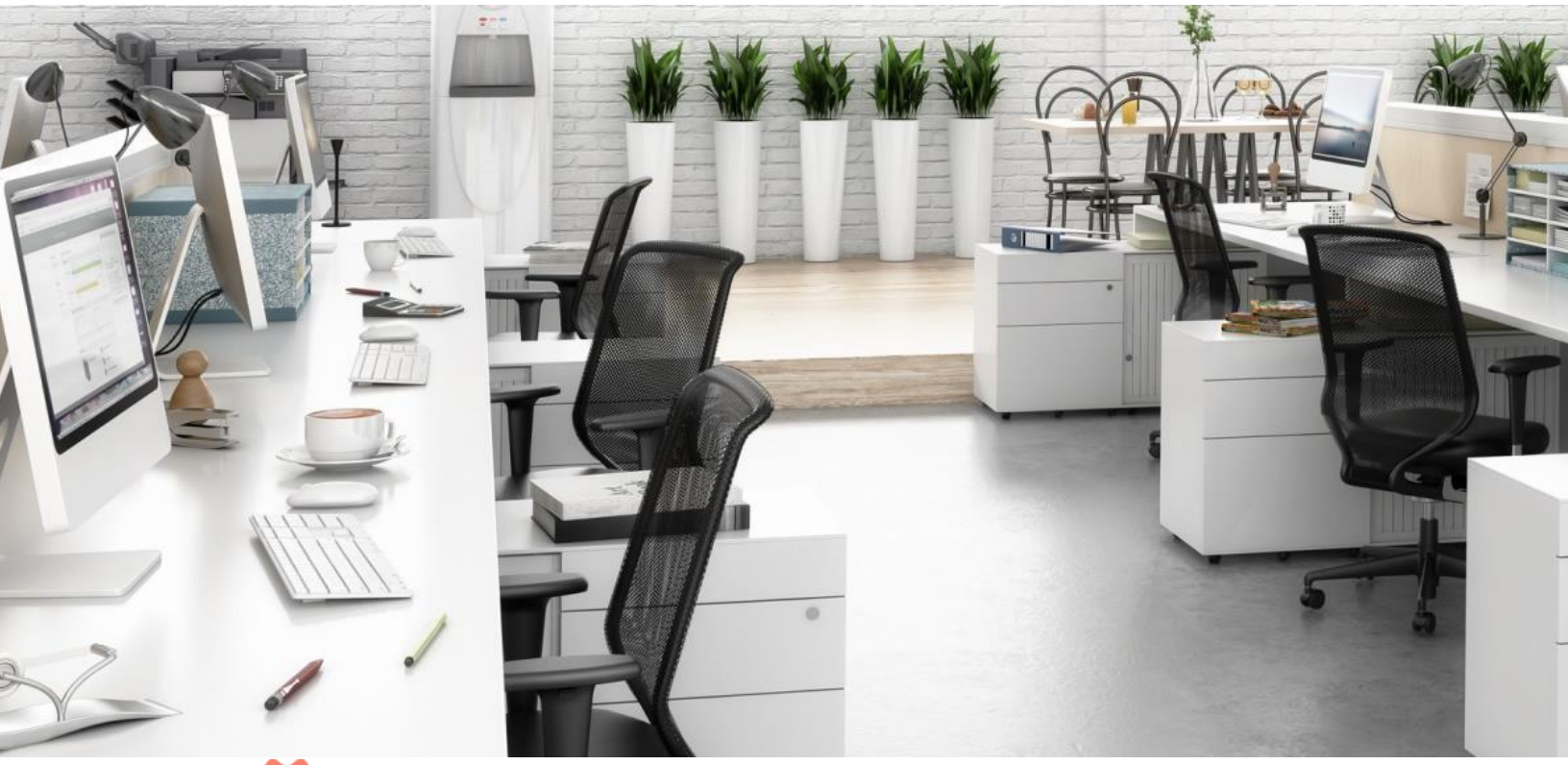


# Wissen Sie wie sich Hacker in SAP-Systeme schleichen?

## Gefahr erkannt? Gefahr gebannt!

Autor: Thomas Werth

Version: 1.0

# Inhaltsverzeichnis

# Über den Autor

Thomas Werth beschäftigt sich seit 2001 in verschiedenen Positionen mit der Sicherheitsanalyse von IT-Systemen. Seit 2011 nimmt dabei die Sicherheit von SAP-Systemen einen wesentlichen Teil seiner Aufmerksamkeit ein. Als Security-Experte hat Thomas Werth verschiedene Fachbücher, -artikel und BSI-Whitepaper insbesondere zu dem Thema SAP-Sicherheit veröffentlicht.

Mit seinen umfassenden Kenntnissen in der IT- und SAP-Security sowie der Software-Entwicklung hat Thomas Werth 2013 die Werth IT GmbH gegründet und mit seinem Experten-Team einen prämierten SAP-Security Scanner entwickelt, der vollständig das Prüfspektrum für SAP-Systeme abdeckt.

Als Vorreiter in der IT-Sicherheit von SAP Systemen ist es das Ziel der Werth IT, dass digitale Unternehmensdaten genau dortbleiben sollen, wo sie hingehören – nämlich im Unternehmen.

Thomas Werth
Geschäftsführer werth IT GmbH

# Einleitung

Ziel dieses Dokumentes ist es Transparenz in potentielle Angriffswege auf Applikationsserver und deren Komponenten zu schaffen. Dazu werden hier die typischen Risiken der einzelnen Komponenten angesprochen und passende Schutzmaßnahmen aufgeführt. Der Kernaspekt ist dabei SAP Netweaver. Im Folgenden wird ein Überblick über mögliche Angriffsszenarien und Handlungsempfehlungen geboten.

# SAP Netweaver

SAP Netweaver bildet das Basisgerüst für SAP-Systeme mit ABAP oder JAVA Stack. Bei der Prüfung eines Systems auf Schwachstellen stellt dies den ersten Berührungspunkt aus dem Netzwerk dar.

## Netzwerksicherheit

Bei der Netzwerksicherheit sind zwei Punkte von besonderer Bedeutung. Zuerst ist die Zugriffskontrolle zu betrachten. Dann folgt die Verschlüsselung der Kommunikation.
SAP beinhaltet diverse Dienste, die größtenteils aus dem Netzwerk heraus erreichbar sind. Es ist wichtig die verfügbaren Dienste zu kennen, daher zeigt der folgende Screenshot einige wichtige Dienste.

# TCP/IP Ports of All SAP Products

Use this information for planning and configuring your network infrastructure according to SAP requirements. You can also use this information to identify specific SAP network traffic for monitoring, prioritization, or security purposes.

Show/hide columns  Show 10 entries.  Previous 1 2 3 4 5 ... 19 Next  Search: Search the entire table

| Product Name | Port Name | Service in etc/services | Default | Range | Rule | External | Fixed | Comments (Explanation of Table Headings) |
|---|---|---|---|---|---|---|---|---|
| Filter | | | | Search in range | | | | |
| Application Server ABAP | SAP Dispatcher | sapdp<NN> | 3200 | 3200-3299 | 32<NN> | Yes | Yes | Used by SAP GUI for Windows and Java. |
| Application Server ABAP | Gateway | sapgw<NN> | 3300 | 3300-3399 | 33<NN> | Yes | Yes | Used for CPIC and RFC communication. |
| Application Server ABAP | Gateway secured | sapgw<NN>s | 4800 | 4800-4899 | 48<NN> | Yes | Yes | SNC secured for CPIC and RFC communication. i Note There is no related sapdp<NN>s(47<NN>) port for the SAP Dispatcher. |
| Application Server ABAP | ICM HTTP | None | 8000 | 8000-8099 | 80<NN> | Yes | No | You can configure to port 80 after installation. Not active by default. |
| Application Server ABAP | ICM HTTPS | None | 44300 | 44300-44399 | 443<NN> | Yes | No | Must be configured after installation. Not active by default. |
| Application Server ABAP | ICM SMTP | None | Not active | 25 | None | Yes | No | Must be configured after installation. Only one instance per host should offer SMTP services. |
| Application Server ABAP | HTTP | sapctrl<NN> | 50013 | 50013-59913 | 5<NN>13 | Yes | Yes | On the SAP Central Services (SCS and ASCS) instance the default instance is 01 making the default port 50113. |
| Application Server ABAP | HTTPS | sapctrls<NN> | 50014 | 50014-59914 | 5<NN>14 | Yes | Yes | On the SAP Central Services (SCS and ASCS) instance the default instance is 01 making the default port 50114. |

*SAP Portliste, Quelle: https://help.sap.com/viewer/ports*

Um Remote zu erkennen, welche Dienste konkret von einem SAP-System in Netzwerk angeboten werden, ist ein Netzwerkscan des Systems der erste Schritt. Ein Beispiel eines NMap-Scans kann wie folgt ausfallen:

```
PORT STATE SERVICE VERSION
21/tcp open ftp?
22/tcp open ssh SSH (SSH-2.0-WeOnlyDo 2.1.3)
445/tcp open microsoft-ds?
3200/tcp open sapdisp SAP ABAP Dispatcher release 7010, patch level 111,
database release 701 (DB name T11)
3300/tcp open sapgateway SAP Gateway (Monitoring mode disabled)
3389/tcp open ms-wbt-server Microsoft Terminal Service
3600/tcp open sapms SAP Message Server (SID T11, ID 00)
3900/tcp open sapms SAP Message Server (SID T11, ID 00)
7210/tcp open maxdb SAP MaxDB 7.7.07
8000/tcp open sapicm SAP Internet Communication Manager
8100/tcp open sapmshttp SAP Message Server httpd release 701 (SID T11)
```

```
40080/tcp open sapigs SAP Internet Graphics Server
50013/tcp open sapstartservice SAP Management Console (SID T11, NR 00)
```

Hier sieht man neben typischen SAP Diensten, der SID und Instanznummer auch noch weitere kritische Dienste wie SSH, MSRDP, SMB und FTP.

## Technische Risiken und unsicherer Betrieb

Wenn die Zugriffskontrolle nicht korrekt greift und einige dieser Dienste in unsicheren Netzwerken oder dem Internet angeboten werden, können Angreifer verschiedene Schwachstellen ausnutzen.
Zunächst existieren Sicherheitslücken in einigen Diensten. Als Beispiel sei hier die Schwachstelle CVE-2012-2611 in dem SAP Dispatcher genannt. Dies ist der Dienst der die Verbindungen der SAP-GUI-Klienten entgegennimmt und diesen Zugriff auf das SAP-System gewährt. Diese Schwachstelle erlaubt die Ausführung von beliebigem Code auf dem SAP-System. Ein Angreifer kann über diesen Weg demnach problemlos eine Backdoor oder einen Trojaner in das System einschleusen.
Ein entsprechender Exploit für diese Schwachstelle ist kostenlos und frei verfügbar im Internet erhältlich.

```
       Name: SAP NetWeaver Dispatcher DiagTraceR3Info Buffer Overflow
     Module: exploit/windows/misc/sap_netweaver_dispatcher
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-05-08

Provided by:
  Martin Gallo
  juan vazquez <juan.vazquez@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   SAP Netweaver 7.0 EHP2 SP6 / Windows XP SP3
  1   SAP Netweaver 7.0 EHP2 SP6 / Windows 2003 SP2

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  3200             yes       The target port (TCP)

Payload information:
  Space: 4000
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the SAP NetWeaver
  Dispatcher service. The overflow occurs in the DiagTraceR3Info()
  function and allows a remote attacker to execute arbitrary code by
  supplying a special crafted Diag packet. The Dispatcher service is
  only vulnerable if the Developer Traces have been configured at
  levels 2 or 3. The module has been successfully tested on SAP
  Netweaver 7.0 EHP2 SP6 over Windows XP SP3 and Windows 2003 SP2 (DEP
  bypass).
```

*Angriffsmodul für CVE-2012-2611*

Doch auch abgesehen von technischen Schwachstellen, existieren weitere zu beachtende Risiken. In den Grundeinstellungen kommunizieren nicht alle Dienste sofort sicher mit den Gegenstellen.
An einigen bekannten Diensten lässt sich dies veranschaulichen. Diese besitzen im Standard weder eine funktionierende Verschlüsselung der übertragenen Zugangsdaten (Passwörter) noch eine sichere Verschlüsselung der übertragenen Daten. Die folgende Tabelle listet die Dienste und zeigt welche Betriebseinstellungen standardmäßig aktiv sind.

In der letzten Spalte ist zu sehen mit welcher Einstellung eine Absicherung des Dienstes möglich ist.

| Dienst | Port | Protokoll | PWD Enc | Daten Enc | Schutz |
|---|---|---|---|---|---|
| SAPGUI | 32NN | DIAG | Kompression (Kann dekomprimiert werden) | Kompression (Kann dekomprimiert werden) | SNC |
| WebGUI | 80NN | HTTP | Base64 | Keine | SSL |
| RFC | 33NN | RFC | XOR | Keine | SNC |
| sapstartservice | 5NN13 | HTTP | Base64 | Keine | SSL |

## Schutzmaßnahmen

SAP bietet diverse Dienste im Netzwerk an, um mit anderen Systemen kommunizieren zu können. Einen Scan der tatsächlich aus dem Netzwerk erreichbaren Dienste, ist wesentlich zur Prüfung der Wirksamkeit der Zugriffsfilterung und zeigt die verbleibende Angriffsfläche. Hier können Dienste technische Schwachstellen enthalten oder mit unsicherer Konfiguration betrieben werden.
Die Erkennung von Schwachstellen in den Diensten und das Einspielen von Patchen ist zur Absicherung des SAP-Systems von enormer Bedeutung. Weiterhin ist die Konfiguration für einen sicheren Betrieb anzupassen. Letztlich gilt es auch den Netzwerkzugriff der angebotenen Dienste zu reglementieren. Daher dürfen nur die in den jeweiligen Netzwerksegmenten benötigten Dienste im Netzwerk verfügbar sein.

# SAP Datenbanksicherheit

Die Datenbank beinhaltet alle geschäftskritischen Daten, die in einem SAP-System verarbeitet werden. Im Rahmen eines Cyberangriffs kann es für den Angreifer leichter sein direkt die Datenbank anzugreifen statt den Weg über das SAP-System an die Daten zu suchen.

## Datenbanksicherheit bei SAP-Systemen

Obwohl HANA immer stärkere Verbreitung findet, ist weiterhin Oracle die meist genutzte SAP-Datenbank. Entsprechend liegt hier der Fokus auf Oracle Datenbanken. Informationen zu HANA finden sich in "SAP-HANA Sicherheitsübersicht".

### Kritische Daten

Zunächst ist zu verstehen, welche aus Sicht der Systemsicherheit kritischen Daten in der Datenbank eines SAP-Systems liegen?
Für einen Angreifer sind solche Daten von Interesse, die ihm helfen in das System einzudringen.
Generell liegen die SAP bezogenen Daten oftmals in einem Datenbankschema mit dem Namen SAPR3 oder SAP<SID>.
Für einen Angreifer besonders interessant sind folgende Tabellen:
Zuerst ist die Tabelle USR02 zu nennen. Hier sind alle Benutzer des Systems inklusive Passworthashes zu finden. Passwortcracker wie John oder Hashcat können diese Hashes in Klartextpasswörter überführen.

| | | | |
|---|---|---|---|
| Tabelle | USR02 | Anmeldedaten (kernelseitige Verwendung !!!) | |
| Texttabelle | | Ohne Texte | |
| Anzeigevariante | | | |
| Maximale Trefferzahl | 500 | Einträge pflegen | |

Selektionskriterien

| Feldname | O. | Von-Wert | Bis-Wert | Mehr | Ausgabe | Technischer Name |
|---|---|---|---|---|---|---|
| Mandant | | | | | | MANDT |
| Benutzer | | | | | ☑ | BNAME |
| Initialkennwort | | | | | ☑ | BCODE |
| Gültig von | | | | | ☑ | GLTGV |
| Gültig bis | | | | | ☑ | GLTGB |
| Benutzertyp | | | | | ☑ | USTYP |
| Benutzergruppe | | | | | ☑ | CLASS |
| Falschanmeldungen | | | | | ☑ | LOCNT |
| Benutzersperre | | | | | ☑ | UFLAG |
| Abrechnungsnr. | | | | | ☑ | ACCNT |
| Anleger | | | | | ☑ | ANAME |
| Anlegedatum | | | | | ☑ | ERDAT |
| Letzes Login-Datum | | | | | ☑ | TRDAT |
| Letzte Anmeldezeit | | | | | ☑ | LTIME |
| Initialkennwort | | | | | ☑ | OCOD1 |
| Kennwortänderung | | | | | ☑ | BCDA1 |
| Codeversion | | | | | ☑ | CODV1 |
| Initialkennwort | | | | | ☑ | OCOD2 |
| Kennwortänderung | | | | | ☑ | BCDA2 |
| Codeversion | | | | | ☑ | CODV2 |
| Initialkennwort | | | | | ☑ | OCOD3 |
| Kennwortänderung | | | | | ☑ | BCDA3 |
| Codeversion | | | | | ☑ | CODV3 |
| Initialkennwort | | | | | ☑ | OCOD4 |
| Kennwortänderung | | | | | ☑ | BCDA4 |
| Codeversion | | | | | ☑ | CODV4 |
| Initialkennwort | | | | | ☑ | OCOD5 |
| Kennwortänderung | | | | | ☑ | BCDA5 |
| Codeversion | | | | | ☑ | CODV5 |
| Version des Benutzer | | | | | ☑ | VERSN |
| Codeversion | | | | | ☑ | CODVN |
| Zeitzone | | | | | ☑ | TZONE |
| ZBV-Benutzertemplate | | | | | ☑ | ZBVMASTER |
| Kennwort-Hashwert | | | | | ☑ | PASSCODE |

(Tabelle USR02 – Passworthashes)

Für einen Angreifer sind dabei die Felder BCODE (MD5 basierter Hash, 8 Zeichen, Uppercase), PASSCODE (SHA-1 basierter HASH, 40 Zeichen, Case sensitive) sowie PWDSALTEDHASH (generisches Hash, 40 Zeichen, Case sensitive). Mit der genannten Reihenfolge steigt auch die notwendige Rechenpower, um solche Hashes zu brechen.

Als zweites folgt die Tabelle SSF_PSE_D. Hier sind Sicherheitszertifikate (PSE) gespeichert. Erhält ein Angreifer darauf Zugriff, kann er beispielsweise SSO-Tickets für ein Login verwenden.
Zuletzt sei noch die Tabelle UST04 zu nennen. Hat ein Angreifer schreibenden Zugriff auf die Daten, kann er hier beliebigen Benutzern SAP_ALL zuweisen.

## Angriffe auf die Datenbank

In der Regel lauscht die Oracle Datenbank auf Port 1527 auf eingehende Verbindungen.
Zu den häufigsten Angriffsursachen zählt die Nutzung von Standardzugangsdaten. Dies gilt auch bei Datenbanken.

Für SAP gibt es diesen Standarduser:
Benutzer „SAPR3“ mit dem Passwort „SAP“.

Es gibt aber auch Oracle Standardbenutzer:

| Benutzer | Passwort |
|---|---|
| SYS | CHANGE_ON_INSTALL |
| SYSTEM | MANAGER |
| SCOTT | TIGER |
| DBSNMP | DBSNMP |

Bei Oracle gibt es noch eine zweite Besonderheit. In der Konfiguration kann die REMOTE OS Authentifizierung (REMOTE_OS_AUTHENT) aktiviert werden. Ist diese aktiv, so überlässt Oracle die Authentifizierung des Benutzers dem entfernten Betriebssystem des Klienten. Ein Angreifer kann diesen Umstand ausnutzen, indem er einfach auf seinem System einen Benutzer mit dem Namen <SID>ADM (oder mit einem anderen DB-User) anlegt und mit diesem eine Verbindung zur Datenbank aufbaut. Oracle lässt diesen Benutzer nun ohne Passwort rein, da es die Authentizitätsprüfung des Benutzers dem Betriebssystem des Angreifers überlässt.

## Angriff auf die SAP Zugangsdaten in Oracle

Der zuvor genannte Umstand der Remote Authentication ermöglicht es auch die Zugangsdaten des SAPR3 Benutzers in Erfahrung zu bringen.
Dazu kann man einen Benutzer mit dem Schema OPS$<SID>ADM oder OPS$SR3ADM (je nach Version) auf seinem Klienten anlegen. Dann verbindet man sich mit der Datenbank.

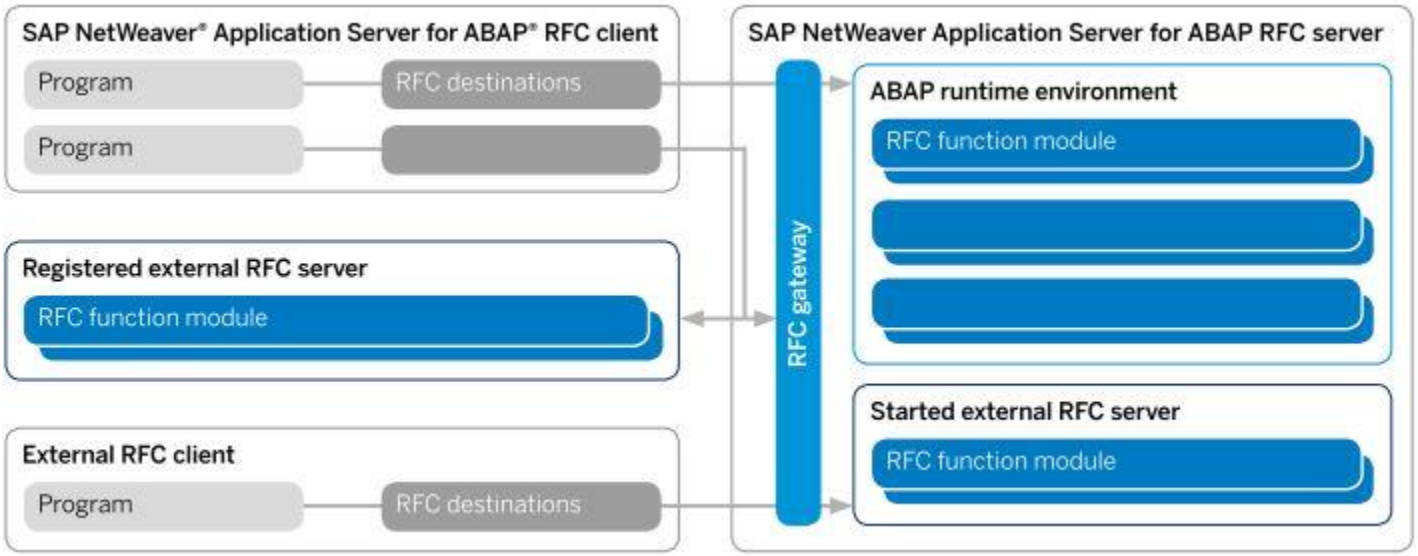
Nun kann man aus der SAPUSER Tabelle die verschlüsselten Passwörter auslesen. Diese sind mit DES und dem Schlüssel „BE_HAPPY“ zu dekodieren. Dann kann mit diesem Passwort und einem der Benutzernamen SAPR3, SAPSR3 oder SAPSR3DB eine Verbindung zur Datenbank aufgebaut werden.
Hier ist es dann möglich die Daten der Tabelle USR02 aus dem Schema SAPR3 oder SAP<SID> auszulesen. Die dort geladenen Hashes lassen sich dann mit Hashcat oder John knacken.

## Schutzmaßnahmen

Zum Schutz vor den genannten Angriffen sind einige Maßnahmen möglich.
Zunächst sollte der Port 1527 nur für das SAP-System erreichbar sein. Der Zugriff auf die Datenbank sollte nur mit Authentifizierung möglich sein und diese ist von der Datenbank selbst vorzunehmen.
In den Passwortrichtlinien sind beschränkende Werte für Fehlanmeldungen (FAILED_LOGIN_ATTEMPTS) zu setzen. Ebenso sollten Passwörter einer gewissen Komplexität entsprechen. Dies ist in der PASSWORD_VERIFY_FUNCTION einzupflegen.
Nur Systeme in der Whitelist dürfen sich mit der Datenbank verbinden (tcp.validnode_checking=true und tcp.invited_nodes= (<ip>,...).
Weiterhin sind Standard-Zugangsdaten abzuändern. Letztlich sollte die Datenbank verschlüsselt kommunizieren und das Auditing in der Datenbank aktiviert sein.

# SAP Gateway

Das SAP Gateway ist eine Schnittstelle des Systems nach außen. Es dient der Kommunikation mit anderen Systemen oder Programmen und regelt jegliche RFC Kommunikation. Das Gateway ist eine Kernkomponente der SAP Netweaver Systeme.




*RFC Kommunikation, Quelle: SAP – Securing Remote Function Calls*

Für einen Angreifer sind folgende Eigenschaften des Gateways von Bedeutung.
Es besitzt Funktionen zur Befehlsausführung mit <SID>adm Rechten im System auf OS-Ebene. Letztlich ist das Gateway ohne Authentifizierung nutzbar.

## Angriff über das SAP Gateway

Bis zum Release Netweaver 7.3 erlauben die Default-Einstellungen jedem Zugriff aus dem Netzwerk auf das SAP Gateway. Seit 7.4 folgt die Default Einstellungen dem „Deny“ Prinzip. Doch wer glaubt damit sind die Systeme sicher, der unterliegt einem Irrglauben. Denn durch eine fehlerhafte Konfiguration der Zugriffsfilter kann sich die Sicherheitslücke wieder öffnen.
Unter dem Begriff 10KBLAZE ist zudem eine Variante bekannt geworden, die unter Ausnutzung eines SAP-Routers oder ungeschützten Messageserver-Port, auch die Default-Deny-Konfiguration aushebeln kann.
Folglich kann ein Angreifer bei aktiver Sicherheitslücke auf das SAP Gateway anonym zugreifen und Systembefehle zur Ausführung bringen. Als Ergebnis kann er dann Beispielweise direkt auf die SAP Datenbank zugreifen und einen SAP_ALL User im System anlegen.
Das folgende Video zeigt diesen Angriff:

https://www.youtube.com/watch?v=aJev7pPtmho

Nachdem der Angreifer auf diesem Weg einen SAP_ALL Zugang zum System etabliert hat, stehen ihm dort alle Türen offen. Zusätzlich hat er über das SAP Gateway Vollzugriff auf das Betriebssystem. Dies führt dazu, dass der Angreifer das Zielsystem komplett unter seine Kontrolle bringen konnte.

## Schutzmaßnahmen SAP Gateway Hardening

Aufgrund der dargestellten Auswirkungen eines Angriffs, ist eine Absicherung des SAP Gateways von hoher Priorität.
Die Absicherung des Gateways setzt im Wesentlichen auf Zugriffskontrollen. Dazu sieht SAP die Dateien reginfo und secinfo vor.
Die reginfo Datei kontrolliert die Registrierung externer RFC-Server an dem Gateway. In der Regel handelt es sich hierbei um RFC fähige Serverprogramme, die ihre Dienste auf diesem Gateway bereitstellen möchten.
Im Gegensatz zur reginfo regelt die secinfo Datei den Zugriff auf die Ausführung von Programmen, die auf diesem Gateway verfügbar sind.
Weiterhin bietet SAP inzwischen auch eine ACL Datei an, die allgemein den Zugriff auf das Gateway regeln kann.
Im Kern sind die Dateien identisch zu pflegen. Man kann zeilenweise Einträge in der Datei nach einer gewissen Syntax vornehmen, die Zugriffe erlaubt oder ablehnt.
Natürlich bietet SAP einen Hinweis an, der die Syntax der Dateien beschreibt.
Dennoch sollte klar sein, dass eine sichere Konfiguration der ACL Dateien immer individuell anhand der SAP-Landschaft und Netzwerkstruktur vorzunehmen ist. Immerhin ist zumindest ab Version 7.4 per Default nur ein interner Zugriff erlaubt.
Dies stellt folgende Konfigurationen sicher:
secinfo:

**P TP=* USER=* USER-HOST=local HOST=local**

**P TP=* USER=* USER-HOST=internal HOST=internal**

reginfo:

**P TP=* HOST=local**

**P TP=* HOST=internal**

## Sicherheitsparameter

Zusätzlich zu den ACL-Dateien stehen noch Sicherheitsparameter zur Konfiguration bereit. Diese sind gw/acl_file, gw/acl_mode, gw/sec_info, gw/reg_info und die SNC Parameter. Hervorzuheben ist hier der Parameter gw/acl_mode, da die anderen „nur“ die Pfade zu den ACL Dateien angeben.
Der Parameter gw/acl_mode definiert das Verhalten des Gateways, falls eine ACL-Datei (gw/sec_info oder gw/reg_info) nicht existiert. Es sind zwei Einstellungen möglich:

- 0: Keine Einschränkung beim Starten von externen Server und bei der Registrierung von Servern.
- 1: Externe und registrierte Server werden nur innerhalb des Systems (Applikationsserver des gleichen Systems) erlaubt. Alle anderen Server werden abgelehnt oder müssen in den jeweiligen Dateien gepflegt werden.

Ein Wert von 1 ist bei produktiven Systemen empfehlenswert.

# Message Server

SAP beschreibt den Message Server wie folgt:

„Der SAP Message-Server läuft als eigener Prozess meist auf demselben Rechner wie die Zentralinstanz. Wenn in dem System eine SCS-Instanz (SAP Central Services) oder ASCS (ABAP SCS) konfiguriert ist, ist der Message-Server Teil dieser Instanz.
In jedem SAP-System läuft genau ein Message-Server. Er nimmt folgende Aufgaben im SAP-System wahr:

- Zentraler Kommunikationskanal zwischen den einzelnen Applikationsserver (Instanzen) des Systems
- Lastverteilung bei Anmeldungen über SAP GUI und RFC mit Logongruppen
- Informationsstelle für den Web Dispatcher und die Applikationsserver (jeder Applikationsserver des Systems meldet sich als Erstes bei dem Message-Server an)

Beim Start einer Instanz kontaktiert der Dispatcher-Prozess den Message-Server, um die von ihm zur Verfügung gestellten Dienste (DIA, BTC, SPO, UPD, etc.) bekannt zu geben. Schlägt der Verbindungsaufbau zum Message-Server fehl, erfolgt ein entsprechender Eintrag in das Systemprotokoll (Syslog).
Fällt der Message-Server aus, muss er so bald als möglich nachgestartet werden, um einen reibungslosen Betrieb des Systems zu gewährleisten.“

Seit der Version 7.0 können zwei getrennte Ports von dem Message Server verwendet werden.
Ein „internal“ Port und ein externer Port. Der interne Port wird für die Kommunikation mit den Applikation-Servern verwendet.
Der externe Port bedient die Anfragen der Clients.
Zur Konfiguration stehen drei Profilparameter bereit

| Parameter | Funktion |
|---|---|
| rdisp/mshost | Konfiguration der Host Adresse |
| rdisp/msserv | Name des Services, muss auf allen Applikations-Servern eines SAP-Systems identisch sein. |
| rdisp/msserv_internal | Konfiguration des internen Ports (bei einem Wert von 0, wird der externe Port für beide Kommunikationen verwendet) |

## Cyberangriff „fake“ Applikationsserver

Erfolgt keine Trennung der Kommunikation nicht, kann ein Client –im Standard sogar ohne Authentifizierung- sich als fake Applikationsserver am Message Server anmelden und die Kommunikation anderer Clients belauschen und Daten einsehen.

Um zu verhindern, dass sich Clients beim Message-Server als Applikations-Server ausgeben, ist der Parameter rdisp/msserv_internal auf einen Wert zwischen 1024 und 65535 zu setzen.
Damit wird für die interne Kommunikation ein anderer Port als für die externe verwendet. Und somit strikt zwischen Clients und Applikationsservern getrennt.

## Schutzmaßnahme Zugriffskontrolle

Über den Parameter ms/acl_info lässt sich eine Datei mit Zugriffsberechtigungen für den Message-Server spezifizieren. Damit kann gesteuert werden von wo sich Applikationsserver am Message-Server anmelden können. Die Datei wirkt sich nicht auf externe Clients aus.

Die Einträge müssen diese Syntax aufweisen:
HOST=[* | ip-adr | hostname | Subnetz-Maske | Domäne ] [, . . .]

Die Datei legen Sie auf Betriebssystemebene an. Im Message-Server-Monitor (SMMS) können Sie dann die Datei anzeigen und nachladen. Wählen Sie dazu Anfang des Navigationspfads Springen -> Sicherheitseinstellungen -> Zugriffskontrolle.
Beispiele
HOST = sapapp1, sappapp2 bedeutet: nur Anmeldungen von den Rechnern sapapp1 und sapapp2 sind erlaubt.

HOST = *.sap.com bedeutet: alle Rechner aus der Domäne sap.com sind erlaubt.

HOST = 157.23.45.56, 157.23.45.57 bedeutet: nur Rechner mit diesen IP-Adressen sind erlaubt.

HOST = 157.23.45.* bedeutet: alle Rechner aus diesem Subnetz sind erlaubt.

## Cyberangriff remote Message-server Monitoring

Das Monitoring erlaubt den Zugriff auf Informationen zum Message-Server. Dazu zählen seine Konfiguration, Traces und Statistiken.
Im Standard dürfen nur Applikationsserver internen Speicher des Message-Servers ändern.

Diese Einstellung wird über den Profilparameter ms/monitor gepflegt. Besitzt dieser den Wert 1, dürfen auch externe Programme wie msmon diese Änderungen vornehmen.
Über den Parameter ms/admin_port wird dazu ein Port angegeben, auf den sich die Klienten zur Administration verbinden können.
Steht also ms/monitor auf 1 und ms/admin_port > 0, dann kann jeder ohne Anmeldung mit dem msmon Werkzeug den Message-Server über diesen Weg administrieren.

## Schutzmaßnahmen Monitoring

Deaktivieren Sie den administrativen Zugriff durch Clients (ms/monitor = 0).
Setzen Sie eine ACL Datei zur Zugriffskontrolle für Applikationsserver (ms/acl_info).
Setzen Sie ms/admin_port auf 0.

## Cyberangriffe Message-Server http

Dieser Dienst (Port 81NN) bietet über das http Protokoll verschiedene Informationen an. So kann ein Angreifer man anonym Informationen über den Applikationsserver auslesen:

| Name | Hostname | Service | IP adress | Port | Types |
|---|---|---|---|---|---|
| [redacted] | SAP[redacted] | sap[redacted] | 1[redacted] | 3200 | DIA UPD ENQ BTC SPO UP2 ICM |

Damit sieht er neben der Instanznummer und der SID auch welche SAP-Prozesse und –Dienste auf dem System verfügbar sind.

Zudem kann ein Angreifer anonym Profilparameter auslesen und damit wesentliche Sicherheitseinstellungen des Systems in Erfahrung bringen:

```
rsau/enable = 1
rec/client = 100,200
login/password_compliance_to_current_policy = 0
login/min_password_digits = 0
login/min_password_lng = 6
login/min_password_letters = 0
login/min_password_lowercase = 0
login/min_password_specials = 0
login/min_password_uppercase = 0
snc/enable = 0
snc/accept_insecure_gui = 0
snc/accept_insecure_rfc = 0
rdisp/gui_auto_logout = 0
login/failed_user_auto_unlock = 0
login/password_max_idle_initial = 0
login/fails_to_user_lock = 5
login/disable_multi_gui_login = 1
```

Ein wirksamer Schutz ist die Deaktivierung und Zugriffsfilterung mittels Firewall für diesen Dienst, da er in der Regel nicht benötigt wird.

# SAP MMC

Die SAP Management Console ist über den Port 5NN13 erreichbar. Sie erlaubt die Remote Verwaltung des SAP Servers. Dabei verwendet Sie die SOAP Schnittstelle zur Kommunikation. In der Standardinstallation ist kein SSL eingerichtet und die Zugangsdaten werden mit dem Basic Authentication Verfahren (base64 Encoding) übertragen.

## Angriffsfläche

Ein Mitlesen dieser Datenübertragung ermöglicht es vollen Zugriff auf das SAP-System zu erhalten, da die übertragenen Zugangsdaten nur encodiert und nicht verschlüsselt sind. Eine Decodierung ist im Handumdrehen durchgeführt und ein Angreifer besitzt die administrativen Zugangsdaten zum System.

Verschiedene anonym aufrufbare SOAP Funktionen erlauben Denial of Service Angriffe oder den Zugriff auf Informationen.
Eine Liste aller Funktionen erhält man über die WSDL Datei des SAP MMC:
http://<host>:5NN13/SAPControl/?wsdl

Beispielsweise erlaubt eine dieser Funktionen ein Auslesen von Benutzernamen:

**Ausgabe**


Authentifiziert lassen sich sogar Betriebssystembefehle über die Funktion OSExecute ausführen.
Ebenso sind weitere kritische Angriffe möglich. Log und Trace Dateien können über diese Schnittstelle eingesehen werden. Ist das Trace aktiv, dann werden in der userinterface.log Datei auch JSESSIONIDs gespeichert. Kann ein Angreifer diese Auslesen, so ist damit anschließend ein Login am SAP-System möglich.

## Schutzmaßnahmen

Der Dienst ist mit Authentisierung und Härtung der Konfiguration zu schützen. Dazu sind verschiedene SAP Notes relevant.

- Setzen Sie die Empfehlungen der SAP Note 927637 - Webservice Authentisierung in sapstartsrv ab Release 7.00 um.
- Spielen Sie die SAP Note 1439348 - Erweiterte Sicherheitseinstellungen für sapstartsrv ein, um unautorisierte Zugriffe zu unterbinden.
- Stellen Sie sicher, dass kein Denial of Service möglich ist und beachten dazu die SAP Note 1469804 - Möglicher Denial of Service in sapstartsrv.

Im Rahmen der Konfigurationshärtung sind die folgenden Parameter zu setzen.
Zur Vermeidung von Zugriffen auf die JSESSIONID, sollte keine TRACE!= 3 sein. Trace Files mit diesen Einstellungen sollten sofort gelöscht werden.
Schützen Sie kritische Funktionen über den Parameter
service/ protectedwebmethods = SDEFAULT .

Aktivieren Sie eine Zugriffskontrolle mittels ACL Dateien über die Parameter:
service/http/acl_file
service/https/acl_file .

# Host Agent

SAP Host Control ist sehr ähnlich wie die Management Console aufgebaut. Der SAP-Host-Agent bietet die folgenden Funktionen:

- SAP-Instanz-Such-Services und Bestand
- SAP-Instanzsteuerung
- Datenbanküberwachung und -verwaltung
- System oder Instanz Bereitstellung:
    - Hosting der Infrastructure des SAP NetWeaver Landscape Virtualization Management (LVM), das vorher unter dem Namen SAP NetWeaver Adaptive Computing Controller (ACC) bekannt war
    - Hosting der Software-Lebenszyklus(SL)-Werkzeugschnittstellen
- Betriebssystemüberwachung:
    - Unter Verwendung von saposcol
    - Unter Verwendung von Common Information Model (CIM)-basierten Infrastrukturen
- IBM i-spezifische Funktionen:
    - Dynamisch angepasste Berechtigung für SAP-Kernel 7.20 und höher
    - SAP ILE daemon (SAPILED)
    - SAP-Datenbank-Performance-Kollektor für IBM i

Die verfügbaren Funktionen sind über diese WSDL einzusehen:

- SAP Host Control URL: http://<server name>:1128/SAPHostControl/?wsdl
- SAPOSCOL URL: http://<server name>:1128/SAPOscol/?wsdl

Die Grundkonfiguration in aktuellen Releases erfordert eine Authentifizierung für den Zugriff auf diese Schnittstelle und entsprechend wenig Raum besteht für anonyme Cyberangriffe.

In älteren Versionen existiert jedoch eine kritische Schwachstelle zur Einschleusung von Befehlen.

### Schutzmaßnahmen

Die Sicherheitslücke ist mit der SAP Note 1341333 - Mögl. Informationspreisgabe und Code-Ausführung in sapdbctrl zu schließen.
Zusätzlich sollte eine ACL Datei für den Zugriffsschutz eingerichtet werden. Diese wird im „host_profile“ des HOST Agend über diese Parameter angegeben:
service/http/acl_file = <Path_to_an_ACL_file> or service/https/acl_file = <Path_to_an_ACL_file> if you use HTTPS.
Damit kann der Zugriff auf den Dienst auch bei Bekanntwerden von Zugangsdaten erschwert werden.

## SAP NetWeaver Application Server ABAP

Mit diesem Beitrag startet die Serie „Howto SAP Security“. In der Serie werden typische SAP Angriffsflächen vorgestellt – mitsamt Angriffsvektoren und Gegenmaßnahmen. Zu Beginn der Serie wird daher mit dem SAP Gateway das wahrscheinlich größte Angriffsziel betrachtet.
Der Application-Server stellt eine Runtime-Umgebung und Middleware für die entsprechende Programmierumgebung ABAP dar, die unter anderem die Zugriffe auf die Datenbank und das Betriebssystem übernimmt. So läuft ein ABAP- NetWeaver-Programm unabhängig von der Datenbank oder dem Betriebssystem.
SAP ERP Systeme bieten ihre Funktionalität mithilfe von ABAP-Programmen an. Entsprechend basieren ERP Systeme auf einem ABAP Stack.
Die für einen Angreifer interessanten Dienste sind RFC sowie ICM im Rahmen des ABAP-Stacks. Der Dispatcher (SAP-GUI) wird an dieser Stelle nicht betrachtet, da nur sehr alte Versionen über kritische Schwachstellen verfügen und die weitere Kommunikation einen authentifizierten Benutzer benötigen. Die Sicherheit authentifizierter Benutzer regelt ein

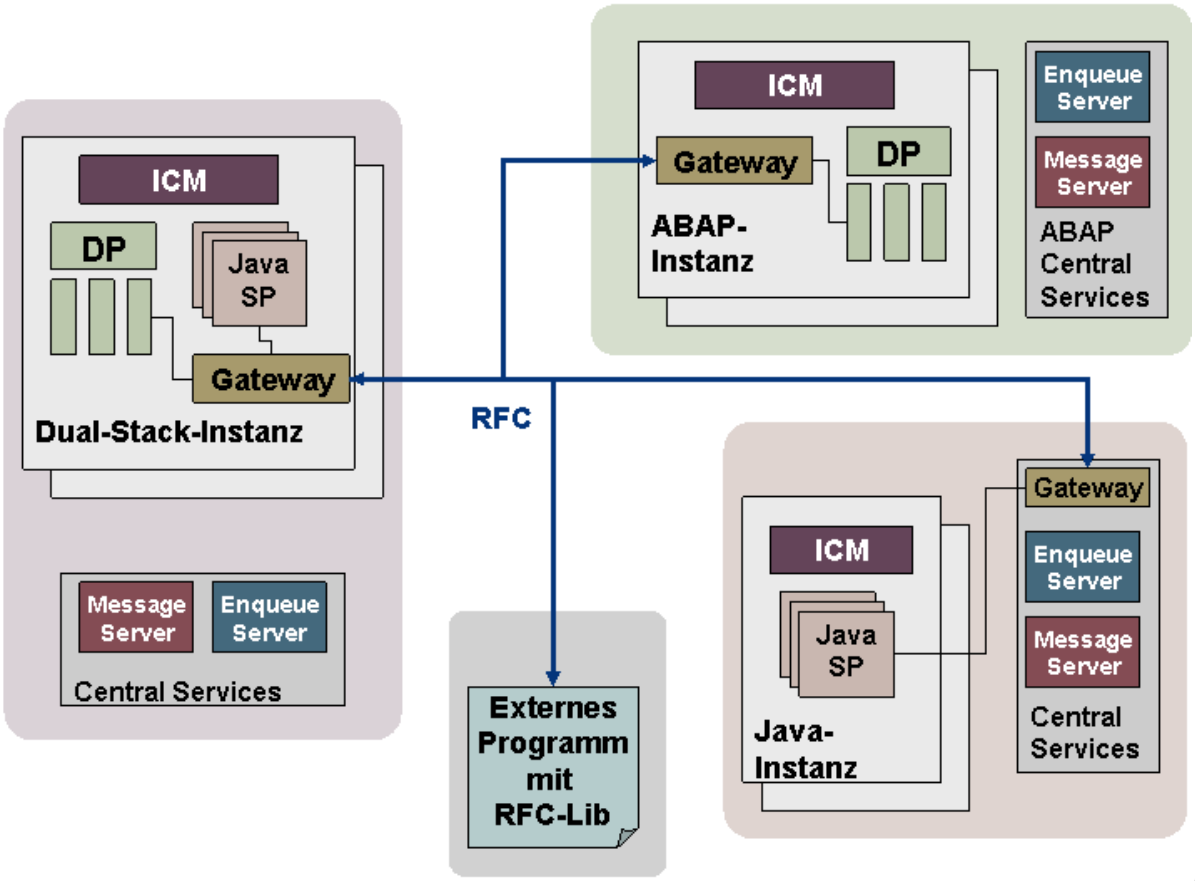
Berechtigungskonzept, welches den Rahmen dieses E-Books sprengen würde. Zwei Tipps in Bezug auf die Sicherheit des SAP-Dispatchers seien dennoch erwähnt:

1. Ändern Sie die Standardzugangsdaten im SAP-System.
2. Spielen Sie regelmäßig die SAP-Security Notes ein, um Problemstellen wie fehlende Berechtigungsprüfungen oder Rechteausweitungen umgehend bei Bekanntwerden zu schließen.

## Die RFC-Schnittstelle

Die Remote Function Calls (RFC) finden breite Anwendung in SAP ABAP Systemen. Ein Benutzer kann ABAP Funktionen, die Remote aufrufbar sind, von anderen Systemen aus aufrufen.
Dazu muss er jedoch die System ID, den Mandanten, sowie die Zugangsdaten des Benutzers kennen.
Es gibt weit über 30.000 RFC Funktionen im ABAP Standard. Diese sind in unterschiedlichen Gruppen gebündelt.
SAP stellt verschiedene Lösungen bereit, um die RFCs aufrufen zu können. Dazu zählen unter anderem das RFC SDK, NW RFC SDK oder JCo. In den Beispielen sind auch Programme enthalten, die direkt verwendet werden können, um RFCs aufzurufen. Beispielsweise startrfc.exe.

SAP-Systeme ermöglichen nicht nur Benutzern RFC für Aufrufe zu verwenden, sondern nutzen diesen Weg auch selbst zur Kommunikation mit anderen Systemen.




*RFC*

*Kommunikation bei SAP-Systemen [(Quelle SAP)]*

## Angriffe mittels anonymen RFC-Aufrufen

Aus Sicherheitsaspekten ist es vorteilhaft, wenn eine Aktion im System immer einem Benutzer zugeordnet werden kann und ebenso ein Benutzer die erforderlichen Berechtigungen für diese Aktion besitzen muss.

Eben dieses Konzept hebeln anonyme RFC Aufrufe aus. Dessen muss man sich bewusst sein, wenn man diese Aufrufe erlaubt.

Typische anonyme Funktionen sind:

- RFC_PING: Einfache Prüfung der Erreichbarkeit
- RFC_SYSTEM_INFO: Informationen zu dem System (OS, Datenbank, Version, Identifier)
- RFC_GET_LOCAL_DESTINATIONS: Zeigt alle momentan aktiven RFC-Destinations.
- RFC_GET_LOCAL_SERVERS: Informationen zu den lokalen Servern
- SYSTEM_INVISIBLE_GUI: Setzt die Sichtbarkeit der aktuellen SAP GUI auf unsichtbar.

Mit diesen Funktionen kann ein Angreifer bereits Informationen über das System sammeln oder die SAP GUI unsichtbar im Hintergrund steuern. Beispielsweise kann er auf diesem

Weg das Betriebssystem und die Datenbank in Erfahrung bringen und diese Informationen nutzen, um einen kritischen Angriff über ein ungesichertes SAP-Gateway auszuführen.

## Risiko Standardzugangsdaten

Standardbenutzer dürfen in der Regel RFC Aufrufe tätigen. Teilweise mit weitreichenden Berechtigungen. Faktisch kann dies zu einem Vollzugriff auf das System über das Einfallstor RFC führen.
Folgende User können hierzu verwendet werden:

| USER | Passwort | Mandanten |
|---|---|---|
| SAP* | „06071992“ oder „PASS“ | 000, 001, Kundenmandanten |
| DDIC | 19920706 | 000,001,066, Kundenmandanten |
| TMSADM | „PASSWORD“ oder „$1Pawd2&“ | 000 |
| SAPCPIC | ADMIN | 000,001 |
| EARLYWATCH | SUPPORT | 066 |

Einige dieser Benutzer sind in der Lage über RFC weitere Benutzer anzulegen und diese mit SAP_ALL auszustatten.

## SMB Relay Angriffe

Bei dieser Art von Angriffen, wird das SAP-System dazu gebracht eine beliebige Datei auf dem System des Angreifers über das Netzwerk anzufragen.
Bei einer solchen Anfrage sendet das SAP-System dann automatisch die Zugangsdaten des <SID>ADM Benutzers an das System des Angreifers. Allerdings in Form eines Hashes. Doch der kann mit Hashcat oder John in Klartext überführt werden.

Es gibt viele RFC Funktionen die für diesen Angriff anfällig sind, dazu zählen auch diese:
EPS_DELETE_FILE
EPS_CLOSE_FILE
CLBA_CLASSIF_FILE_REMOTE_HOST
CLBA_UPDATE_FILE_REMOTE_HOST
EDI_DATA_INCOMMING
RZL_READ_FILE

## Befehlsausführung

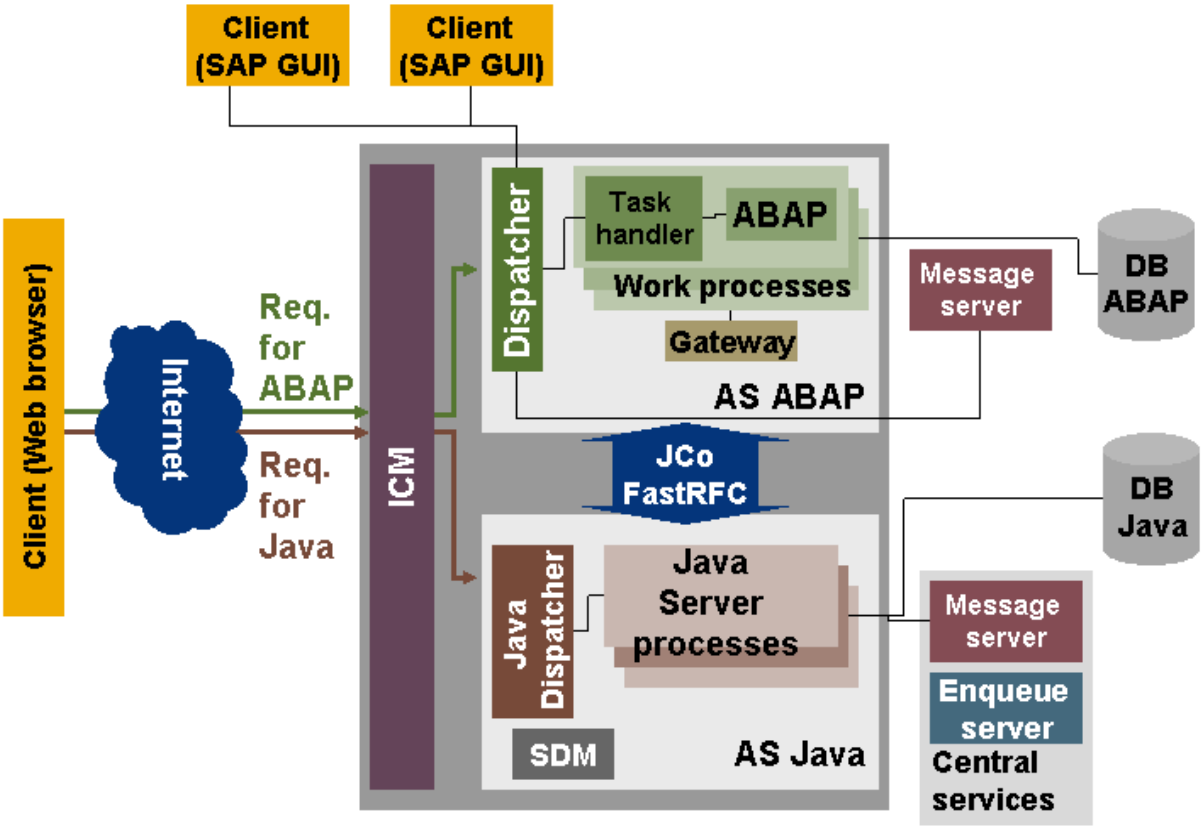
Einige Funktionen wie SXPG_COMMAND_EXECUTE erlauben sogar die Ausführung von Betriebssystembefehlen. Allerdings nur unter Ausnutzung der existierenden Schwachstellen in einigen Kommandos. Dennoch zeigt dies wie schnell ein RFC Aufruf zu der Ausführung eines Befehls auf OS-Ebene als <SID>ADM erfolgen kann.

## Schutzmaßnahmen

Zum Schutz vor den hier genannten Angriffswegen reichen schon wenige Schritte aus. Schränken Sie zunächst die Nutzung von anonymen RFC-Aufrufen über den Parameter auth/rfc_authority_check ein.
Dann ändern Sie Standardzugangsdaten ab.
Zuletzt gilt es RFC Berechtigungen restriktiv zu vergeben. Nur Benutzer die RFC wirklich benötigen dürfen Zugriff erhalten und auch nur in dem notwendigen Umfang. Ein S_RFC * ist zwar einfach, aber ermöglicht auch die hier vorgestellten Angriffe. Besser ist es moderne Schutzmaßnahmen wie SAP UCON zu nutzen.

# Internet Communication Manager (ICM)

Der ICM nimmt Anfragen über das HTTP(s) Protokoll entgegen. Insbesondere Aufrufe aus dem Internet an das SAP-System lassen sich so seit geraumer Zeit realisieren. Diese Aufrufe gibt der ICM je nach Architektur an den JAVA oder ABAP Dispatcher zur Verarbeitung weiter. Dies ist auf dem folgenden Schaubild zu erkennen:




*Architektur SAP ABAP / JAVA mit ICM (Quelle SAP: https://help.sap.com/doc/saphelp_scm70/7.0/ru-RU/48/03b72c49f04aa5e10000000a421937/frameset.htm)*

## ICM Dienste

Der ICM bietet eine Vielzahl an Diensten. Teils wird allein bei den kritischen Diensten von einer Gesamtzahl von ca. 1500 berichtet.

Die meisten ICM-Dienste erfordern eine Authentifizierung und bieten so zumindest einen gewissen Grundschutz. Allerdings ist es wichtig zu wissen, dass jeder registrierte Benutzer im System Zugriff auf diese Dienste erhält. Weiterhin sind im Standard keine weiteren Berechtigungsprüfungen an diese Dienste gebunden. Daher kann jeder Benutzer jeden Dienst ausführen (solange im Code keine weiteren Berechtigungsprüfungen explizit enthalten sind).

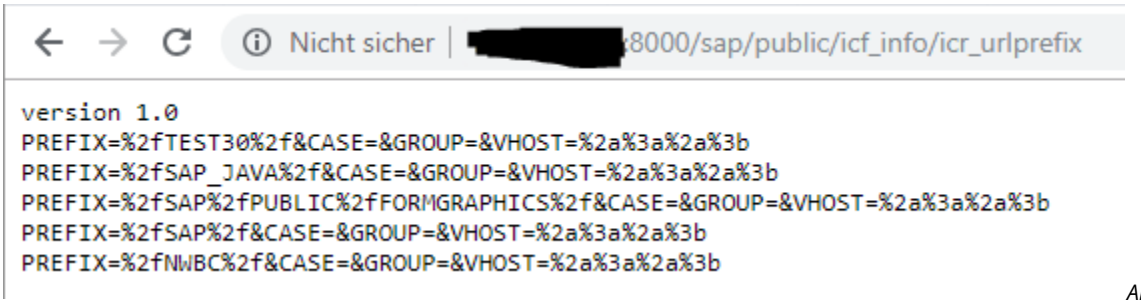
## Angriffsfläche anonyme Dienste

Ca. 40 Dienste lassen sich sogar ganz anonym aufrufen – teils mit nachgeschalteter Authentifizierung. Daher besteht in der Standardkonfiguration die Gefahr von unerwünschten Zugriffen.

Exemplarisch sind hier einige genannt, die bereits eine gewisse Angriffs-Historie besitzen:

| URI | Funktion |
|---|---|
| /sap/bc/gui/sap/its/webui | Anmeldung zur WebGUI [Gefahr Standardbenutzer] |
| /sap/bw/Bex | Erlaubt das Lesen von Infoobjekten |
| /sap/bc/soap/rfc | Ausführung von Remote RFC Bausteinen [Gefahr Standardbenutzer] |
| /sap/public/icf_info/icr_groups | Anzeige der Installierten Komponenten |
| /sap/public/info | Anzeige von Systeminformationen |
| /sap/bc/bsp/sap/htmlb_samples | verwundbare Test Anwendung |
| /sap/bc/srt/xip/sap | Zugriff auf XI Funktionen |

Die Verwendung einer solchen URL zur Informationsgewinnung oder Angriffsausführung ist einfach im Browser zu realisieren:




*Anonymer Aufruf der Services: /sap/public/icf_info/icr_urlprefix*

## Angriffe mittels RFC Funktionsaufruf über den ICM

RFC Funktionsbausteine bilden grob die Möglichkeiten eines Benutzers in der SAP GUI als eine Art technische API für Programme ab. Der Service /sap/bc/soap/rfc erlaubt das Ausführen von RFC Funktionsbausteinen und ist anonym erreichbar. Allerdings benötigen die RFCs zur Ausführung einen gültigen Benutzer, der mindestens die Berechtigung S_RFC für die Gruppe des aufzurufenden RFC Funktionsbausteins besitzt. Ebenso benötigt der Benutzer die Berechtigungen, die innerhalb des RFC Funktionsbausteins abgefragt werden. Jedoch besitzen viele RFC Funktionsbausteine keine zusätzlichen Berechtigungsprüfungen. Erschwerend kommt hinzu, dass einige Standardbenutzer bereits die Berechtigung zur Ausführung von kritischen RFC Funktionen besitzen:

| Benutzer | Passwort | Mandant |
|---|---|---|
| SAP* | '06071992' oder 'PASS' | 000,001,066, Kundenmandanten |
| DDIC | '19920706' | 000, 001, Kundenmandanten |
| TMSADM | 'PASSWORD' oder '$1Pawd2&' | 000 |
| SAPCPIC | 'ADMIN' | 000,001 |
| EARLYWATCH SUPPORT | | 066 |

Mit einem dieser Benutzer könnte ein Angreifer den genannten Dienst nutzen, um kritische RFC Funktionen im System auszuführen. Es müssen jedoch die Standardbenutzer im System vorhanden sein.

## Schutzmaßnahmen

Neuere SAP-Systeme besitzen von Haus aus Sicherheitsoptimierungen und verbesserte Einstellungen. Zusätzlich helfen einige Konfigurationsoptionen den ICM weiter zu härten. Zuerst sei die SAP Note 1329326 erwähnt. Diese enthält eine Anleitung wie man eigene Header für den ICM hinterlegen kann. Damit lässt sich beispielsweise ein Informationsabfluss über Fehlerseiten verhindern.
Ein weiterer Hinweis ist die SAP Note 747818. Auch hier wird die Preisgabe von Versionsinformationen unterbunden.
Weiterhin ist die SAP Note 1498575 zu nennen. Diese beschreibt wie nicht notwendige Dienste zu deaktivieren sind.
Zusätzlich sollten Sie ICF Authorizations für die aktiven Services aktivieren .
Letztlich sind noch die Zugangsdaten der Standardbenutzer zu ändern.

# SAP NetWeaver Application Server Java

Der Java Stack von SAP wird unter anderem bei SAP Portal, PI, XI oder auch im Solution Manager verwendet.
Hierbei kommuniziert der Anwender über seinen Browser mit dem SAP-System. Die J2EE Engine kommuniziert dann über JDBC, RFC oder auch HTTP mit anderen Datenbanken, SAP-Systemen oder Web-Services.

## Standard Ports der SAP J2EE Engine

Die J2EE nutzt folgende Ports und ein Angreifer kann gezielt nach J2EE Diensten suchen:

*J2EE Engine Dispatcher Ports*

| Service Name | Port Number | Default Value | Range (min-max) |
|---|---|---|---|
| HTTP | 5NN00 | 50000 | 50000-59900 |
| HTTP over SSL | 5NN01 | 50001 | 50001-59901 |
| IIOP | 5NN07 | 50007 | 50007-59907 |
| IIOP Initial Context | 5NN02 | 50002 | 50002-59902 |
| IIOP over SSL | 5NN03 | 50003 | 50003-59903 |
| P4 | 5NN04 | 50004 | 50004-59904 |
| P4 over HTTP | 5NN05 | 50005 | 50005-59905 |
| P4 over SSL | 5NN06 | 50006 | 50006-59906 |
| Telnet | 5NN08 | 50008 | 50008-59908 |
| JMS | 5NN10 | 50010 | 50010-59910 |

## J2EE-Dienste

Zu den Standard Diensten gehören der SAP Visual Admin (P4) und der SAP NetWeaver HTTP (Webserver).
Zusätzlich können bei Bedarf noch ein SAP Portal, SAP SDM, SAP SDM Admin, SAP LogViewer oder SAP J2EE Telnet angeboten werden.

## Angriffsziel SecStore

Die zum Betrieb der J2EE Engine erforderlichen Zugangsdaten (wie die Verbindung zur Datenbank) speichert die J2EE Engine unter Verwendung des SAP Java Cryptography Toolkits in einer Datei unter diesem Pfad:
\usr\sap\<SID>\SYS\global\security\data\SecStore.properties

Im Wesentlichen ist dies eine KEY = VALUE Datei, bei der die „Values“ verschlüsselt sind.

Erhält ein Angreifer Zugriff auf die Schlüsseldatei und den SecStore selbst, kann er diese entschlüsseln und die hinterlegten Zugangsdaten auslesen.
Entsprechend ist der Zugriff auf diese Datei auf Betriebssystemebene einzugrenzen (SAP-System und SIDADM). Ebenso sind Schwachstellen, die den Abfluss von Informationen oder den Zugriff auf Dateien erlauben zu schließen. Dies bedeutet konkret, dass Angreifer Schwachstellen in den Web-Anwendungen ausnutzen, um Zugriff auf lokale Dateien zu erhalten. Mit dem Erscheinen einer solchen SAP-Note ist diese umgehend einzuspielen. Ein Beispiel hierzu ist die SAP Note 2486657 - Directory-Traversal Schwachstelle in SAP NetWeaver AS Java Web Container. Diese schließt eine Sicherheitslücke, die in realen Angriffen auf SAP-Systeme verwendet wurde, um unter anderem auch Zugriff auf den SecStore zu erhalten.

## Visual Admin P4

Der Visual Admin ist ein Werkzeug zur Konfiguration und Steuerung der J2EE Engine. Es nutzt ein eigenes proprietäres Protokoll „P4“. Die Datenübertragung erfolgt im Standard im Klartext. Zum Schutz der Vertraulichkeit kann SSL aktiviert werden:
https://help.sap.com/saphelp_nwpi71/helpdata/de/14/ef2940cbf2195de10000000a1550b0/content.htm?no_cache=true .

Dieser Dienst besitzt verschiedene Module mit bekannten Schwachstellen, die den Zugriff auf Informationen oder sogar auf das Dateisystem (SecStore) teilweise anonym erlauben. Entsprechend ist der Dienst aktuell zu halten und es sollte generell der Zugriff auf die P4 Schnittstelle nur von administrativen Arbeitsplätzen zugelassen werden.

## HTTP Webserver

Ein SAP-System mit J2EE Engine ist für den Einsatz als Web-Server konzeptioniert. Daher sind solche Server oftmals einem erweiterten Netzbereich angeschlossen oder aus dem Internet erreichbar.
Entsprechend gibt es bereits spezielle Suchbegriffe für Suchmaschinen, die solche SAP-Systeme aufspüren können:

- inurl:/irj/portal
- inurl:/IciEventService sap
- inurl:/IciEventService/IciEventConf
- inurl:/wsnavigator/jsps/test.jsp
- inurl:/irj/go/km/docs/

In diesen Diensten finden sich verschiedene Schwachstellen:

- Bekanntgabe von Versionsinformationen
- Zugriff auf Logs und Trace Dateien
- Auslesen / Erraten von Benutzernamen
- Missbrauch zum Port-Scanning im angeschlossenen internen Netzwerk

Als ein Beleg für die immer wieder kehrenden Verwundbarkeiten sind CVE-2018-2415 genannt.
Als einzig wirksame Schutzmaßnahme gegen Schwachstellen dieser Art hat sich das Einspielen der jeweils aktuellen SAP Notes als Sinnvoll erwiesen.

## Authentifizierung

Die J2EE Engine unterscheidet zwei Wege zur Authentifizierung von Benutzern.
Bei Servlets übernimmt der Web Container die Authentifizierung. Dies jedoch „nur“ entsprechend den in der Konfigurationsdatei (Web.xml) des Servlets konfigurierten Regeln.
Für alle Komponenten unterhalb der J2EE Engine (Web Dynpro, Portal iViews) übernimmt die UME die Authentifizierung.

### Angriff Invoker Servlet zur Umgehung der Authentifizierung

Servlets lassen sich indirekt auch mittels Invoker Servlet über deren Klassennamen aufrufen. Hierdurch kann ein Angreifer die erforderliche Authentifizierung umgehen und ohne Zugangsdaten Zugriff auf ein Servlet erhalten.
Jedes Servlet besitzt einen Klassennamen unter dem Tag <servlet-class>:
<servlet---class> com.sap.<*categroy*>.<*Name*></servlet---class>
Normalerweise wird ein Applet über die Kombination seiner url-pattern und seines servlet-name aufgerufen. Dort greift dann die Berechtigungsprüfung.
Das Invokerservlet erlaubt jedoch den Aufruf über die Servlet-class in dieser Form:
<application name>/servlet/<servlet-name-or-class>

Ein möglicher Angriff soll an dem kritischen /ctc/ConfigServlet veranschaulicht werden.
Ein typsicher get Aufruf im Browser hat folgende Syntax:
GET /ctc/ConfigServlet?param=xxxxxxx
Um die dortige Prüfung der Authentifizierung zu umgehen, kann ein Aufruf mittels Invoker Servlet erfolgen:
GET /ctc/servlet/com.sap.ctc.util.ConfigServlet?param=xxxxxxxx

Daher sollte das Invoker Servlet global deaktiviert werden über die Einstellung EnableInvokerServletGlobally in dem servlet_jsp Dienst. Weitere Informationen liefert die SAP Note 1445998 - Deaktivieren des Invoker-Servlets.
Bei Betrieb eines SAP Portals zeigt die SAP Note 1467771 - Deaktivieren von Invoker Servlet im Portal welche Details hier zu beachten sind.

Angriff Verb Tampering zur Umgehung der Authentifizierung

Eine zweite Gefahrenquelle ist das so genannte Verb Tampering. Hierbei verändert ein Angreifer einfachen den gewohnten Zugriffsweg. In der Regel nutzen Web-Browser für Ihre Anfragen an Web-Server einen GET oder POST Befehl. Dies sind die mit Abstand verbreitetsten Zugriffswege, um Webseiten von einem Webserver anzufordern. Daher ist es auch nicht verwunderlich, dass im Rahmen der Konfiguration der Authentifizierung bei Servlets eben diese beiden Wege angegeben werden. Allerdings greift die Notwendigkeit der Authentifizierung dann auch nur bei diesen beiden wegen.
Erzwingt ein Angreifer nun einen anderen Weg zur Anfrage eine Webseite – wie einen HEAD Befehl – kann er ganz ohne Authentifizierung die Seite anfordern.
Der Nachteil eines HEAD Requests ist, dass der Server die Anfrage zwar annimmt und verarbeitet, er aber kein Ergebnis (also die Webseite selbst) an den Aufrufer sendet.
Doch findet der Angreifer Seiten, die Befehle ausführen, dann werden diese auch ausgeführt.
Beispielsweise existieren Serverlets, die

- Neue Benutzer anlegen
- Rollen an Benutzer zuweisen
- Systembefehle auf dem Server ausführen
- RFC Destinations anlegen

Damit kann ein Angreifer sich einen Weg in das System erarbeiten. Hierzu sei obiges Beispiel erneut aufgegriffen, um einen Angriff mittels Verb Tampering anhand eines HEAD Zugriffs zu verdeutlichen:
HEAD /ctc/ConfigServlet?param=xxxxxxxxx

Zum Schutz ist hier ein aktuelles Release der SAP-Systeme zu verwenden oder entsprechende SAP Notes einzuspielen:

- 1503579 - NetWeaver PI: Anfälligkeit für Umgehung d. Authentifizierung

Alternativ kann man in allen WEB.XML Dateien die Angabe der <http-method> entfernen, da dann der Zugriffschutz für alle Zugriffsmethoden gilt statt „nur“ für die dort angegebenen.

## SAP Portal

Ein SAP Portal stellt immer einen Web-Zugriffspunkt auf bewusst bereit gestellte Informationen eines Unternehmens dar. Es kann auch als Plattform für die Zusammenarbeit zwischen Unternehmen oder zur Kommunikation mit den Kunden genutzt werden.
In Kombination mit einem Single-Sign-On, kann ein Portal auch „das“ Anmeldesystem für SAP sein.
Angriffsfläche Knowledge Management
Ein Zusatzmodul für ein SAP Portal ist das SAP Knowledge Management. Im Kern ist es wie ein Sharepoint zu sehen. Da Benutzer hier Seiten erstellen können, ist dieses Module gleich doppelt interessant für einen Angreifer:

- Er kann lesenden Zugriff auf kritische Dokumente erhalten
- Er kann Phishing Seiten erstellen, um den Login Cookie (SSO!) zu stehlen.

Das KM Modul ist unter dem Pfad /irj/go/km/navigation aufrufbar.
Beispiele für Ordner mit Dokumenten sind:

- /irj/go/km/navigation/userhome/
- /irj/go/km/navigation/docs/
- /irj/go/km/navigation/documents/Public Documents/
- /irj/go/km/navigation/Entry Points/Public Documents/

Einige Ordner wie /irj/go/km/navigation/documents/Public Documents/ erlauben das hochladen von Dokumenten. Ein Angreifer kann dort also eine HMTL-Webseite hochladen, die –wenn ein Anwender diese Seite aufruft- den Login-cookie ausliest und an einen Server des Angreifers übermittelt oder er fragt dort einfach direkt die Zugangsdaten ab und hofft, dass der Benutzer auf seine Seite hereinfällt.

### Schutzmaßnahmen

Das KM Modul sollte nicht genutzt werden oder es ist mit strengen Zugriffsregeln zu betreiben. Ebenso sind die Login Cookies zu schützen. Sie müssen sicher (secure) übertragen werden und ein Zugriff über Javascript darf nicht erlaubt sein (http_only). Die SAP Note 2068872 - HttpOnly and Secure cookie attributes beschreibt das notwendige Vorgehen.

# Schlusswort

In einem typischen SAP-System finden sich tausende sicherheitsrelevante Konfigurationsoptionen.
Gängige Leitfäden wie der DSAG-Prüfleitfaden oder das BSI-Kompendium listen auf hunderten Seiten Prüfungen und Maßnahmen auf.
Dieses E-Book hat daher nur die Spitze des Eisberges potentieller Angriffsflächen eines SAP-Systems und zugehörige Schutzmaßnahmen auflisten können.

Das Thema SAP-Sicherheit beruht jedoch auf 8 Säulen:

- Sicherheit der Datenbank
- Rollen- und Berechtigungskonzept
- Härtung der Systemkonfiguration
- Sicherheit des Custom ABAP-Codings
- Auditing und Analyse
- Patch-Management
- Sicherheit der Schnittstellen
- Sicherheit des Betriebssystems

Am meisten beachtet wird das Berechtigungskonzept. Hier werden große Projekte aufgesetzt. Die Sicherheit des Betriebssystems wird meist in die Hände der Abteilung IT-Operation gelegt.
Problematisch wird es jedoch wenn die weiteren Aspekte vernachlässigt werden oder es Bruchstellen aufgrund der unterschiedlichen Verantwortlichkeiten gibt und kein ganzheitlicher Ansatz verfolgt wird.

Die ganzheitliche Beachtung der 8 Säulen gehört zwingend zu jedem Sicherheitskonzept dazu. Um dies zu gewährleisten, reichen jedoch die SAP-Standardwerkzeuge bei weitem nicht aus. Kompliziert wird die Situation noch zusätzlich dadurch, dass ein SAP-System nicht isoliert betrachtet werden kann. Es ist immer die SAP-Landschaft und deren Integration zu betrachten.

werth IT bietet mit dem werthAUDITOR eine ganzheitliche Lösung, die die 8 Säulen abdeckt.
werthAUDITOR ist ein innovatives und intuitives Werkzeug zur Absicherung von SAP-Systemen. Durch den Zero-Footprint Ansatz werden keinerlei Produkt-Artefakte in den zu prüfenden SAP-Systemen benötigt und eine zentrale und flexible Prüfung der SAP-

Landschaft ist einfach und schnell einzurichten. Dadurch wird den SAP-Basis-Administratoren ein Großteil des zur Absicherung notwendigen Aufwandes abgenommen. Auf Knopfdruck oder zu geplanten Zeiten kann die gesamte SAP-Landschaft auf unsichere Systeme geprüft werden – ohne manuellen Aufwand zu erzeugen. Dabei werden die geschilderten Risiken des SAP-Gateways oder fehlende Härtung der weiteren Dienste direkt erkannt. Ebenso sind unterschiedliche Vorgaben für Profilparameter bezüglich Produktions- oder Entwicklungssysteme erlaubt. Eine Korrektur abweichender Werte ist sogar auf Knopfdruck oder im Rahmen der automatischen Überwachung möglich.

Unsere Expertise ist in die Entwicklung des werthAUDITOR. Die ganzheitliche Sicherheit von SAP-Systemen wird bei werth IT mit Herzblut gelebt.

# Haftungsausschluss



HERAUSGEBER
werth IT GmbH
Herbert-Wehner-Str. 2
59174 Kamen
Deutschland

Kontakt:
Mail: info@werth-it.de
Phone: +49 2307 287 15 00
Web: https://www.werth-it.de

## Bildrechte

© arsdigital – Fotolia.com