SAP-HANA

Sicherheitsübersicht

Autor: Thomas Werth

Version: 1.0

Inhaltsverzeichnis

Allianz für Cybersicherheit

“Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die im Jahr 2012 in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet wurde.

Ziele und Angebote der Allianz
Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, die Cyber-Sicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Zur gemeinsamen Förderung der Cyber-Sicherheit arbeitet das BSI dabei im Rahmen der Allianz intensiv mit Partnern und Multiplikatoren zusammen.
Zur Erreichung dieser Ziele verfolgt die Allianz die folgenden Maßnahmen:

- Erstellung und Pflege eines aktuellen Lagebilds
- Bereitstellung von Hintergrundinformationen und Lösungshinweisen
- Intensivierung des Erfahrungsaustausches zum Thema Cyber-Sicherheit
- Ausbau von IT-Sicherheitskompetenz in Organisationen mit intensivem IT-Einsatz

Die Allianz für Cyber-Sicherheit baut hierfür eine umfangreiche Wissensbasis auf und initiiert und betreibt Erfahrungs- und Expertenkreise zur Cyber-Sicherheit. Ergänzt werden diese Angebote durch weitere Beiträge der Partner z.B. in Form von Schulungen, zusätzlichen Informationsveranstaltungen oder der kostenlosen Bereitstellung von Sicherheitsprodukten.” (Quelle: ACS-Homepage https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/Einfuehrung/einfuehrung.html)

Als Partner der Allianz für Cyber-Sicherheit veröffentlicht die Werth IT dieses Dokument.

Was ist SAP HANA?

Zunächst wurde HANA 2011 von SAP als Datenbank auf dem Markt eingeführt. Der Name HANA steht für High Performance Analytic Appliance und beschreibt damit direkt den Einsatzzweck von HANA: Die schnelle Ausführung von Daten-Analysen. Auch im Big Data Umfeld. HANA hält sämtliche Daten im Arbeitsspeicher, dies wird In-Memory genannt und ermöglicht so einen sehr schnellen Zugriff auf die Daten.

2013 folgt der nächste Entwicklungsschritt in der noch jungen Geschichte von HANA, die Entwicklung zur Plattform. Damit ist es von nun an möglich Algorithmen direkt in HANA umzusetzen statt wie bisher klassisch ABAP mit Datenbankabfragen zu nutzen. Durch die In-Memory-Technologie hat man hier einen enormen Geschwindigkeitsvorteil, da direkt auf den Daten gearbeitet werden kann.

SAP hat diese Kernfunktionaltität konsequent weiter ausgebaut und zahlreiche Zusatzfunktionen ausgeliefert. So bringt HANA inzwischen Werkzeuge zur Textanalyse und Data Mining frei Haus mit. Echtzeit Analysen von Daten lassen sich damit einfach umsetzen. 2015 folgt mit S/4HANA die erste Komplettlösung von SAP, die auf HANA optimiert ist und auf Basis der HANA Plattform entwickelt wurde.

Einsatzszenarien

Für SAP HANA existieren drei Einsatzszenarien:

1. SAP HANA als primärer Datenbankserver für SAP-Systeme. [11]
Hierbei ersetzt HANA die bisherige Datenbank und beschleunigt durch seine Technologie das gesamte SAP-System.

2. SAP HANA als Data Mart. [12]
Hier wird HANA zusätzlich zur bestehenden Datenbank eingesetzt und dupliziert ausgewählte Datensätze. Damit wird gezielt die Analyse und die Auswertung von beispielsweise BI Tools ohne Programmänderungen beschleunigt.

3. SAP HANA als Applikations- und Entwicklungs-Plattform. [13]
Über einen integrierten Applikationsserver lassen sich direkt auf der HANA Plattform Anwendungen entwickeln, die optimiert auf die Daten zugreifen können. Somit lassen sich hoch performante Analyse- und Auswertungsprogramme entwickeln.

Für die Betrachtung der System-Sicherheit ergeben sich unabhängig des Einsatzszenarios in der Regel dieselben Anforderungen. Bei besonderen Anforderungen an die Sicherheit aufgrund des Einsatzes von HANA werden diese entsprechend im Dokument vermerkt.

Erweiterbarkeit und Zukunftsvision

HANA ist als offene Plattform konzipiert und kann durch Eigenentwicklungen oder Fremdentwicklungen mittels SAP HANA XS erweitert werden.
Ebenso bietet SAP mit der HANA Cloud Plattform die Möglichkeit eigenständige Applikationen auf Basis von HANA zu entwickeln und an bestehende SAP-Systeme anzubinden und im Internet für mobile Geräte freizugeben.

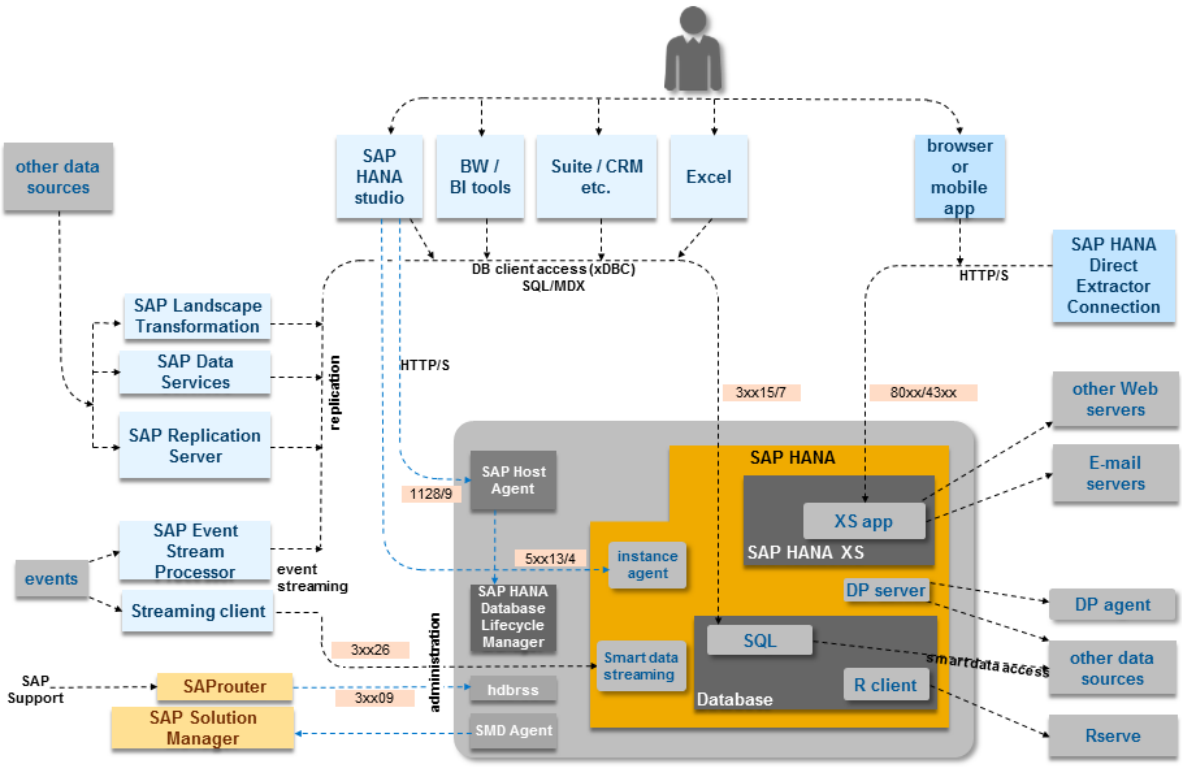
SAP verfolgt das Ziel HANA als Standard-Datenbank für Ihre SAP-Systeme zu etablieren und damit die bisherigen Wettbewerber-Produkte zu verdrängen. Mit S/4HANA ist bereits das erste SAP-System verfügbar, dass direkt auf HANA ausgeliefert wird.

Daten und Sicherheitsanforderungen

Mit diesem klar definierten Ziel wird auch offensichtlich welche Daten in einer HANA Datenbank zu erwarten sind: Unternehmenskritischen Daten.
In diesem System finden sich Kunden-, Lieferanten- und Personaldaten. Ebenso werden hier die Finanzdaten wie Bilanzen, Bankkonten und Buchungen verarbeitet. Zusätzlich trifft man Planungsdaten, Konstruktionsdaten und Vertriebsinformationen - wie z.B. Preislisten - an.
Jeder einzelne Datenbereich ist bereits sensibel und in Kombination hoch kritisch.
Ein angemessener Schutz von HANA ist also unabdingbar.

Netzwerksicherheit

SAP HANA besitzt verschiedene Netzwerkschnittstellen zur Kommunikation, diese gilt es entsprechend dem Einsatzzweck abzusichern.
Welche Schnittstellen ein SAP HANA System besitzt veranschaulicht die folgende Skizze:



(Bild 1: Verbindungen eines SAP HANA Systems, Quelle: SAP® [4])

Die wichtigsten HANA Dienste

Damit HANA seine eigentlichen Aufgaben als Datenbank und Applikationsserver (HANA XS) wahrnehmen kann, startet das System verschiedene Dienste und öffnet dazu einige Ports im Netzwerk. Die wichtigsten werden hier in der Tabelle aufgeführt.

Dienst	Beschreibung	Port (XX = Instanz Num., XY = Instanz Num. + 1)	Firewall Empfehlung
HANA Datenbank	Dienst für Klienten und Applikationsserver, um HANA als Datenbank zu nutzen. Protokoll SQLDBC (ODBC/JDBC)	3xx15	Dieser Port ist für Klienten der Datenbank und Applikationsserver zu öffnen.
HANA Indexserver	Indexserver für die Datenbank. Protokoll SQLDBC (ODBC/JDBC)	3xx17	Der Port ist für Klienten des Data Provisioning und Applikationsserver zu öffnen zu öffnen.
HANA HTTP Server	Zugriff mittels Web Clients auf HANA und HANA XS	80xx, 43xx	Jedem legitimen Nutzer der Web-basierten Dienste von HANA ist die Nutzung zu gestatten.
HANA SAP_SUPPORT	Für den SAP Support wird eine Verbindung auf diesen Port benötigt. Siehe SAP HANA Admin Guide [3] Kapitel 2.11.7	3xx09	Zugriff bei Bedarf erlauben
HANA DISTRIBUTED SYSTEMS	Wird HANA auf verteilten Systemen eingesetzt, werden diese Ports zur internen Kommunikationen zwischen den HANA Instanzen genutzt.	3xx00, 3xx01, 3xx02. 3xx03, 3xx04, 3xx05, 3xx07, 3xx10, 3xx40, 3xx99	Der Zugriff darf nur aus dem privaten Netzwerk der verteilten Systeme untereinander erlaubt sein.
Instanz Agent	Das SAP HANA Studio nutzt diesen Dienst, um administrative Aufgaben zu erledigen. Protokoll SOAP/HTTP(S)	5xx13, 5xx14	Erlaubte Clients sollten nur Hosts von legitimen Nutzern / Entwicklern mit SAP HANA Studio sein.
Host Agent	Der SAP HANA Lifecycle	1128,	Der Zugriff sollte nur für

	Manager nutzt den SAPHost Agent. Protokoll SOAP/HTTP(S)	1129	den Host des Lifecycle Managers freigegeben werden.
HANA SYSTEM REPLICATION	Wird HANA auf verteilten Systemen eingesetzt, werden diese Ports zur internen Kommunikationen zwischen den HANA Instanzen genutzt.	3xy01, 3xy02, 3xy03, 3xy04, 3xy05, 3xy07, 3xy40, 3xy99	Der Zugriff darf nur aus dem privaten Netzwerk der verteilten Systeme untereinander erlaubt sein.

Ausgehende Kommunikation sollte nur erlaubt werden für

- den Diagnostic Agenten zu dem Solution Manager
- zu dem SAP Service Marketplace für den SAP HANA Lifecycle Manager
- Sowie für die SAP HANA XS Engine für deren verwendete Server
- Verbindungen zu R Servern sollte nur erlaubt werden, wenn diese unbedingt erforderlich sind.

Die Interne Kommunikation zwischen HANA Instanzen sollte immer mit einer separaten Netzwerkkarte in einem privaten „Instanz“ Netzwerk erfolgen.

Der System Benutzer

Der System Benutzer wird während der Installation angelegt und für administrative Zwecke wie dem Anlegen von Benutzern verwendet. Die ihm zugeordneten System Privilegien können ihm nicht entzogen werden. Er besitzt damit nahezu uneingeschränkten Zugriff auf die Datenbank. Daher empfiehlt SAP auch nach Abschluss der Installations- und Einrichtungsphase diesen Benutzer zu deaktivieren. Der Vorgang ist in dem SAP Administration Guide [3] in Abschnitt 6.5 Deactivate the SYSTEM User beschrieben. Diesem Hinweis sollte man unbedingt folgen, zumal SAP HANA Systeme bis zur Revision 102 den System Benutzer von der Sperre durch zu viele Falschanmeldungen ausnehmen. Somit wäre ein Brute-Force-Angriff mit dem Ziel das Kennwort des System-Benutzers zu erraten möglich, sofern der Benutzer nicht deaktiviert wurde.
Erst der SAP-Hinweis 2216869 entfernt die Ausnahmeregelung für den System Benutzer. Weiterhin ist es empfehlenswert bei einem System, das durch Dritte eingerichtet wurde, nach der Übergabe direkt das Passwort des System Benutzers zu ändern.

Verschlüsselung

Grundlegend sollte die Kommunikation des SAP HANA Systems verschlüsselt erfolgen. Eine Klartext-Kommunikation ist nicht mehr zeitgemäß. Hierzu sollte das SSL-Protokoll verwendet werden. Dies ist zwar nicht unangreifbar – SSL Proxies und Man in the Middle (MitM) Tools sind im Internet leicht zu finden – doch immerhin wird die Hürde für Angreifer erhöht.

SQL-Verschlüsselung

Der verschlüsselte Zugriff von Klienten auf die Datenbank erfordert Konfiguration sowohl auf Klienten- und Serverseite. Es kann entweder OpenSSL oder die SAP CommonCryptoLib genutzt werden. SAP empfiehlt den Einsatz der CommonCryptoLib und bietet mit dem SAP Hinweis 2093286 eine Anleitung zur Migration von OpenSSL an. In jedem Fall sind private und öffentliche Schlüssel zu erzeugen, die in dem personal security enviroment (pse) abgelegt werden. Hinweise zur Einrichtung finden sich in dem SAP HANA Security Guide [2] unter Punkt 5.3 Securing Data Communication und 5.3.1 Secure Communication Between SAP HANA and
JDBC/ODBC Clients .
Der Einsatz von Selbst-Signierten-Zertifikaten sollte unterbunden werden, da diese besonders anfällig für MitM-Angriffe sind. Diese Einstellung erfolgt über den Parameter sslCreateSelfSignedCertificate (= false) in der indexserver.ini .

Web-Server

Wird HANA mit Applikationsserver betrieben, ist auch der Web-Server ab zu sichern. Der SAP Web Dispatcher sollte ebenfalls SSL verwenden. Dies kann auf verschiedenen Arten erfolgen. Entweder entschlüsselt er Anfragen und verschlüsselt diese erneut bei der Weiterleitung zu dem ICM-Server oder er nutzt eine Ende-zu-Ende SSL Verschlüsselung. Entsprechend sollte die Option wdisp/ssl_encrypt des Parameters icm/server_port_<xx> auf
1, 2 oder ROUTER gesetzt werden. Dies setzt die Einrichtung und Konfiguration von SSL voraus. Der Vorgang ist wiederum in dem SAP HANA Security Guide [2] unter den Punkten 5.3 Securing Data Communication und 5.3.1.1 SSL Configuration on the SAP HANA Server beschrieben. Nach erfolgreicher Einrichtung sollte HANA XS keine unverschlüsselten HTTP Anfragen mehr annehmen. Dies erreicht man über die Option ForceSSL in der Laufzeit Konfiguration.

Persistente Daten

Die In-Memory Daten werden von HANA automatisch zu Widerherstellungszwecken in einem internen Datenvolumen gespeichert. Diese Daten können mit einer 256-Bit AES Verschlüsselung gespeichert werden. Sollte die Verschlüsselungsoption noch nicht konfiguriert sein kann dies mit dem SQL-Befehl „ALTER SYSTEM PERSISTENCE ENCRYPTION ON“ aktiviert werden. Kontrolliert werden kann die Einstellung mit der Prüfung des Feldes ENCRYPTION_ACTIVE_AFTER_NEXT_SAVEPOINT (= true) des System Views M_PERSISTENCE_ENCRYPTION_STATUS.
Die zur Verschlüsselung genutzten Schlüssel sollten regelmäßig geändert werden. Dies übernimmt der SQL-Befehl „ALTER SYSTEM PERSISTENCE ENCRYPTION CREATE NEW KEY” . Eine erneute Verschlüsselung der vorhandenen Daten mit den neuen Schlüsseln bewirkt der Befehl „ALTER SYSTEM PERSISTENCE ENCRYPTION APPLY CURRENT KEY“ .
Nicht verschlüsselt werden bei SAP HANA die redo log und Trace Dateien, diese können auch sensible Daten enthalten. Beispielsweise bei Passwortwechseln. Der unerlaubte Zugriff auf

diese Dateien ist entsprechend einzuschränken. Diese Dateien liegen in der Regel unter /usr/sap/<SID>/HDB<nn>/<hostname>/trace oder $DIR_INSTANCE/<hostname>/trace . Dieses Verzeichnis darf nur für <sid>adm lesbar sein. Auf Datenbankebene sind die Rollen TRACE ADMIN oder DATA ADMIN , welche den Zugriff auf die Logs ebenfalls erlauben entsprechend granular zu vergeben.
Selbiges gilt für Backups der Datenbank. Diese liegen gewöhnlich unter /usr/sap/<SID>/HDB<nn>/backup/data oder $(DIR_INSTANCE)/backup/data und sind auf Dateiebene vor unbefugten Zugriff zu schützen.

Encryption Keys

SAP HANA verwendet diverse Keys zur Datenverschlüsselung. Es wird dringend empfohlen nach der Einrichtung des Systems oder Übergabe die folgenden Schlüssel zu ändern:

- SSFS Master key
- Data volume encryption root key
- Data encryption service root key

Eine Anleitung ist in dem SAP HANA Security Guide [2] unter Abschnitt 9.1.1 Encryption Key Management zu finden.
SSFS liegt gewöhnlich unter /usr/sap/<SID>/SYS/global/hdb/security/ssfs und werden von HANA genutzt um verschiedene sensitive Daten wie einige technische Benutzerdaten zusammen mit den Schlüsseln zur Entschlüssung von automatisch gespeicherten Wiederherstellungsdaten auf Festplatte zu verschlüsseln. Im Auslieferungszustand ist der Master Key jedoch auf allen HANA Systemen derselbe. Daher ist es zwingend notwendig den Master Key unmittelbar zu ändern, andernfalls können die sensiblen Daten mit dem Standard Master Key jederzeit entschlüsselt werden und damit dann auch alle weiteren von HANA gespeicherten Daten.
Eine Anleitung wie der Master Key mit dem rsecssfx Tool geändert werden kann ist hier [6] zu finden.

Benutzer und Autorisierung

HANA bietet viele Möglichkeiten der Authentifizierung. Die verbreitetste Methode ist die Kombination aus Benutzername und Passwort. Es können aber externe Benutzerverwaltungen wie Kerberos oder Security Assertion Markup Language (SAML) genutzt werden. Dies erfordert jedoch immer auch einen passenden Datenbank Benutzer, der eine Zuordnung zur externen Verwaltung enthält.
Ebenso lassen sich auch Zertifikate verwenden, um über HANA XS auf die Datenbank zuzugreifen. Dies setzt jedoch immer die Nutzung von SSL voraus. Auch SAP Login Tickets wie von dem SAP Applikationsserver oder dem Portal erlauben einen Web-basierten Zugriff über HANA XS.
Die letzten 4 Optionen lassen sich auch für Single-Sign-On (SSO) nutzen, wobei Kerberos dann die Installation von Bibliotheken auf dem HANA Klienten erfordert sowie die Zuordnung von Datenbank-Benutzern zu Kerberos Identitäten in dem Kerberos Key Distribution Center.

SAML hingegen kann auch die Installation von zusätzlichen Bibliotheken verzichten und benötigt nur eine Zuordnung der Externen Identitäten zu Datenbank Benutzern.
Eine Nutzung von Benutzername und Passwort zur Authentifizierung sollte nur mit sicheren Passwortrichtlinien einhergehen.

Passwort-Richtlinien

Die Parameter für die Passwort-Richtlinien werden in der indexserver.ini Datei gesetzt. Über den System View M_PASSWORD_POLICY lassen sich die aktuellen Einstellungen einsehen. Die folgende Tabelle vermittelt einen Überblick über die wichtigsten Einstellungen für sichere Passwort-Richtlinien.

Parameter	Standard	Empfehlung DSAG 2015 [5]
minimal_password_length	8	8-10
password_layout	Aa1	A1a$
force_first_password_change	True	True
last_used_passwords	5	15
maximum_invalid_connect_attempts	6	3
password_lock_time	1440	259200
minimum_password_lifetime	1	1
maximum_password_lifetime	180	90
maximum_unused_initial_password _lifetime	28	5
maximum_unused_productive_password _lifetime	365	180
password_expire_warning_time	14	14
password_lock_for_system_user	False bis R102, dann True	true

Technische Benutzer lassen sich von dem Passwort Lifetime Check über folgenden SQL Befehl ausnehmen „ALTER USER <benutzername> DISABLE PASSWORD LIFETIME“ .
Verbotene Passwörter können in der Tabelle _SYS_PASSWORD_BLACKLIST (_SYS_SECURITY) hinterlegt werden. Im Auslieferungszustand sind keine Passwörter dort hinterlegt.

Rollen und Berechtigungen

SAP empfiehlt die Nutzung von (den mitgelieferten) Rollen statt Berechtigungen direkt an Benutzer zu vergeben. Dazu liefert SAP viele Rollen aus, die für die meisten Geschäftsprozessen passen sollten. Ebenso gibt es ein Template zur Erstellung von angepassten Rollen.
Bei der Erstellung von Benutzern und der Vergabe von Rechten sollten folgende Punkte beachtet werden:

- Benutzer sollten immer mit dem Befehl „Create Restricted User“ angelegt werden, damit sie nicht automatisch die Rolle „Public“ erhalten.
- Benutzer sollten immer nur die minimal notwendigen Berechtigungen erhalten.
- Prüfen Sie regelmäßig ob Benutzer sensible Berechtigungen erhalten haben. Dies kann mit der SQL Abfrage „SELECT * FROM SYS.EFFECTIVE_PRIVILEGES WHERE USER_NAME=<USERNAME>“ erfolgen.
- Wird SAP HANA nur als Datenbank verwendet, sollten nur technische Nutzer für Verbindungen zur Datenbank erforderlich sein.

Auditing und Logging

Zur Nachverfolgung von kritischen Systemaktivitäten ist ein aktives Auditing und Logging erforderlich. Dies kann unter HANA mit dem Befehl ALTER SYSTEM LOGGING ON aktiviert werden. Hierzu benötigt man entweder AUDIT ADMIN oder INFILE ADMIN Rechte. Ob das Auditing aktiv ist zeigt der auditing_state Parameter der global.ini Datei mit dem Wert true an.
Eine Ausführliche Anleitung zur Konfiguration des Loggings ist im SAP HANA Security Guide [2] unter Abschnitt 10 Auditing Activity in SAP HANA Systems zu finden.

Audit Policies

Mittels Audit Policies wird definiert was konkret von HANA geloggt werden soll. Hier empfiehlt es sich lesende und ändernde Zugriffe auf die Datenbank sowie die Ausführung von Befehlen zu loggen.
Die Erstellung einer Entsprechende Policy „access_audit“ kann mit diesem Befehl erfolgen:
CREATE AUDIT POLICY access_audit AUDITING SUCCESSFUL INSERT, UPDATE, DELETE, SELECT, EXECUTE LEVEL CRITICAL;

Manipulationssicheres Logging

Die Logdaten sind vor unbefugten Lese- und Schreibzugriff zu schützen. In der Standardeinstellung werden alle Logdaten in das Trace Verzeichnis /usr/sap/<sid>/<instance>/<host>/trace gespeichert. Auf dieses Verzeichnis haben alle Datenbank Benutzer mit den Rechten DATA ADMIN, CATALOG READ, TRACE ADMIN oder INFILE ADMIN automatisch Zugriff ebenso wie alle System Benutzer aus der SAPSYS Gruppe auf Dateiebene. Die Pfad-Einstellung kann mit dem Parameter default_audit_trail_path geändert werden.
Grundlegend sollte zur Speicherung der Logdaten der Syslog-Dienst genutzt werden. Hierzu ist der Parameter default_audit_trail_type auf SYSLOGPROTOCOL zu setzen. Zusätzlich sollte der lokale Syslog-Dienst so konfiguriert sein, dass er alle Logs an einen zentralen und sicheren Logserver weiterreicht. Somit erreicht man ein manipulationssicheres Logging.
Einen Haken jedoch hat auch das Syslog Protokoll. In der Regel versendet es die Daten im Klartext, was sensible Informationen im Netzwerk preisgeben kann. Entweder richtet man ein privates Netzwerk zur Übertragung ein, eine zusätzliche Transportverschlüsselung wie VPN oder IPSec oder nutzt Syslog mit TLS (TCP 6514).

Patchmanagement

SAP HANA hält als Datenbank System geschäftskritische Daten in seinem Speicher. Neben dem Schutz der Daten durch eine sichere Systemkonfiguration, muss auch ein Schutz gegen technische Schwachstellen erfolgen.
SAP veröffentlicht hierzu regelmäßig im Rahmen seines Patchdays auch Security-Updates für SAP HANA. Teilweise enthalten diese Fehlerbereinigungen für kritische Lücken wie

beispielsweise die Ausführung von beliebigen Befehlen oder Dateizugriffen aus dem Netzwerk ganz ohne Authentifizierung am System.
Es ist daher notwendig HANA Systeme zeitnah mit den neuesten Updates zu versorgen.

Validierung von Benutzereingaben bei HANA XS Eigenentwicklungen

Bei einem Einsatz als Applikationsserver und Entwicklungssystem, sind die hier im Folgenden beschriebenen zusätzlichen Sicherheitsempfehlungen zu beachten. HANA ist eine offene Plattform und ermöglicht mit der HANA XS Engine die Entwicklung eigener XSJS-Anwendungen.
Damit diese Eigenentwicklungen nicht zum Einfallstor für Angreifer werden, muss ein sicherer Umgang mit allen Benutzereingaben gewährleistet sein.

XSS-Filter

Nahezu ein Viertel alle Schwachstellen in SAP Produkten sind XSS Schwachstellen [8]. SAP hat darauf reagiert und seinem Web Dispatcher einen XSS-Filter spendiert. Dieser prüft alle eingehenden Anfragen entweder nach dem White-List Ansatz auf rein erlaubte Muster [7] oder nach dem Black-List Ansatz auf Angriffs-Muster. Entsprechend werden nur „gültige“ Anfragen erlaubt. Der Standard Filter enthält eine Black-List mit diesem Muster:
<\s*script[^>]*>(.*)<\s*/script\s*>
Jedoch gibt es im Internet [10] zahlreiche Tipps wie solche Filter umgangen werden können. Daher ist der XSS-Filter nicht als alleiniger Schutz ausreichend. Benutzereingaben sind in HANA XS Anwendungen zwingend sicher zu handhaben. Hierzu stellt SAP eine Reihe an Werkzeugen zur Verfügung, die ein Entwickler nutzen kann.
Die Controls der SAPUI5 validieren automatisch die Inhalte der Eingaben und sorgen dafür, dass nur legitime Eingaben als Werte enthalten sind.
Werden Benutzereingaben in HTML-Ausgaben verwenden gibt es diverse Funktionen, um diese sicher anzuzeigen. Hierzu zählen writeEscaped(oControl.getSomeStringProperty()) statt write oder writeAttributeEscaped(“someHtmlProperty”, oControl.getSomeStringProperty()) statt writeAttribute und jQuery.sap.escapeHTML(oControl.getSomeStringProperty()) für alle übrigen Datenwerte.

SQL-Injection

Ein weiterer Angriffspunkt sind SQL-Injections [9]. Diese werden möglich, wenn Benutzereingaben ungefiltert in SQL-Anweisungen eingebettet werden. Ein einfaches Beispiel soll das Gefährdungspotential von SQL-Injection veranschaulichen:
Eine exemplarische Login Seite erfordert die Angabe von Benutzer (Variable Name) und Passwort (Variable PWD) . Zur einfachen Veranschaulichung prüft die Login-Seite anschließend ob die eingegebene Kombination von Benutzer und Passwort so in der Datenbank vorkommt.
Dies übernimmt diese Abfrage

*var query = "SELECT * FROM USERS WHERE name = '" + Name + "' AND password = '" + PWD +"'";*
Bei einer normalen Eingabe wie *Name = Hans* und *PWD = 123* kann die Login Seite nun prüfen ob ein solcher Eintrag in der User Tabelle existiert und entsprechend Zugang gewähren oder verweigern.
Die zu den Eingaben generierte Abfrage sieht in diesem Fall wie folgt aus:

*SELECT * FROM USERS WHERE name = 'Hans' AND password = '123'*

Gibt ein findiger Benutzer nun aber folgendes ein

Benutzer = Dietrich
PWD = egal' or 'a' = 'a

werden diese Benutzereingaben ungeprüft von der Login Seite übernommen führt dies zu der folgenden Abfrage:

*SELECT * FROM USERS WHERE name = 'Dietrich' AND password = 'egal' or 'a' = 'a'*

Damit wäre sodann ein Login an der Seite ohne gültige Zugangsdaten möglich, da die Datenbank den Teil "*or 'a' = 'a'*" immer mit wahr beantworten wird und alle Datensätze der Tabelle Users zurückgeben werden. Eine einfache Abwehrmaßnahme ist hier die Verwendung von Prepared-Statements [14]. Natürlich sollte weiterhin jede Benutzereingabe validiert erfolgen mit den bereits zuvor beschriebenen Möglichkeiten die die SAPUI5 bietet.

Zusammenfassung

SAP HANA verarbeiten und speichern kritischen Geschäftsdaten. Die hier gelagerten und verarbeiteten Daten sind sehr wertvoll. Verschiedenartig motivierte Angreifer haben den Wert der Systeme erkannt und verfügen über spezialisierte Angriffswege, um Zugriff auf die Systeme zu erhalten. Die Komplexität von HANA erfordert bewusste Sicherheitsmaßnahmen an verschiedenen Stellen (Netzwerk, Verschlüsselung, Autorisierung, Patchmanagement,…) zur Erhöhung der Robustheit gegen Angriffe. Ein erfolgreicher Angriff hat immenses Schadenspotential für das betroffene Unternehmen. Zur Minimierung der Risiken muss eine kontinuierliche Überwachung des Sicherheitsniveaus von HANA-Systemen erfolgen und Maßnahmen zur Beseitigung von Schwachstellen abgeleitet und umgesetzt werden. Sicherheitsprogramme wie unsere Lösung Werth Auditor [1] unterstützen diesen Prozess und führen zu einer Entlastung der Ressourcen.

Quellen

[1] SAP-Security-Scanner Werth Auditor
http://www.werth-it.de/auditor.html

[2] SAP HANA Security Guide
http://scn.sap.com/docs/DOC-60371

[3] SAP HANA Administration Guide
http://scn.sap.com/docs/DOC-60368

[4] Connections from Database Clients and Web Clients to SAP HANA
http://help.sap.com/saphelp_hanaplatform/helpdata/en/37/d2573cb24e4d75a23e8577fb4f73b7/content.htm

[5] DSAG Prüfleitfaden 2015
http://www.dsag.de/E-Pruefleitfaden6.0

[6] Change the SSFS Master Keys
https://help.sap.com/saphelp_hanaplatform/helpdata/en/58/1593c48739431caaccc3d2ef55c23f/frameset.htm

[7] Muster
http://help.sap.com/saphelp_nw73/helpdata/de/4e/2606c0c61920cee10000000a42189c/content.htm?current_toc=%2Fde%2Fae%2Fad1640033ae569e10000000a155106%2Fplain.htm

[8] Cross-site Scripting (XSS)
https://www.owasp.org/index.php/XSS

[9] SQL Injection
https://www.owasp.org/index.php/SQL_Injection

[10] XSS Filter Evasion Cheat Sheet
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

[11] SAP HANA as Primary Persistence for SAP NetWeaver-Based Applications
http://help.sap.com/saphelp_hanaplatform/helpdata/en/d6/7f115f365040c88127522cf5634671/content.htm?frameset=/en/5d/c576aee5d04deba9fba37b2d758df2/frameset.htm&current_toc=/en/d4/3377c2bb57101489ebe2e6a1813cfc/plain.htm&node_id=7

[12] SAP HANA as Data Mart
http://help.sap.com/saphelp_hanaplatform/helpdata/en/5d/c576aee5d04deba9fba37b2d758df2/content.htm?frameset=/en/26/832459dd8c46649645bc6cec492966/frameset.htm&current_toc=/en/d4/3377c2bb57101489ebe2e6a1813cfc/plain.htm&node_id=8

[13] SAP HANA as Application and Development Platform
http://help.sap.com/saphelp_hanaplatform/helpdata/en/ed/9798305fbd46628de3dee3e3b04b48/content.htm?frameset=/en/5d/c576aee5d04deba9fba37b2d758df2/frameset.htm&current_toc=/en/d4/3377c2bb57101489ebe2e6a1813cfc/plain.htm&node_id=16

[14] Beispiel für die Verwendung von Prepared Statements
https://help.hana.ondemand.com/help/frameset.htm?937ca0a472bb101490cf767db0e91070.html

Über Werth IT

Die Werth IT GmbH kennt die Forderungen von Unternehmen an die IT-Sicherheit von SAP Systemen und nimmt den besonderen IT-Security-Bedarf sehr ernst. Aus diesem Grunde hat das Experten-Team mit hohem Bewusstsein für Qualität einen SAP-Security Scanner entwickelt, der vollständig das Prüfspektrum für SAP-Systeme abdeckt.

Mit dem intuitiv bedienbaren SAP-Security Scanner setzt die Werth IT GmbH bewusst auf die leichte Handhabung und aussagekräftige Ergebnislisten, die heute bereits namhaften Unternehmen helfen, die vorhandenen SAP-Sicherheitslücken auch bei wachsender Komplexität und gleichzeitigem Fachkräftemangel effizient zu schließen.

Als Vorreiter in der IT-Security von SAP Systemen ist es das Ziel der Werth IT GmbH, dass digitale Unternehmensdaten genau dort bleiben sollen, wo sie hingehören – nämlich im Unternehmen. Um das gemeinsam sicher zu erreichen, setzt sich der IT-Dienstleister voller Leidenschaft immer für faire Partnerschaften und wertschätzende Kundennähe ein.

werth
sap security solutions
http://www.werth-it.de