WERTH

WERTH auditor
sicherheit für sap-systeme

Forensische Analyse

von SAP- Systemen

Autor: Thomas Werth

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 veröffentlich die Werth IT dieses Dokument.

Einleitung

SAP ist einer der größten Softwarehersteller weltweit. Der Fokus liegt dabei auf Enterprise Resource Planning (ERP) Produkten. In diesen Systemen speichern Unternehmen ihr wahres Kapital – nämlich Ihre Daten.
Die folgenden fünf Anwendungen stellen die wichtigsten Bereiche in SAP dar:

- SAP ERP Central Component (SAP ECC), ehemals bekannt als R/3
- Customer Relationship Management (CRM)
- Product Lifecycle Management (PLM)
- Supply Chain Management (SCM)
- Supplier Relationship Management (SRM)

Damit sind SAP-Systeme ein lohnendes Ziel für Cyber-Angriffe. Egal ob Spionage, Sabotage oder Betrug die Motivation ist, die Daten in dem SAP-System geben ein attraktives Ziel ab. Daher ist es von immenser Bedeutung Angriffe auf ein SAP-System identifizieren zu können. Dieser Leitfaden dient daher dem Ziel Angriffe durch forensische Analyse mittels der SAP-Bord-Möglichkeiten aufzuspüren.

Vorbemerkung zur forensischen Analyse

Damit eine forensische Auswertung eines SAP-Systems erfolgen kann, muss der Analytiker zwingend wissen an welcher Stelle im System welche Sicherheitsrelevanten Ereignisse protokolliert werden. Ebenso muss er die Einschränkungen und Eigenschaften der jeweiligen Log-Daten kennen, um den Inhalt (oder eben den fehlenden Inhalt) korrekt in seine Untersuchung einfließen lassen zu können.
Weiterhin ist zu beachten, dass die meisten Logging-Mechanismen zunächst deaktiviert sind und erst in Betrieb genommen werden müssen. Es gilt also zu prüfen, welche Logs stehen überhaupt zur Verfügung und wo sind diese zu finden.
Dieses Dokument soll daher die wichtigsten Logs eines SAP-Systems aufzeigen und deren Inhalt und Eigenschaften beschreiben, damit im Falle einer notwendigen Untersuchung eines SAP-Systems ein Leitfaden existiert, der aufzeigt wo welche Informationen zu finden sind.
Ebenso sind die System-Betreiber frühzeitig angehalten die Protokollierung zu aktivieren, denn nur eine aktive Protokollierung kann bei Aufklärung von Verdachtsfällen unterstützen. Weiterhin sollten Maßnahmen ergriffen werden, um das Risiko erfolgreicher Angriffe zu senken:

- SAP Empfehlungen und Guides befolgen
- Regelmäßge Security Audits
- SAP Patches einspielen
- ABAP Code Kontrolle
- Pflege und Prüfung des Berechtigungskonzepts
- Protokollierung aktivieren und prüfen.

Security Audit Log

Beschreibung

"Das Security-Audit-Log ist ein Werkzeug für Auditoren, die sich die Ereignisse im SAP-System detailliert ansehen müssen. Wenn Sie das Security-Audit-Log aktivieren, zeichnen Sie die Aktionen auf, die Sie für die Verfolgung als relevant einstufen. Sie können dann in Form eines Audit-Analysereports auf diese Informationen zugreifen und sie auswerten.

Oberstes Ziel des Audit-Log ist die Aufzeichnung von:

- *sicherheitsbezogenen Änderungen an der SAP-Systemumgebung (z. B. Änderungen an Benutzerstammsätzen)*

- *Informationen, die mehr Transparenz bieten (z. B. erfolgreiche und erfolglose Anmeldeversuche)*

- *Informationen, die der Nachvollziehbarkeit einer Reihe von Ereignissen dienen (z. B. erfolgreiche oder erfolglose Transaktionsstarts)"* [1]

Das Security Audit Log ist im Standard nicht aktiviert und muss manuell gestartet werden. Die Logdatei wird im Pfad /usr/sap/<SID>/<INSTANCE>/log/audit_date gespeichert. Die Größe der Logdatei kann über den Profilparameter rsau/max_diskspace/local definiert werden. Der Vorschlagswert ist 1MB. Wird dieses Limit erreicht stoppt das Logging und erst mit dem nächsten Tag und einer neuen Logdatei wird wieder protokolliert!
Der Inhalt des Logs kann über die SAP-Transaktion SM20 eingesehen werden. Jede Logmeldung verfügt über folgende Informationen:

- Servername

- Instanzname
- Workprozess-Typ
- SAP-Benutzer
- Terminalname
- Workprozessnummer
- Transaktionscode
- Programmname
- Mandant
- Meldungstext
- Meldungsgruppe
- Untergeordneter Name (wird zur Bestimmung der Meldungsgruppe verwendet)
- Audit-Klasse
- Sicherheitsstufe
- Dateinummer
- Adresse in Datei
- Parameter, die für den Meldungstext verwendet werden

Damit lässt sich der genaue Zeitpunkt, der verursachende User und Quellcomputer sowie die protokollierte Aktion bestimmen.
Dieses Log beinhaltet sehr viele Informationen und kann durch die Abfrage-Filter in der SM20 sehr gezielt ausgewertet werden.

Systemlog

Beschreibung

„Mit Hilfe des Systemlogs können Sie Fehler in Ihrem System und dessen Umfeld feststellen und beheben.“ [2]
Das Systemlog ist automatisch aktiv und findet sich unter /usr/sap/<SID>/<INSTANCE>/log/SLOG<SYSNR> wie das Auditlog wird sein maximale Größe durch einen Profilparameter (rslg/max_diskspace/local) bestimmt und liegt im Standard bei 1MB. Der Zugriff auf das Log erfolgt über die Transaktion SM21 im SAP-System.
Hauptsächlich finden sich hier technische Informationen zu Programmfehlern. Ein Eintrag beinhaltet immer Daten zu dem User, Clienten sowie der Aufgerufen Transaktion oder dem Programm und Details zu dem Fehler.

SAP-Gateway-Logging

Beschreibung

„Das Gateway stellt eine Schnittstelle des Applikationsserver zu anderen SAP-Systemen bzw. Programmen dar. … Das SAP-Gateway-Logging dient zum Überwachen der Aktivitäten des SAP-Gateways. Sie können konfigurieren, welche Aktionen des SAP-Gateways protokolliert werden sollen. Diese werden dann in eine Log-Datei geschrieben. Die Log-Datei wird nach dem Zeitstempel Ihrer Erzeugung benannt, wobei Sie das genaue Format ebenfalls konfigurieren können.“ [3]

Das SAP-Gateway-Logging ist per Default nicht aktiviert. Der Speicherort der Datei befindet sich unter /usr/sap/<SID>/<INSTANCE>/work/<file_name>, wobei <file_name> durch den Parameter LOGFILE zu definieren ist. Die maximale Größe richtet sich nach dem Parameter MAXSIZEKB . [4]

Sobald die maximale Dateigröße erreicht ist, wird eine neue Datei angelegt und das Logging läuft weiter. Es sei denn der Parameter FILEWRAP wird auf on gesetzt, dann wird die vorhanden Logdatei einfach wieder geöffnet und überschrieben.

Der Zugriff auf die Loginhalte erfolgt im SAP-System über die Transaktion SMGW.

Das Gateway-Log liefert Informationen zu dem Datum und der Uhrzeit, dem Quellserver und der ausgeführten Aktion (Verbindung zu Server, Start Server, Register Server, usw.) .

Aus forensischer Sicht wird in den Log-Einträgen nach der Ausführung von Monitor-Befehlen, Änderungen in der Sicherheitskonfiguration sowie der Registrierung potentiell schädlicher RFC-Server oder dem Start kritischer RFC-Server gesucht.

ICM und SAP Web Dispatcher Logging

Beschreibung

„Der SAP Web Dispatcher steht zwischen dem Internet und Ihrem SAP-System. Er dient als Einstiegspunkt für HTTP(S)-Requests in Ihr System, das aus einem oder mehreren SAP NetWeaver Application Servern besteht. Als "Software-Web-Switch" kann er Verbindungen abweisen oder annehmen und nimmt dann die Request-Verteilung für eine gleichmäßige Serverauslastung vor. Der SAP Web Dispatcher trägt also zum einen zur Sicherheit bei und führt zum anderen den Lastausgleich (oder Loadbalancing) in Ihrem SAP-System durch.

Sie können den SAP Web Dispatcher sowohl in reinen ABAP-Systemen als auch in kombinierten

ABAP/Java-Systemen ("Dual-Stack") und reinen Java-Systemen einsetzen." [5]

Der SAP Web Dispatcher nimmt somit die Funktion eines Load-Balancers und / oder einer Web Application Firewall ein. Aus der forensischen perspektive sind der SAP Web Dispatcher und der ICM nahezu gleich zu betrachten.

„Der Internet Communication Manager gewährleistet die Kommunikation zwischen dem SAP-System (SAP NetWeaver Application Server) mit der Außenwelt über die Protokolle HTTP, HTTPS und SMTP. In der Serverrolle kann er Anfragen aus dem Internet bearbeiten, die mit URLs mit der Server/Port-Kombination, auf die der ICM hört, ankommen. Abhängig von der URL ruft der ICM dann den entsprechenden lokalen Handler auf." [6]

Beide erzeugen zwei forensisch relevante Logdateien: Das Security Log und das HTTP Log.

Security Log

Das Security Log ist nur bei dem ICM standardmäßig aktiviert und liegt in dem Pfad /usr/sap/<SID>/<INSTANCE>/work/dev_icm_sec .
Bei dem SAP Web Dispatcher muss das Log erst von einem Administrator aktiviert werden und dieser muss auch den Dateipfad vorgeben.
Die Größe des Logfiles wird mit dem Parameter *MAXSIZEKB* vorgegeben, der Standardwert liegt bei 10000. [7]
Wie sich das Log verhalten soll, wenn das Limit erreicht ist, spezifiziert der Parameter *FILEWRAP*. Wird dieser Parameter auf *on* gesetzt, wird bei Erreichen der Maximalen Größe die Logdatei zurückgesetzt und neu geschrieben. Alle Logeinträge gehen verloren!
Die Logdatei kann bei dem Web Dispatcher über das Betriebssystem eingesehen werden. Das ICM bietet den Weg über die Transaktion MICM in dem SAP-System.
Dieses Log kann genutzt werden, um fehlgeschlagene Loginversuche an der Web Administration zu erfassen. Sowie HTTP Fuzzing Versuche aufzudecken.
Das Log bietet dabei die Informationen über Datum und Uhrzeit, der IP des Angreifers und Inhalt der Anfrage in Abhängigkeit des eingestellten Loglevels.

HTTP Log

Das HTTP Log ist weder bei dem ICM noch bei dem SAP Web Dispatcher per Voreinstellung aktiv. Der Speicherort wird über den Parameter icm/HTTP/logging_XX angegeben. [8]

Wie bei dem Security Log wird die maximale Dateigröße durch den Parameter MAXSIZEKB und das Verhalten bei Erreichen der Grenze durch den Parameter FILEWRAP gesteuert. Auch der Zugriff auf die Logdatei ist identisch über die MICM beim ICM sowie über den Dateizugriff auf Betriebssystemebene bei dem Web Dispatcher gehandhabt.

Das HTTP Log vermerkt spezifische Zugriffsereignisse wie Zugriffe ohne Authentifizierung (HTTP Code 401) oder Fuzzing Zugriff (HTTP Code 400). Generell wird auch der Zugriff auf kritische Webseiten hier protokolliert.

Das Log bietet dabei die Informationen über Datum und Uhrzeit, der IP des Angreifers, den angegebenen Benutzer zur Autorisierung, die HTTP Anfrage mit Parametern und Headern, den HTTP Antwort Code sowie den Inhalt der Anfrage in Abhängigkeit des eingestellten LOGFORMATes.

J2EE Logging

Beschreibung

SAP Java Instanzen haben Standardmäßig das Logging aktiv. Dabei wird es im „simple mode“ betrieben, es werden also nur schwerwiegende Fehler und Ereignisse protokolliert. [19]
Der Standardpfad der Logdateien liegt unter \usr\sap\<SID>\<Instanzname>\j2ee\cluster\<Servername>\log [20]
Es werde alle sicherheitsrelevanten und administrativen Tätigkeiten des Systems erfasst. Ebenso alle Ereignisse, die die Geschäftslogik betreffen.
Zusätzlich finden sich Entwickler-Traces in \usr\sap\<SAPSID>\<instance name>\work und die Java Server-Logs in \usr\sap\<SAPSID>\<instance name>\j2ee\cluster\server<n>\log [21]

Ein sehr wichtiges Log ist die Logdatei für die Responses. In diesem sieht man wann das System wie auf HTTP-Anfragen reagiert hat. [22]
Finden sich in diesem Log „HEAD“ Anfragen, so können diese Einträge als Hinweise auf Verb Tampering Angriffe gesehen werden. Hier gilt es dann besonders gründlich die Angefragte URL mitsamt Ihren Parametern zu prüfen.
Ebenso lassen sich XSS Angriffe durch die Suche nach Schlüsselwörtern wie „%3C/script%3E“ identifizieren. Auch die berühmten Diretory-Traversal-Angriffe können hier aufgespürt werden. Eine Suche nach „/../“ oder „!252f..!252f“ kann hier als Ausgangspunkt verwendet werden.

Message Server Logging

Beschreibung

Das Message Server Logging ist abhängig von dem globalen Trace-Logging [14] as. Die Trace-Datei (dev_ms) kann über die Transaktion SMMS und dem Menüpunkt Springen->Trace eingesehen werden. Über den Parameter ms/audit kann die Protokollierung für den Message Server eingeschaltet werden. Mit dem Wert 1 werden An- und Abmeldungen protokolliert und der Wert 2 loggt auch Aktivierungen und Suspends eines Clients [18] ohne die Erfordernis das Trace Level zu erhöhen.

Protokollierung Datenänderungen in Tabellen

Beschreibung

Ein SAP-System legt seine Daten in Tabellen ab. Änderungen an Tabellen können protokolliert werden. So kann nachvollzogen werden wer wann welche Tabellen und Werte geändert hat.
Die Tabellenprotokollierung ist im Standard nicht aktiv. Änderungen können über zwei Wege erfolgen. Entweder über das Transportsystem oder durch Änderungen im SAP-System selbst.
Die Protokollierung von Änderungen ist für die möglichen Wege getrennt zu aktivieren. Für den Weg über das SAP-System selbst ist der Profilparameter rec/client auf ALL oder eine Komma-getrennte Liste der zu überwachenden Mandanten zu setzen. Für das Transportwesen muss der Wert r3transoptions = recclient="XXX" in das Transportprofil aufgenommen werden. [9]
Die Protokolldaten werden in der Tabelle DBTABLOG hinterlegt und es existiert keine Obergrenze für die Datengröße. Die Logdaten können über die SAP-Transaktion SCU3 eingesehen werden.
Ein Logeintrag liefert Informationen zu dem Zeitpunkt, zu dem Benutzer und dem Applikations-Server auf dem die Änderung vorgenommen wurde sowie zu der Tabelle und den Feldwerten (alt und neu).

Protokollierung Änderung Benutzer und Berechtigungen

Beschreibung

Ein SAP-System protokolliert Änderungen an Benutzer- und Berechtigungsdaten automatisch. [10]
Die Logdaten werden in den USHXX Tabellen (wie USH02, USH04,...) unbegrenzt abgelegt. Die historischen Daten sind über den ABAP-Report RSUSR100N einsehbar.
In den Logdaten ist ersichtlich wann und von wem eine Änderung vorgenommen wurde. Ebenso welcher Benutzer von der Änderung betroffen ist und über welchen Programm oder Transaktion die Änderung erfolgt ist.
Direkte Änderungen von Benutzer auf Datenbankebene können von diesem Log nicht erfasst werden. Unter normalen Umständen sollte so etwas jedoch niemals vorkommen. Interessant ist

hier unter anderem welche Benutzer SAP_ALL oder SAP_NEW Profile erhalten bzw. verloren haben.

Protokollierung Änderungsbelege

Beschreibung

Betriebswirtschaftliche Objekte wie Verkaufsbelege, Kreditkartendaten oder Lieferantendaten unterliegen häufigen Änderungen. SAP-Systeme protokollieren Änderungen an diesen Objekten in Änderungsbelegen. Dies ist besonders wichtig für Objekte die kritisch sind oder der Revisionen unterliegen. Oft ist es sinnvoll oder sogar notwendig, solche Änderungen später nachvollziehen zu können, z. B. zu Revisionszwecken. Ebenso können eigene Änderungsbelege angelegt werden. [11]
Die Daten der Protokollierung werden in den Tabellen CDHDR und CDPOS abgelegt. Eine Limitierung für den Speicherplatz gibt es nicht. Der Zugriff auf die Daten erfolgt über den ABAP-Report RSSCD200.
In den Logs ist der Benutzername, das Datum der Änderung die genutzte Transaktion sowie die Art der Änderung und die Änderungsnummer des Belegs einsehbar.

Systemtrace

Beschreibung

Ein Systemtrace wird genutzt um interne SAP-Systemaktivitäten im Bedarfsfall aufzuzeichnen. Dazu gehören Berechtigungsprüfungen, Datenbankzugriffe oder auch RFC-Aufrufe. [12]
Die Logdatei wird unter */usr/sap/<SID>/<INSTANCE>/log/TRACE* abgelegt. Die Logdatei ist in der Regel auf 10 MB begrenzt und auf 10 Dateien limitiert. Die Dateien werden bei Erreichen der maximalen Größe überschrieben. Zu erreichen ist der Systemtrace über die Transaktion ST01. In einem Trace finden sich Informationen zu dem Zeitpunkt, den Benutzer und den Mandanten sowie zu dem RFC oder Tabellen Zugriff, der Dauer und einige Ereignisbezogene Informationen.

Entwickler-Trace

Beschreibung

„Entwickler-Traces sind Aufzeichnungen, die technische Informationen enthalten und im Fehlerfalle herangezogen werden. Um mit diesen Einträgen effektiv arbeiten zu können, sind genaue Kenntnisse des Hostsystems, in dem Ihr SAP-System läuft, und des SAP-Systems im allgemeinen erforderlich.

Diese Art der Ablaufverfolgung ist besonders nützlich, um Host- und SAP-interne Probleme zu untersuchen, die Ihr SAP-System beeinträchtigen.“
[13]

Entwickler-Traces sind standardmäßig aktiv mit dem TRACE Level 1. Alle Entwickler-Traces werden in separaten Dateien in dem Verzeichnis */usr/sap/<SID>/<INSTANCE>/work/* gespeichert.

Eine Übersicht der Dateinamen ist der SAP-Hilfe wie auf folgendem Screenshot [13] dargestellt zu entnehmen.

Dateinamen von Entwickler-Traces

Die Trace-Dateien haben folgende Namen:

Dateinamen für Entwickler-Traces

Komponente	Dateiname
Dispatcher	`dev_disp`
Workprozess /Taskhandler	`dev_w<n>`, wobei `n` die Nummer des Workprozesses ist
Gateway	`dev_rd`
Message-Server	`dev_ms`
Internet Communication Manager (ICM)	`dev_icm`
SAP Web Dispatcher	`dev_wdisp`
RFC- (Remote Function Call) Funktion	`dev_rfc`, `dev_rfc<n>` `dev_rfc` verfolgt RFC-Aufrufe externer Funktionen (in C oder Visual Basic geschrieben). `dev_rfc<n>` verfolgt RFC-Aufrufe, die in SAP-Workprozessen ausgeführt werden. `<n>` ist die Nummer des Workprozesses im Server (wie oben gezeigt). Ein Workprozess verwendet für alle RFC-Aufrufe dieselbe Protokolldatei.
ICF (Internet Communication Framework	`dev_icf<n>` Weitere Informationen: Fehlerinformationen verwalten
Enqueue (Sperre)	Beim Betrieb einer klassischen Zentralinstanz mit Enqueue-Workprozessdev_w<n>, wobei `w<n>` der Enqueue-Workprozess ist. Beim Einsatz des Standalone-Enqueue-Server in einer ASCS-Instanz mit dem Message-Server gibt es mehrere Trace-Dateien, die alle mit `dev_enq` beginnen. Weitere Informationen: Trace-Dateien des Standalone-Enqueue-Servers und Replikationsservers
Startup Service (`sapstart`)	`dev_sapstart`
Transportprogramme `R3trans` und tp	`dev_tp`
Überwachungsinfrastruktur (nur Test-Modus)	`dev_moni` Bei normalen Betrieb ist diese Datei nicht zu sehen. Sie wird nur von Test-Tools der Überwachungsinfrastruktur verwendet. Sie erscheint daher nur, wenn die Test-Tools während einer Support-Sitzung aktiviert werden müssen.

Die maximale Größe kann über den Parameter *rdisp/TRACE_LOGGING* gesetzt werden. Wird die maximale Größe erreicht, wird der geloggte Inhalt in die Datei mit dem Lognamen+ „.log“ kopiert und die eigentliche Logdatei erneut überschrieben. [14]

Der Detailgrad der Protokollierung kann über den Profilparameter *rdisp/TRACE* gesetzt werden. [15]

Ebenso akzeptiert das SAP-System per Default das Remote-Vorgeben von Trace-Leveln (*rdisp/accept_remote_trace_level* und *gw/accept_remote_trace_level*). Auch mit den Umgebungsvariablen *CPIC_TRACE* und *RFC_TRACE* kann der Level angegeben werden.

Den Zugriff auf die Traces erhält man über die SAP-Transaktion *ST11* . Die geloggten Informationen unterscheiden sich stark nach dem Dienst, der die Log-Datei anlegt und nach dem Trace-Level. So lassen sich hier unter anderem Informationen zu RFC, Speicher, Konfigurationen oder Fehlermeldungen finden.

SAProuter

Beschreibung

„SAProuter ist ein SAP-Programm, das Ihr SAP-Netzwerk vor unbefugtem Zugriff schützen kann. Es handelt sich um ein kleines Standalone-Programm, das normalerweise auf dem Firewallrechner installiert wird." (Quelle: https://help.sap.com/saphelp_nwpi71/helpdata/de/4f/993172446d11d189700000e8322d00/frameset.htm)
Über die Route-Permission-Tabelle werden die zu erlaubenden und zu verbietenden Zugriffe auf die zu schützenden SAP-Systeme definiert.

SAProuter Log

Das SAProuter Log ist manuell zu aktivieren. Der Speicherort wird über den Programmparameter –G definiert. Das Logfile besitzt keine maximale Größe, außer es wird über den Parameter –J eine vorgegeben. Bei dem Erreichen einer maximalen Größe wird in einer neuen Datei weiter geloggt. Der Zugriff auf die Logdatei erfolgt über das Betriebssystem.
Analysiert man die Logdatei erkennt man erlaubte Zugriffe an dem Schlüsselwort *CONNECT TO*. Abgewiesene Zugriffe geben sich durch ein *PERM DENIED* zu erkennen.
Fehlkonfigurierte SAProuter erlauben das ungefilterte Abrufen von internen Informationen. Erfolgreiche Info_Requests lassen sich an dem Eintrag *SEND INFO* erkennen. Fehlgeschlagene Versuche werden mit *PERM DENIED XX/- info request* protokolliert.
Ein SAProuter erlaubt zwei Verbindungstypen:
Das SAP Protokoll für SAP DIAG Verbindungen sowie den Typ Native, welcher einfache TCP Verbindungen erlaubt. Zugriffe über das Native Protokoll sind in der Logdatei an dem Schlüsselwort ****NATIVE ROUTING **** zu erkennen.

Anhand der hier geschilderten Einträge lässt sich erkennen wann (Datum und Uhrzeit) ein Zugriff mit welchem Verbindungstyp erfolgreich oder nicht erfolgreich unternommen wurde. Finden sich in der Logdatei viele verbotene Zugriffsversuche wo sich lediglich der Port bei dem Verbindungsziel (Logeintrag: XXX PERM DENIED XXX to <IP>/<Port>) ändert, kann man hier sicher von einem identifizierten Port-Scan sprechen.

SQL Audit

Beschreibung

Das SQL Audit protokolliert alle OPEN SQL SELECT Statements auf bestimmte Tabellen in Dialog Work Prozessen. Es schreibt die Statements in Dateien auf den Applikations-Server. Je Dialog Work Prozess wird eine Datei verwendet. [16]
Ab der Basis Version 8.0 wird der SQL-Audit nicht mehr zur Verfügung stehen. Weiterhin warnt SAP davor, dass dieses Log Auswirkungen auf die SAP-Performance haben kann und sehr große Datenmengen anfallen. [17]
Die Logdaten werden unter /usr/sap/<SID>/<INSTANCE>/log/SQL_++++++++.AUD gespeichert und haben im Standard eine maximale Größe von 645MB.
Das SQL-Audit-Log ist standardmäßig deaktiviert und kann mit dem Parameter rsau/SQL-Audit/switch = on aktiviert werden. Der Speicherort kann mit rsau/SQL-Audit/logdir = D:\SQL-Audit ebenso frei gewählt werden wie mit rsau/SQL-Audit/filename = SQL_++++++++.AUD der Dateiname. Die Loggröße kann mit rsau/SQL-Audit/filesize = 100m gesetzt werden. Wird die maximale Dateigröße erreicht, wird in einer neuen Datei weiter protokolliert.

Quellen

[1] SAP Dokumentation Security-Audit-Log
http://help.sap.com/saphelp_nw73ehp1/helpdata/de/4d/41bec4aa601c86e10000000a42189b/content.htm

[2] SAP Dokumentation Systemlog
http://help.sap.com/saphelp_nwes73/helpdata/de/4b/615c237dd33cbae10000000a42189c/content.htm

[3] SAP Dokumentation SAP-Gateway-Logging einrichten
http://help.sap.com/saphelp_nw74/helpdata/de/48/b2a710ca1c3079e10000000a42189b/content.htm?frameset=/de/48/b2096e7895307be10000000a42189b/frameset.htm&current_toc=/de/1d/bc8ac3c2604d678840c421c591a0a8/plain.htm&node_id=5

[4] SAP Dokumentation Konfigurationsparameter
http://help.sap.com/saphelp_nw74/helpdata/de/48/b0e64ba49c2883e10000000a42189c/frameset.htm

[5] SAP Dokumentation SAP Web Dispatcher
http://help.sap.de/saphelp_nw73ehp1/helpdata/de/48/8fe37933114e6fe10000000a421937/content.htm

[6] SAP Dokumentation Internet Communication Manager (ICM)
https://help.sap.com/saphelp_nwpi71/helpdata/de/12/3c21366f62450b92bce1e2e4773f43/frameset.htm

[7] SAP Dokumentation icm/security_log
http://help.sap.de/saphelp_nw74/helpdata/de/48/3d14a6b08c72d1e10000000a42189c/content.htm?current_toc=%2Fde%2F62%2Fd678c5330a4992bc6fe927e6137c9d%2Fplain.htm&frameset=%2Fde%2F48%2F3d9f2504bb58d5e10000000a421937%2Fframeset.htm&node_id=130

[8] SAP Dokumentation Logging im ICM
http://help.sap.com/saphelp_nw70/helpdata/de/73/b5f99a019f11d5991400508b6b8b11/content.htm

[9] SAP Dokumentation Protokollierung von Tabellenänderungen einschalten/ausschalten
http://help.sap.de/saphelp_crm700_ehp02/helpdata/de/4d/b6d15036311dcee10000000a42189c/content.htm

[10] SAP Dokumentation Protokollieren von Änderungen der Benutzer- und Berechtigungsdaten
http://help.sap.com/saphelp_dm40/helpdata/de/c7/69bcd8f36611d3a6510000e835363f/content.htm?frameset=/de/c7/69bccff36611d3a6510000e835363f/frameset.htm&current_toc=/de/8e/a8b5386f64b555e10000009b38f8cf/plain.htm&node_id=14

[11] SAP Dokumentation Protokollieren mit Änderungsbelegen
http://help.sap.com/saphelp_dm40/helpdata/de/c7/69bccff36611d3a6510000e835363f/content.htm?frameset=/de/c7/69bcd2f36611d3a6510000e835363f/frameset.htm&current_toc=/de/8e/a8b5386f64b555e10000009b38f8cf/plain.htm&node_id=11

[12] SAP Dokumentation Systemtrace
http://help.sap.com/saphelp_nw73/helpdata/de/47/cc212e3fa5296fe10000000a42189b/frameset.htm

[13] SAP Dokumentation Entwickler-Traces
http://help.sap.com/saphelp_nw70ehp2/helpdata/de/47/ceaf2883423c85e10000000a42189c/content.htm?current_toc=%2Fde%2Fba%2F104e0763ce4615a384c98f05c33385%2Fplain.htm&frameset=%2Fde%2F47%2Fceab9b83423c85e10000000a42189c%2Fframeset.htm&node_id=41

[14] SAP Dokumentation Trace-Logging
http://help.sap.com/saphelp_nw70ehp2/helpdata/de/47/cfdbfcc3ad2972e10000000a42189b/content.htm?frameset=/de/47/cea164f8862970e10000000a42189b/frameset.htm&current_toc=/de/ba/104e0763ce4615a384c98f05c33385/plain.htm&node_id=46&show_children=false

[15] SAP Dokumentation rdisp/TRACE*-Parameter
http://help.sap.com/saphelp_nw70ehp2/helpdata/de/47/cea164f8862970e10000000a42189b/content.htm?frameset=/de/47/cfdbfcc3ad2972e10000000a42189b/frameset.htm&current_toc=/de/ba/104e0763ce4615a384c98f05c33385/plain.htm&node_id=48

[16] SAP Dokumentation SQL Audit
http://help.sap.com/saphelp_46c/helpdata/en/36/b80e890ac039c2e10000009b38f984/content.htm

[17] SAP Note 115224
http://service.sap.com/sap/support/notes/115224

[18] SAP Dokumentation Message-Server-Parameter
http://help.sap.com/saphelp_nw70/helpdata/de/c3/eff4e4e84811d3acee0000e83539c3/frameset.htm

[19] SAP Dokumentation Log Configuration
http://help.sap.de/saphelp_nw70ehp1/helpdata/de/e2/f410409f088f5ce10000000a155106/frameset.htm

[20] SAP Dokumentation Protokolldateien überwachen und anzeigen
http://help.sap.de/saphelp_nw70ehp1/helpdata/de/48/bb6edff5fe307be10000000a42189b/content.htm?frameset=/de/48/bc10cca70a0611e10000000a42189b/frameset.htm&current_toc=/de/ec/9e1802dd600947abafd2248518697f/plain.htm&node_id=100

[21] SAP Dokumentation Viewing Logs with the SAP Management Console
http://www.hcc.in.tum.de/saphelp/nw731/PLAINHTM/DE/48/6b79c178dc4f93e10000000a42189d/frameset.htm

[22] SAP Dokumentation Logging Additional Information
http://www.hcc.in.tum.de/saphelp/nw731/PLAINHTM/DE/4a/96995945995ff3e10000000a421937/frameset.htm

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 das 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.

http://www.werth-it.de