Log
- 539404 - FAQ: Antworten auf Fragen zum Security Auditlog

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

[SAPHSCR] SAP HANA Security Checklists and Recommendations: SAP SE, https://help.sap.com/hana/SAP_HANA_Security_Checklists_and_Recommendations_en.pdf

[SAPLOPA] Standardregeln der Profilparameter für Passwort- und Anmelderegeln: SAP SE, https://help.sap.com/saphelp_nw70ehp2/helpdata/de/4a/c3f18f8c352470e10000000a42189c/content.htm

[SAPSECPO] Übersicht der Sicherheitsrichtlinienattribute für die Steuerung der Kennwortregeln: Kennwortänderung und Anmelderestriktionen, SAP SE, https://help.sap.com/saphelp_nw74/helpdata/de/e9/c15fb4c06340558898fda99d98cb0d/content.htm?no_cache=true

[SAPSG] Security Guides zu SAP-Lösungen: SAP SE, https://service.sap.com/

[SAPSOS] SAP Security Optimization Services Portfolio: SAP SE, https://support.sap.com/sos

[SAPSUPP] SAP Support Portal: SAP SE, https://support.sap.com/

[SAPSWP] SAP Security White Paper: SAP SE, https://support.sap.com/securitywp

[SECNOTE] Sicherheitshinweis: SAP SE, https://support.sap.com/securitynotes