Martin Koch, Siegfried Zeilinger

Checklisten zum Buch

SAP® Business Technology Platform – Sicherheit und Berechtigungen

ISBN 978-3-8362-8098-3

Rheinwerk Publishing

Checklisten

Hier finden Sie die Checklisten aus dem Buch zum Ausdrucken und Abgleichen.

Checkliste zur allgemeinen Sicherheit der SAP Business Technology Platform

In Tabelle 1 finden Sie eine Checkliste für die Sicherheitsthemen im Kontext der SAP BTP. Prüfen Sie, ob Sie alle hier aufgeführten Kriterien berücksichtigt haben.

Erledigt	Aufgabe
	Es besteht Klarheit über die verwendeten Domänen.
	Die Zertifizierungsstelle wurde festgelegt.
	Es wurde überprüft, ob die Zertifizierungsstelle als Root-Zertifikat im Standard-Truststore der SAP BTP vorhanden ist. Alternativ wurde ein kundeneigener Truststore erstellt.
	Es wurden Festlegungen zu den Destinations getroffen, d. h. dazu, auf welchen Ebenen welche Verbindungen eingerichtet werden.
	Die Verantwortlichen für die jeweiligen Verbindungen wurden nominiert.
	Ein Ort zur Dokumentation der Destinations wurde vereinbart.
	Der Ablauf der Zertifikate wurde in einem geeigneten Format bzw. Kalender vermerkt (bei kundeneigenen Zertifikaten).
	Es wurden Sicherheitsrichtlinien zu Passwörtern und zur Zwei-Faktor-Authentifizierung definiert.
	Es wurde entschieden, für welche Anwendungen und Subaccounts welcher Identity Provider genutzt wird.
	Die Nutzung eines Identity Authentication Tenants wurde diskutiert und abgewogen.
	Die Berechtigungserteilung für Cloud-Anwendungen wurde in die Organisation des Unternehmens integriert, und Verantwortlichkeiten wurden festgelegt.
	Er wurde geklärt, wie das Monitoring und die periodischen Attestierungen im Umfeld der SAP BTP erfolgen werden.

Tabelle 1 Checkliste für die Sicherheit auf der SAP BTP

Erledigt	Aufgabe
	E-Mails und Branding wurden so angepasst, dass die Benutzer in der Lage sind, die Cloud-Anwendungen als dem Unternehmen zugehörig zu identifizieren. Insbesondere die Absenderadresse der E-Mails wurde entweder auf einen eigenen E-Mail-Server angepasst, oder die SAP-Absenderadresse wurde im E-Mail-Server als sicher bekannt gemacht.
	Bei Verwendung von Webblockern im Browser wurde sichergestellt, dass die Anwendungen in der Cloud zugreifbar sind und dass allfällige Sicherheitshinweise zu externen Seiten nicht angezeigt werden.
	Es wurde festgelegt, von wo aus Zugriffe auf welche Art erfolgen dürfen. Daraus abgeleitet wurden Authentifizierungsregeln angepasst bzw. erstellt.
	Es wurde geklärt, wie die Bereitstellung von Benutzern erfolgt, insbesondere ob der Service Identity Provisioning genutzt werden soll.

Tabelle 1 Checkliste für die Sicherheit auf der SAP BTP (Forts.)

Checkliste zu Sicherheit und Berechtigungen in der Neo-Umgebung

In Tabelle 2 finden Sie die Checkliste für die Berechtigungs- und Berechtigungsverwaltung in der Neo-Umgebung.

Erledigt	Aufgabe
	Sie haben die unterschiedlichen Rechenzentren der Cloud-Foundry- und der Neo-Umgebung im Blick und haben sich am besten die genutzten Server an zentraler Stelle notiert.
	Es wurde festgelegt, welche Authentifizierungsmethode genutzt werden soll. Für Anwendungen, die in Subaccounts der Neo-Umgebung laufen, kann eine spezifische Authentifizierung eingerichtet werden. Das ist vor allem dann sinnvoll, wenn diese Anwendungen für einen eigenen Personenkreis freigegeben werden, der z. B. auch extern verwaltete Identitäten umfasst.
	Sie haben Ihre Subaccounts von anderen Subaccounts abgegrenzt. Das hat speziell bei der Anbindung von On-Premise-Systemen über den Cloud Connector (siehe Kapitel 5) große Bedeutung, weil Sie in diesem Fall die Berechtigungen für die angebundenen Entwicklungssysteme nur auf dem Entwicklungs-Subaccount einrichten können.
	Sie haben festgelegt, wo der Einsatz von Identity Providern dokumentiert wird und wie viele Identity Provider Sie einsetzen wollen.

Tabelle 2 Checkliste zu Sicherheit und Berechtigungen in der Neo-Umgebung

Erledigt	Aufgabe
	Es wurde sichergestellt, dass nur ein eingeschränkter Benutzerkreis Änderungen an der produktiven Konfiguration der Identity Provider vornehmen kann.
	Das Cloud-Sicherheitskonzept ist mit dem lokalen Sicherheitskonzept abgestimmt und stimmig. Beachten Sie insbesondere, welche (alle?) Benutzer Ihres Unternehmens sich an den Cloud-Anwendungen anmelden könnten.
	Sie haben sichergestellt, dass sich die Plattformrollen anwendungsfallweise mit den Benutzerrollen in anderen Systemen decken. Die Benutzerrollen sollten aufeinander abgestimmt sein.

Tabelle 2 Checkliste zu Sicherheit und Berechtigungen in der Neo-Umgebung (Forts.)

Checkliste zu Sicherheit und Berechtigungen in der Cloud-Foundry-Umgebung

In Tabelle 3 finden Sie die Checkliste für die Berechtigungs- und Benutzerverwaltung in der Cloud-Foundry-Umgebung.

Erledigt	Aufgabe
	Sie haben die unterschiedlichen Rechenzentren der Cloud-Foundry- und der Neo-Umgebung im Blick und haben sich am besten die genutzten Server an zentraler Stelle notiert.
	Sie haben geprüft, ob Sie das aktuelle Feature Set der SAP BTP abonnieren. Neue Projekte sollten Sie mit dem aktuellsten Versionsstand der SAP BTP beginnen.
	Den Namen für Ihre Organisation haben Sie so gewählt, das er sich nicht so schnell ändert, da die Namen von Organisationen nur durch Neuanlage des Subaccounts geändert werden können.
	Sie haben Ihre Subaccounts von anderen Subaccounts abgegrenzt. Das hat speziell bei der Anbindung von On-Premise-Systemen über den Cloud Connector (siehe Kapitel 5) hohe Bedeutung. Bei übergreifenden Szenarien haben Sie den Einsatz des Service Identity Provisionings in Betracht gezogen.
	Sie haben festgelegt, wo der Einsatz von Identity Providern dokumentiert wird und wie viele Identity Provider Sie einsetzen wollen.
	Es wurde sichergestellt, dass nur ein eingeschränkter Benutzerkreis Änderungen an der produktiven Konfiguration der Identity Provider vornehmen kann.

Tabelle 3 Checkliste zu Sicherheit und Berechtigungen in der Cloud-Foundry-Umgebung

Erledigt	Aufgabe
	Das Cloud-Sicherheitskonzept ist mit dem lokalen Sicherheitskonzept abgestimmt und stimmig. Beachten Sie insbesondere, welche (alle?) Benutzer Ihres Unternehmens sich an den Cloud-Anwendungen anmelden könnten.
	Die Sammelrollen der SAP BTP passen zu den Benutzerrollen in anderen Systemen Ihrer Landschaft. Die Zuordnung sollte sich anwendungsfallabhängig mit der von On-Premise-Rollen decken. Sammelrollen aus den verschiedenen Systemen sollten auf einer Ebene sein da die Vergleiche Einzelrollen bzw. SAP-BTP-Rollen enthalten.
	Bei der Entscheidung, ob Sie einen Identity Authentication Tenant verwenden, haben Sie folgende Kriterien berücksichtigt: ■ **Die Lizenzfrage** Wenn Sie im Zuge einer Bundle-Lizenz für eine SAP-Cloud-Anwendung ohnehin Zugriff auf den Identity Authentication Service haben, bietet es sich an, diesen auch zu verwenden. ■ **Die Frage der Übersichtlichkeit** Wenn Sie mehr und mehr Subaccounts verwenden, wird die Verwaltung der externen Identity Provider über den Identity Authentication Service als Plattform-Identity-Provider einfacher. Die Vertrauensbeziehung kann dann von den jeweiligen Subaccounts zum Identity Authentication Service und von dort weiter zum externen Identity-Provider eingerichtet werden.
	Wenn Sie einen externen Identity Provider verwenden, haben Sie ein Sammelrollen-Mapping eingerichtet. Sie haben die geeigneten Attribute für ein solches Mapping ausgemacht. Beachten Sie, dass ein Reporting für die gemappten Zuweisungen aktuell nur auf der Seite des externen Providers möglich ist.

Tabelle 3 Checkliste zu Sicherheit und Berechtigungen in der Cloud-Foundry-Umgebung (Forts.)

Checkliste für die Konfiguration des Cloud Connectors

In Tabelle 4 finden Sie die Checkliste zur sicheren Konfiguration von Verbindungen über den Cloud Connector.

Erledigt	Aufgabe
	Sie haben bei der Entwicklung einer Anwendung in der Cloud festgelegt, ob der Cloud Connector zu verwenden ist. Sinnvollerweise wurde dies auch in den Entwicklungsrichtlinien berücksichtigt.

Tabelle 4 Checkliste für die Konfiguration des Cloud Connectors

Erledigt	Aufgabe
	Sie haben festgelegt, wie viele Cloud-Connector-Instanzen installiert werden sollen. Verteilen Sie diese geografisch, um die Ausfallsicherheit zu erhöhen. Beachten Sie auch, ob Entwickler*innen einen eigenen Cloud Connector auf ihren lokalen Rechnern installiert haben.
	Sie haben ein Konzept zur Wartung Ihrer Cloud-Connector-Instanzen ausgearbeitet. Sie sollten festlegen, welche Cloud-Connector-Instanz bei einem Funktions-Upgrade zuerst aktualisiert wird, und sicherstellen, dass die Verbindungen korrekt getestet werden.
	Es wurde definiert, wer Zugriff auf den Cloud Connector erhalten soll. Möglich wären Administrator*innen, Entwickler*innen, aber auch andere Personenkreise, die z. B. Anzeigerechte bekommen könnten.
	Abhängig von der Frage, wer Zugriff bekommt, sollten Sie geklärt haben, ob Sie eine Anbindung an ein LDAP-Verzeichnis benötigen, um die Benutzer zu authentifizieren. Eine solche Anbindung ergibt in vielen Fällen Sinn, speziell wenn mehrere Benutzer Zugang erhalten sollen.
	Ein Monitoring-Konzept für den Cloud Connector wurde erarbeitet. Sie können sich dabei an den Konzepten für das Monitoring anderer Systemverbindungen in Ihrem Unternehmen orientieren und sollten auch festhalten, wer für das Monitoring zuständig ist.
	Sie haben einen Ort zur Dokumentation der Cloud-Connector-Verbindungen definiert. Prüfen Sie in diesem Zusammenhang anhand Ihrer Entwicklungsrichtlinien, ob eine Dokumentation im Cloud Connector ausreicht oder welche anderen Dokumentationen berührt werden. Wichtig wäre auch eine Erfassung der Subaccounts und der angeschlossenen Cloud-Connector-Instanzen.
	Falls für die Daten, die über den Cloud Connector übertragen werden, hohen Schutzanforderungen gelten, empfiehlt sich die Aktivierung des Vieraugenprinzips bei der Überwachung von Netzwerk-Traces.
	Sie haben eine Vereinbarung getroffen, wie hoch die Verfügbarkeit der Verbindung sein sollte. SAP empfiehlt generell eine redundante, hochverfügbare Anbindung. Berücksichtigen Sie dabei auch Ihren eigenen Internet-Uplink, und erarbeiten Sie ein Fallback-Szenario. Dazu sind in der Regel umfassende Klärungen mit den Netzwerkteams nötig.
	Sie haben ein Namenskonzept für virtuelle Host-Namen und Destinationen erarbeitet. Die Namensvergabe kann fachlich (z. B. mit dem Namensbestandteil FI bezogen auf das Finanzwesen) oder applikationsspezifisch (z. B. mit dem Namensbestandteil MRA für eine mobile Reisekostenapplikation) erfolgen, sollte aber durchgängig einheitlich sein.

Tabelle 4 Checkliste für die Konfiguration des Cloud Connectors (Forts.)

Erledigt	Aufgabe
	Sie haben Abläufe zur Freischaltung von Services definiert und hinterlegt, welche Personen dabei in welcher Form informiert werden müssen.

Tabelle 4 Checkliste für die Konfiguration des Cloud Connectors (Forts.)

Checkliste zur Arbeit mit der Kommandozeile und APIs

In Tabelle 5 finden Sie die Checkliste für die Arbeit mit den in Kapitel 6, »Administrationswerkzeuge der SAP Business Technology Platform«, vorgestellten Administrationswerkzeugen.

Erledigt	Aufgabe
	Es wurde festgelegt, wer welche administrativen Berechtigungen für die SAP BTP erhält. Abgeleitet davon sollten nur diese Benutzer gleichartige Berechtigungen für die Kommandozeile bekommen.
	Es wurde definiert, wo API-Zugriffe und API-Schlüssel angefordert und verwaltet werden.
	Es wurde festgelegt, wo die Zugriffe auf oder über APIs der SAP-BTP-Anwendungen dokumentiert werden.
	Es wurde vereinbart, wer die Kommandozeilenwerkzeuge auf den jeweiligen Unternehmensrechnern installieren darf.
	Sie haben speziell bei den APIs der Cloud-Foundry-Umgebung im Blick, dass sich diese häufiger ändern (meist werden Funktionen hinzugefügt, selten geändert). Sie haben daher sichergestellt, dass regelmäßig im SAP API Business Hub geprüft wird, ob es neuere und bessere Ansätze gibt.

Tabelle 5 Checkliste zur Arbeit mit der Kommandozeile und APIs

Checkliste zur Absicherung von Cloud-Services

Die Checkliste in Tabelle 6 behandelt generelle Sicherheitsthemen, die für jeden Service der SAP BTP bzw. jede Subskription in gleicher Weise beachtet werden müssen.

Erledigt	Aufgabe
	Sie haben geprüft, ob ein Service als Subskription oder als Instanz angeboten wird. Für eine Subskription haben Sie geprüft, ob diese in einem Subaccount läuft oder z. B. als mandantenfähige Subskription.

Tabelle 6 Checkliste zur Absicherung von Cloud-Services

Erledigt	Aufgabe
	Sie haben sich vergewissert, wie viele Instanzen des Service Sie benötigen (z. B. eine Entwicklungs- und eine Produktivinstanz).
	Sie haben sich entschieden, ob Sie den Service in einem bestehenden oder in einem neuen Subaccount instanziieren möchten.
	Sie haben in der Dokumentation des jeweiligen Service gegebenenfalls abhängige Services identifiziert. Die Abhängigkeiten wurden dokumentiert. Das erleichtert die Risikoeinschätzung bei Änderungen an Einstellungen oder ganzen Applikationen.
	Sie haben geprüft, wie es mit der Lizenzierung des Service aussieht.
	Es wurde geklärt, welchen Identity Provider Sie verwenden werden bzw. wie allfällige technische Servicezugriffe und/oder Freischaltungen erfolgen sollen.
	Die Dokumentation des Service und seiner Einstellungen wurde geplant, d. h., wo und wie genau dokumentiert wird.
	Der Service verfügt über einen Owner innerhalb Ihrer Organisation, der die Nutzung und Konfiguration koordiniert.
	Die bereitgestellten Sammelrollen wurden analysiert und bei Bedarf angepasst.
	Benötigte Anbindungen über den Cloud Connector und den SAP Destination Service wurden angefordert und modelliert.

Tabelle 6 Checkliste zur Absicherung von Cloud-Services (Forts.)