

# Potentielle Sicherheitslücken in Ihrem SAP-HR-System

## Referent

**Peer Hoelterhoff**

- Studium der Wirtschaftswissenschaften
- Beratung im SAP-Umfeld seit 1998
- Fokus auf SAP Technology, SAP Security und SAP HCM

# Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## 1. Bedrohungen für Ihr SAP-System

### Bedrohungspotentiale für Ihr SAP-System

Steigende Komplexität der Vernetzung

Steigende Anzahl von Servern zur Bereitstellung von Services

Steigende Verfügbarkeit der Systeme im Internet

SAP-Sicherheit wird nicht gelebt

Maßnahmen nicht ganzheitlich

Industriespionage

Script-Kiddies

...

## 1. Bedrohungen für Ihr SAP-System

### Welchen Risiken müssen Sie sich stellen?

Angriffe von Innen und Außen!

Löschen von Logs

Erschleichen von  
Berechtigungen

Schwachstellen  
im SAP-Coding  
und Executables

Organisatorische  
Sicherheitslücken

Ausspähen von  
Passwörtern

Ausnutzen von  
Berechtigungen

Datendiebstahl

Manipulation von  
Daten

Schwachstellen  
der System-  
Infrastruktur

Schwachstellen in Datenbanken und  
Betriebssystemen

Fehlende  
Verschlüsselung  
der Kommu-  
nikationswege

Ungesicherte  
Firewalls

SAP\_ALL-  
Berechtigungen

## 1. Bedrohungen für Ihr SAP-System

### Was können Sie dagegen tun?

Absichern Ihrer webbasierten Services beim Betrieb im Internet

SAP Security Notes

Einsatz Notfall-User-Konzept

Alle beteiligten IT-Systeme  
patchen, patchen und patchen!

Optimieren Ihres eingesetzten  
Berechtigungskonzeptes

SAP Early Watch Alert

Absichern SAPGui, RFC und Web

SAP Security Self-Services

Verschlüsselung einsetzen

Einsatz Custom Code Lifecycle Management (CCLM)

Externe Sicherheitsaudits

Code-Analyse

Einsatz von SSO-Lösungen

SAP System Recommendations

Überprüfen der Parameter der eingesetzten IT-Systeme

## 1. Bedrohungen für Ihr SAP-System

### Womit beschäftigen wir uns nachfolgend?

Absichern Ihrer webbasierten Services beim Betrieb im Internet

SAP Security Notes

Einsatz Notfall-User-Konzept

Alle beteiligten IT-Systeme  
patchen, patchen und patchen!

Optimieren Ihres eingesetzten  
Berechtigungskonzeptes

SAP Early Watch Alert

Absicherung RFC-Verbindungen

SAP Security Self-Services

Verschlüsselung einsetzen

Einsatz Custom Code Lifecycle Management (CCLM)

Externe Sicherheitsaudits

Code-Analyse

Einsatz von SSO-Lösungen

SAP System Recommendations

...



## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## 2. Einsatz des richtigen Berechtigungskonzeptes

### Kritische Erfolgsfaktoren beim Design/Re-Design

- Beachtung sämtlicher Compliance-Anforderungen (Gesetze, Standards, DIN-Normen, Interne Anforderungen)
- So wenig Rollen wie möglich
- Maximale Transparenz
- Nur so viel Rechte, wie nötig
- Wahl der geeigneten Berechtigungsprüfung
- Entwicklung eines Vorgehensmodells

## 2. Einsatz des richtigen Berechtigungskonzeptes

### Möglichkeiten der Berechtigungsprüfung in SAP HCM

#### Allgemeine Berechtigungsprüfung

Berechtigungen auf Daten: Regelt Zugriff auf Daten (Infotypen etc.)

#### Strukturelle Berechtigungsprüfung

Berechtigungen basierend auf Zuordnung im OM: Regelt Zugriff auf Objekte (Planstellen etc.)

#### Kontextabhängige Berechtigungsprüfung

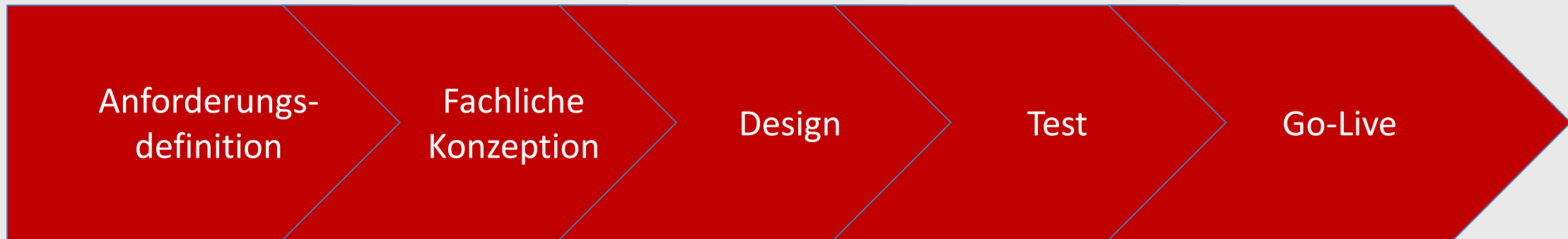
Kombination von allgemeinen und strukturellen Berechtigungen



Empfehlung

## 2. Einsatz des richtigen Berechtigungskonzeptes

### Vorgehensmodell



## 2. Einsatz des richtigen Berechtigungskonzeptes

### Vorgehensmodell



### Ermittlung der Anforderungen

- Einbeziehen der Nutzergruppen Berechtigungsadministration, Personalabteilung, Abteilungsleitung, Unternehmensleitung, ESS-Benutzer, IT-Abteilung, ext. Berater, Datenschutzbeauftragte, Auditoren usw.
- Projektplanung (Budget, Zeit, Ressourcen) erstellen
- Namenskonventionen
- Einsatz der ZBV möglich und sinnvoll?

## 2. Einsatz des richtigen Berechtigungskonzeptes

### Vorgehensmodell



### Definieren Sie Ihre Prozesse

- Welche Prozessabläufe sind in der Organisation relevant?
- Bereinigung der Prozesse um Leistungen, die nicht im SAP-System erbracht werden
- Leistungsermittlung: Sammeln der Transaktionen, Reports etc.
- Berücksichtigung der Eigenentwicklungen
- Erstellen einer Leistungsübersicht und Benutzer-Funktions-Matrix
- Verantwortungsbereiche definieren
- Dokumentation der Prozessbeschreibung
- Prozessdefinition Berechtigungsmanagement
- Ableiten der Rollen

## 2. Einsatz des richtigen Berechtigungskonzeptes

### Vorgehensmodell



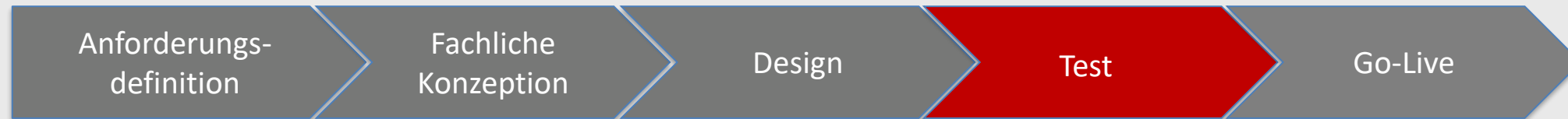
### Implementierung der Rollen auf Basis der fachlichen Konzeption

- Einrichtung bzw. Überprüfung des SAP Profilgenerators
- Organisationsebenen anlegen bzw. überprüfen
- Entwicklung der Rollen
- Erstellung eines Testplans
- Vorabtests durch IT und/oder Key-User
- Zuordnung der Benutzer zu den Rollen auf Basis der Leistungsübersicht
- Design Berechtigungsmanagement (hier Vier-Augen-Prinzip beachten)



## 2. Einsatz des richtigen Berechtigungskonzeptes

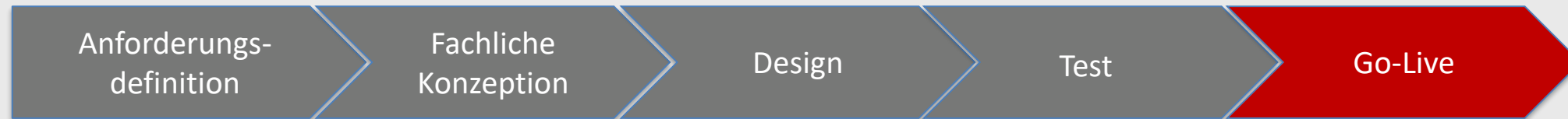
### Vorgehensmodell



- Integrationstest durch Fachabteilung
- Iteratives Vorgehen und Berichtigung von ermittelten Fehlern
- Abnahme und Freigabe der Rollen für den Produktivstart

## 2. Einsatz des richtigen Berechtigungskonzeptes

### Vorgehensmodell



- Transport ins Produktivsystem
- Zuordnung der neu entwickelten Rollen
- Entzug alter Berechtigungen
- Einführung Berechtigungsmanagement

# Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

### 3. Revisionssicheres Notfall-User-Konzept

#### Warum denn ein Notfall-User-Konzept?

- Durch die Implementierung eines Berechtigungskonzeptes haben alle Anwender die für Ihre Arbeit notwendigen Berechtigungen
- Ausnahmesituationen erfordern die Vergabe von weitergehenden Berechtigungen an einzelne Anwender
- Änderungen an diesem Konzept sind in der Regel langwierig und nicht ad-hoc umsetzbar
- Zuordnung von Rollen mit erweiterten Berechtigungen nicht sinnvoll, da Vergabe nur temporär und unter Kontrolle erfolgen soll
- Keine weiterreichenden Berechtigungen für den Alltag vergeben!

### 3. Revisionssicheres Notfall-User-Konzept

#### Wie erreicht man das?

- Definition von Berechtigungsrollen mit der Berechtigung, einen Notfallbenutzer beantragen zu können
- Definition der Rollen für die Notfallbenutzer
- Erstellung von Funktionen für die Beantragung des Notfall-Users und dessen Aktivierung bzw. Deaktivierung
- Erstellung eines Workflows für die Genehmigung durch Vorgesetzten oder Prüfung auf Ticketsystem
- Konfiguration des Security Audit Logs für die Protokollierung
- Implementierung eines Auswertungstools

### 3. Revisionssicheres Notfall-User-Konzept

## Möglicher Prozess Notfall-User-Konzept



### Prozessablauf

- Angabe von Gründen für die Beantragung und der gewünschten Dauer
- Optional Prüfung auf Tickets
- Optional Genehmigung durch Vorgesetzten
- Notfall-Benutzer wird entsperrt und mit neuem Initialkennwort bereitgestellt
- Benachrichtigung entweder per Mail oder Hinweisfenster im SAPGui
- Benutzer meldet sich an

### 3. Revisionssicheres Notfall-User-Konzept

## Möglicher Prozess Notfall-User-Konzept



### Prozessablauf

- Während der Aktivitäten werden alle Schritte im Rahmen des Security-Audit-Logs protokolliert



### 3. Revisionssicheres Notfall-User-Konzept

## Möglicher Prozess Notfall-User-Konzept



### Prozessablauf

- Nach Ablauf der vorher definierten Laufzeit wird der Notfall-User automatisch begrenzt und das Kennwort geändert
- Über die Standard-Auswertungstools des SAP Security Audit Logs oder über einen individuellen Report können die Aktivitäten nachvollzogen werden

### 3. Revisionssicheres Notfall-User-Konzept

#### **Vorteile:**

- Transparente, zeitlich beschränkte Vergabe von Sonderrechten an berechnigte Mitarbeiter
- Zeit- und Kostenersparnis durch Wegfall von umständlichen Vergabeprozessen
- Verzicht auf Universal-Berechtigungen für Standardbenutzer
- Vollständige Protokollierung der Notfalluser-Aktivitäten und Nachvollziehbarkeit für Auditoren und Wirtschaftsprüfer

## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## 4. Effektives Implementieren von SAP-Security-Hinweisen

### Was sind SAP-Security-Notes?

- Standard SAP-Hinweise mit und ohne Korrekturanleitung
- Beinhalten Sicherheitsrisiken und Schwachstellen innerhalb der von SAP ausgelieferten Softwarekomponenten (SAP-Code, Kernel, Datenbank, Infrastruktur)
- Schwachstellen ermöglichen Voll-Zugriff auf Applikation und/oder Datenbank unter Umgehung von implementierten Sicherheitsprüfungen
- Folgen sind Manipulation und Diebstahl von Daten, Verschleierung von Systemaktivitäten, Nichtverfügbarkeit von wichtigen Services
- Veröffentlichung erfolgt monatlich am SAP Security Patch Day, jeden zweiten Dienstag im Monat unter <https://support.sap.com/securitynotes>

## 4. Effektives Implementieren von SAP-Security-Hinweisen

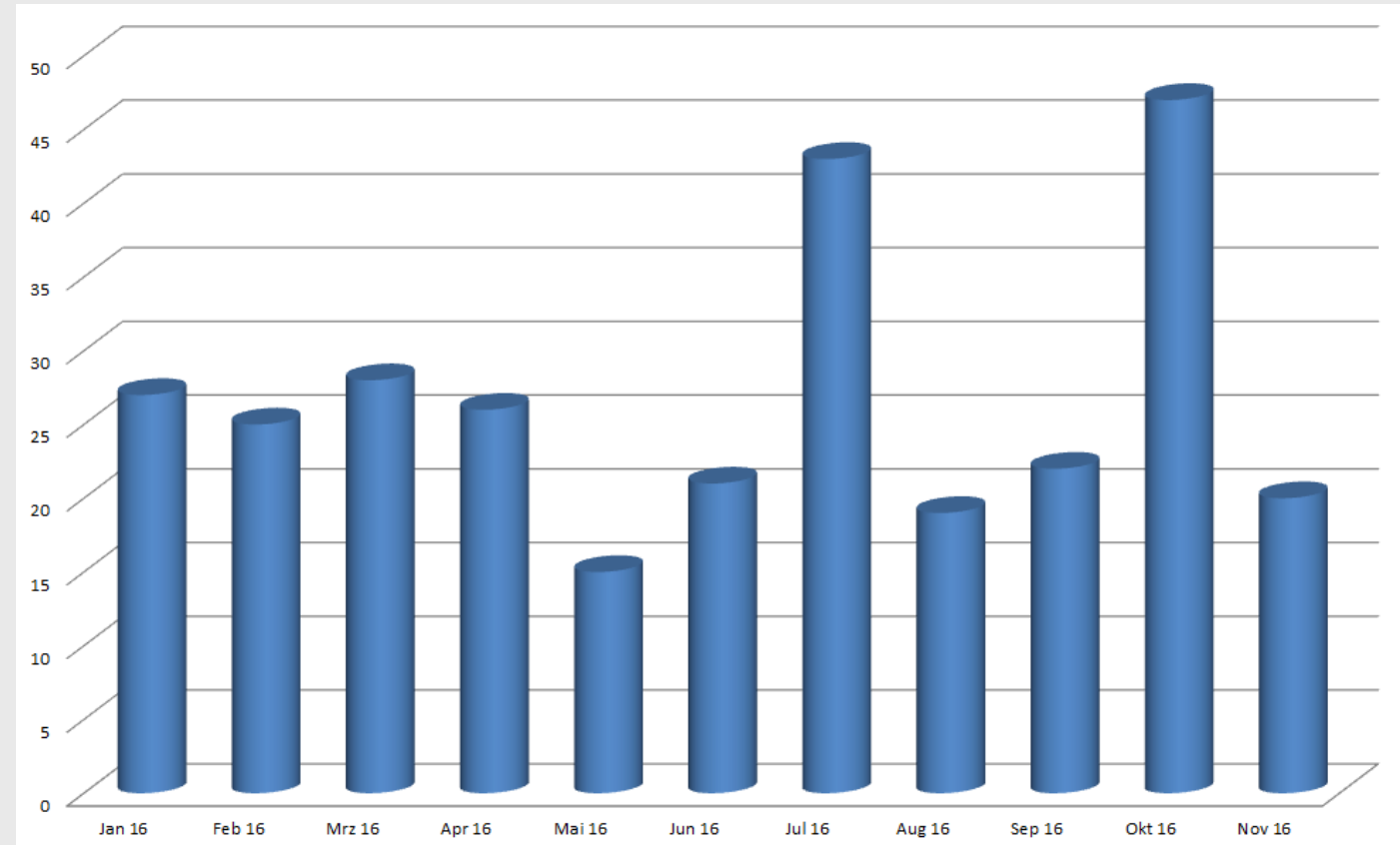
### Anzahl der veröffentlichten Sec-Notes

Erste Sec-Note: Oktober 2001

Seit Beginn veröffentlicht: ca. 3800

Durchschnittliche Anzahl  
je Monat: ca. 25

Quelle: SAP Service Marketplace



## 4. Effektives Implementieren von SAP-Security-Hinweisen

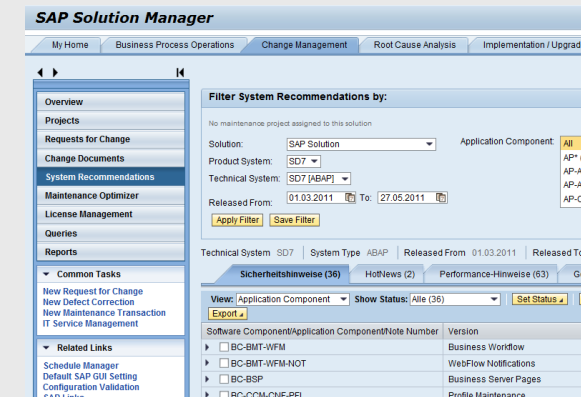
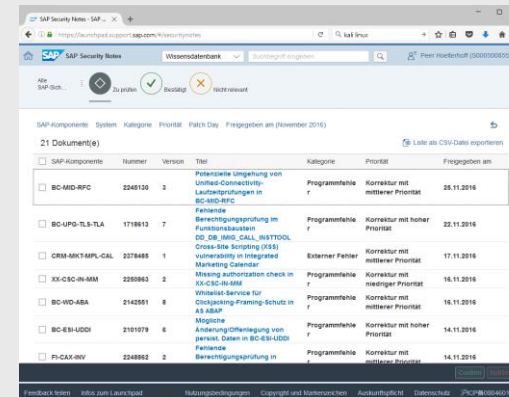
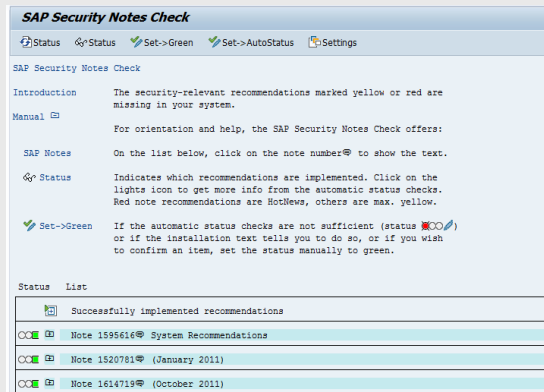
### Herausforderung für den Anwender

- Identifizieren der relevanten SAP Security Notes
- Bedrohungslage oft nicht klar
- Schließen der aufgezeigten Sicherheitslücken
- Nachweis der Bearbeitung für potentiell Audit

## 4. Effektives Implementieren von SAP-Security-Hinweisen

### Welche Werkzeuge stellt SAP bereit?

- Veraltetes Verfahren über RSECNOTE
- Sichtung der Hinweise im Service Marketplace
- Nutzung der System Recommendations im SAP Solution Manager





## 4. Effektives Implementieren von SAP-Security-Hinweisen

### RSECNOTE

- Veralteter Service
- Keine Updates
- Kein umfänglicher Schutz

**SAP Security Notes Check**

Status ⚙️ Status ✅ Set->Green ✅ Set->AutoStatus ⚙️ Settings

SAP Security Notes Check

**Introduction** The security-relevant recommendations marked yellow or red are missing in your system.

**Manual** 📖

**SAP Notes** On the list below, click on the note number ⓘ to show the text.

**⚙️ Status** Indicates which recommendations are implemented. Click on the lights icon to get more info from the automatic status checks. Red note recommendations are HotNews, others are max. yellow.

**✅ Set->Green** If the automatic status checks are not sufficient (status ⚠️🔴🔴🔴) or if the installation text tells you to do so, or if you wish to confirm an item, set the status manually to green.

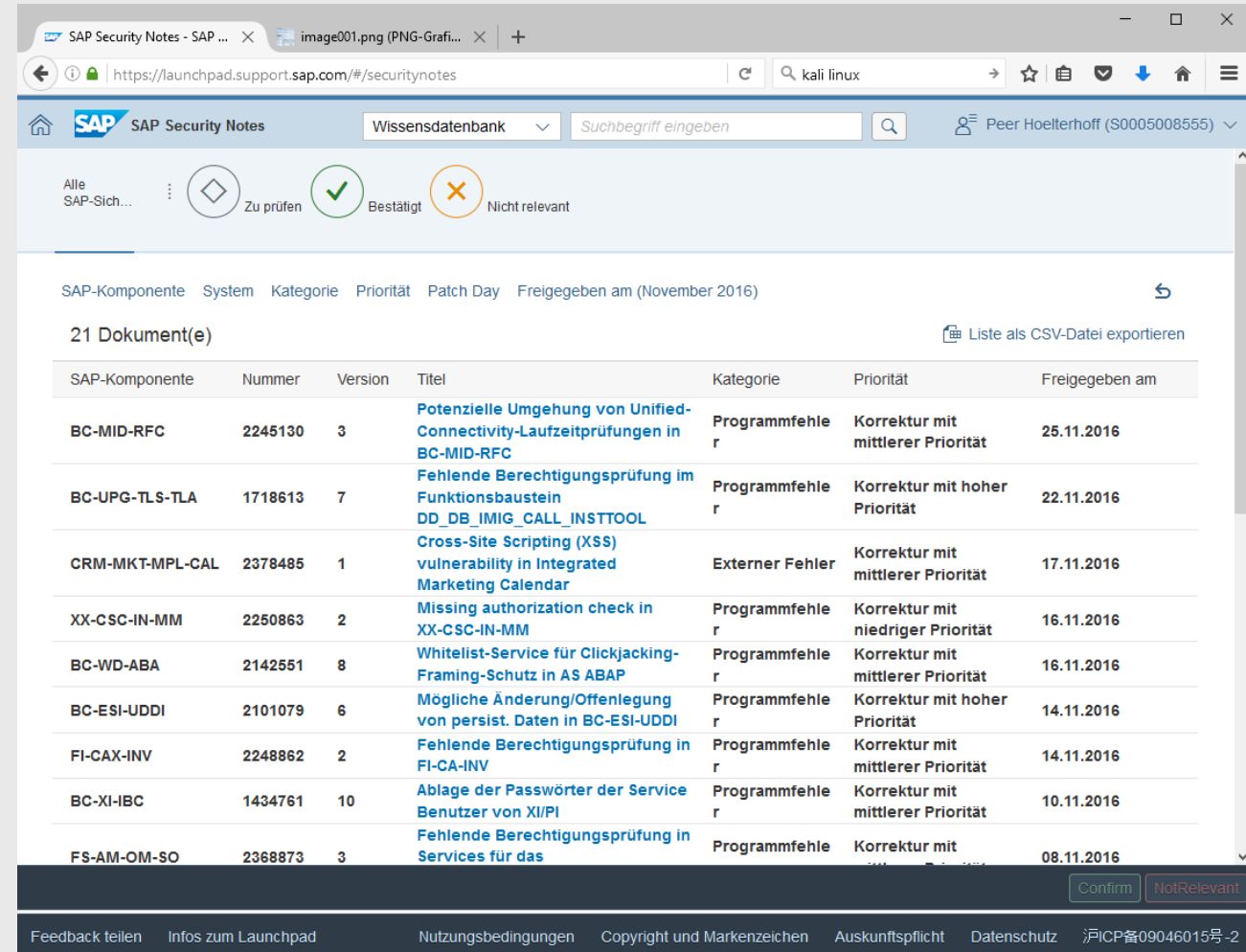
Status List

📁	Successfully implemented recommendations
🔴🔴🔴 ⓘ	Note 1595616 ⓘ System Recommendations
🔴🔴🔴 ⓘ	Note 1520781 ⓘ (January 2011)
🔴🔴🔴 ⓘ	Note 1614719 ⓘ (October 2011)

## 4. Effektives Implementieren von SAP-Security-Hinweisen

### Security Notes im SMP

- Aufruf im Browser unter [support.sap.com/securitynotes](https://support.sap.com/securitynotes)
- Filterung nach eigenen Systemen, Kategorien oder Priorität
- Exportfunktionen



The screenshot shows the SAP Security Notes interface in a browser. The URL is <https://launchpad.support.sap.com/#/securitynotes>. The user is Peer Hoelterhoff (S0005008555). The interface displays a list of 21 documents. The table below represents the data shown in the screenshot.

SAP-Komponente	Nummer	Version	Titel	Kategorie	Priorität	Freigegeben am
BC-MID-RFC	2245130	3	Potenzielle Umgehung von Unified-Connectivity-Laufzeitprüfungen in BC-MID-RFC	Programmmfehler	Korrektur mit mittlerer Priorität	25.11.2016
BC-UPG-TLS-TLA	1718613	7	Fehlende Berechtigungsprüfung im Funktionsbaustein DD_DB_IMIG_CALL_INSTTOOL	Programmmfehler	Korrektur mit hoher Priorität	22.11.2016
CRM-MKT-MPL-CAL	2378485	1	Cross-Site Scripting (XSS) vulnerability in Integrated Marketing Calendar	Externer Fehler	Korrektur mit mittlerer Priorität	17.11.2016
XX-CSC-IN-MM	2250863	2	Missing authorization check in XX-CSC-IN-MM	Programmmfehler	Korrektur mit niedriger Priorität	16.11.2016
BC-WD-ABA	2142551	8	Whitelist-Service für Clickjacking-Framing-Schutz in AS ABAP	Programmmfehler	Korrektur mit mittlerer Priorität	16.11.2016
BC-ESI-UDDI	2101079	6	Mögliche Änderung/Offenlegung von persist. Daten in BC-ESI-UDDI	Programmmfehler	Korrektur mit hoher Priorität	14.11.2016
FI-CAX-INV	2248862	2	Fehlende Berechtigungsprüfung in FI-CA-INV	Programmmfehler	Korrektur mit mittlerer Priorität	14.11.2016
BC-XI-IBC	1434761	10	Ablage der Passwörter der Service Benutzer von XI/PI	Programmmfehler	Korrektur mit mittlerer Priorität	10.11.2016
FS-AM-OM-SO	2368873	3	Fehlende Berechtigungsprüfung in Services für das	Programmmfehler	Korrektur mit	08.11.2016

At the bottom of the table, there are buttons for 'Confirm' and 'NotRelevant'. The footer of the page includes links for 'Feedback teilen', 'Infos zum Launchpad', 'Nutzungsbedingungen', 'Copyright und Markenzeichen', 'Auskunftspflicht', 'Datenschutz', and a license number '沪ICP备09046015号-2'.

## 4. Effektives Implementieren von SAP-Security-Hinweisen

### **Empfohlene Vorgehensweise: SAP System Recommendations**

- Verfügbar auf SAP Solution Manager
- Filtert Hinweise nach Relevanz für den eingesetzten Systemstrang, das System und Applikationskomponente
- Integriertes Statusmanagement
- Exportfunktion
- Integration mit Hinweisimplementierung im Tochtersystem
- Integration mit Change Request Management (CharM)
- Integration mit Business Process Change Analyser (BPCA)

## 4. Effektives Implementieren von SAP-Security-Hinweisen

### Handlungsempfehlungen (1/2)

- Beschreiben Sie den Patchprozess in Ihrer Organisation und teilen Sie die Verantwortung auf
- Monatliche Bearbeitung der Sicherheitshinweise
- Nicht nur Hinweise der eingesetzten Applikation, sondern alle Hinweise der installierten Komponenten sind relevant
- Sofortiges Einspielen der Hinweise mit Korrekturanleitung ohne manuelle Tätigkeiten

## 4. Effektives Implementieren von SAP-Security-Hinweisen

### Handlungsempfehlungen (2/2)

- Analyse der „schwierigen“ Hinweise mit manuellen Tätigkeiten oder Nebeneffekten und Implementierung im Rahmen eines Projektvorgangs
- Analysieren der Hinweise ohne Korrekturanleitung und Beurteilung des Risikos und Einleiten von entsprechenden Maßnahmen
- Reduzierung der manuellen Tätigkeiten durch Einspielen der Support Package Stacks für Ihren Systemstrang
- Definieren Sie Zeitfenster für die Implementierung in Abhängigkeit von Priorität des Patches und des Implementierungsprozesses
- Nutzen Sie das Tool System Recommendations und protokollieren Sie Ihre Entscheidungen und Maßnahmen

## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## 5. Sicherer Betrieb Ihrer Portallösung im Internet

### **Sie betreiben eine Webanwendung im Internet?**

- SAP Learning Solution
- SAP E-Recruiting
- MSS/ESS-Lösung
- SAP Fiori
- Einzelne webbasierte Schnittstellen
- Kundeneigene webbasierte Services



## 5. Sicherer Betrieb Ihrer Portallösung im Internet

### Beachten Sie die Risiken

- Im Internet existieren frei zugängliche Datenbanken mit im Internet erreichbaren SAP-basierenden Endpunkten
- Potentielle Angriffsziele sind für jeden leicht zu ermitteln

The screenshot shows the Shodan search engine interface with the query 'irj/portal country:DE'. The results are categorized into several sections:

- TOP COUNTRIES:** A world map with Germany highlighted, showing 147 results.
- TOP CITIES:** A list of cities in Germany with their respective result counts: Wolfsburg (3), Frankfurt Am Main (3), Regensburg (2), Kronberg (2), and Kaiserslautern (2).
- TOP SERVICES:** A list of services: HTTPS (118) and HTTP (29).
- TOP ORGANIZATIONS:** A list of organizations: Deutsche Telekom AG (53), Siemens AG (12), arvato systems GmbH (9), SAP AG Walldorf (3), and net.de AG (2).
- TOP OPERATING SYSTEMS:** A list of operating systems: Windows 7 or 8 (3) and Linux 3.x (1).
- TOP PRODUCTS:** A list of products: Apache httpd (16), SAP Web Application Server (2), and SAP J2EE Engine httpd (2).

Three specific search results are highlighted with detailed information:

- 141.6.3.192:** BASF Business Services GmbH, Germany. Added on 2016-11-24 13:00:11 GMT. SSL Certificate details: Issued By: GlobalSign, Common Name: GlobalSign, Organization Validation CA - SHA256 - G2, Organization: GlobalSign nv-sa. Issued To: Common Name: tm.basf.com, Organization: BASF Business Services GmbH. Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2. HTTP/1.0 302 Found, Location: /irj/portal/trd?guest\_user=Gues, Server: BigIP, Connection: Keep-Alive, Content-Length: 0.
- 193.238.10.111:** Deutsche Telekom AG, Germany. Added on 2016-11-24 12:32:40 GMT. SSL Certificate details: Issued By: COMODO RSA, Common Name: COMODO RSA, Organization Validation Secure Server CA, Organization: COMODO CA Limited. Issued To: Common Name: \*.k-plus-s.com, Organization: K+S AG. Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2. HTTP/1.0 307 Temporary Redirect, Location: https://portal.k-plus-s.com/irj, Server: BigIP, Connection: Keep-Alive, Content-Length: 0.
- SAP&#x20;NetWeaver&#x20;Portal:** 194.156.246.129, Deutsche Telekom AG, Germany. Added on 2016-11-24 11:27:53 GMT. SSL Certificate details: Issued By: Go Daddy Secure Certificate Authority - G2, Common Name: Go Daddy Secure Certificate Authority - G2, Organization: GoDaddy.com, Inc. Issued To: Common Name: \*.wmf.com. Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2.

Quelle: <https://www.shodan.io>

## 5. Sicherer Betrieb Ihrer Portallösung im Internet

### Beachten Sie die Risiken

#### Mögliches Angriffsszenario:

- Ermitteln des Ziels
- Herausfinden von Details zum Angriffsziel
- Abgleichen der gefunden Informationen mit bekannten Schwachstellen (Exploits)
- Skriptbasiertes, automatisiertes Angreifen des Ziels durch Ausnutzen des Exploits

## 5. Sicherer Betrieb Ihrer Portallösung im Internet

### Hackertools im Einsatz:

```

root@phkl:~# nmap -T4 -v -O -p 3299 sap.hoelterhoff.info

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-25 21:22 CET
Initiating Ping Scan at 21:22
Scanning sap.hoelterhoff.info (81.20.135.34) [4 ports]
Completed Ping Scan at 21:22, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:22
Completed Parallel DNS resolution of 1 host. at 21:22, 0.02s elapsed
Initiating SYN Stealth Scan at 21:22
Scanning sap.hoelterhoff.info (81.20.135.34) [1 port]
Discovered open port 3299/tcp on 81.20.135.34
Completed SYN Stealth Scan at 21:22, 0.05s elapsed (1 total ports)
Initiating OS detection (try #1) against sap.hoelterhoff.info (81.20.135.34)
Nmap scan report for sap.hoelterhoff.info (81.20.135.34)
Host is up (0.012s latency).
Other addresses for sap.hoelterhoff.info (not scanned):
PORT      STATE SERVICE
3299/tcp  open  saprouter
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X, Microsoft Windows 7|2012
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Microsoft Windows 7 or Windows Server 2012
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/./share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.96 seconds
Raw packets sent: 36 (3.582KB) | Rcvd: 13 (694B)
root@phkl:~#

```

```

Matching Modules
=====

```

Name	Disclosure Date	Rank	Description
auxiliary/scanner/sap/sap_router_info_request		normal	SAPRouter Admin Request
auxiliary/scanner/sap/sap_router_portscanner		normal	SAPRouter Port Scanner

```

msf auxiliary(sap_service_discovery) > use auxiliary/scanner/sap/sap_router_info_request
msf auxiliary(sap_router_info_request) > show options

Module options (auxiliary/scanner/sap/sap_router_info_request):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    3299             yes       The target address range or CIDR identifier
  RPORT     3299             yes       The target port
  THREADS   1                yes       The number of concurrent threads

msf auxiliary(sap_router_info_request) > set RHOSTS sap.hoelterhoff.info
RHOSTS => sap.hoelterhoff.info
msf auxiliary(sap_router_info_request) > run

[+] 81.20.135.34:3299 - 81.20.135.34:3299 - Connected to saprouter
[+] 81.20.135.34:3299 - 81.20.135.34:3299 - Sending ROUTER ADM packet info request
[+] 81.20.135.34:3299 - 81.20.135.34:3299 - Got INFO response
[-] 81.20.135.34:3299 - 81.20.135.34:3299 - Access denied

[*] Scanned 1 of 2 hosts (50% complete)
[+] 81.20.135.34:3299 - 81.20.135.34:3299 - Connected to saprouter
[+] 81.20.135.34:3299 - 81.20.135.34:3299 - Sending ROUTER ADM packet info request
[+] 81.20.135.34:3299 - 81.20.135.34:3299 - Got INFO response
[-] 81.20.135.34:3299 - 81.20.135.34:3299 - Access denied

[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(sap_router_info_request) >

```

## 5. Sicherer Betrieb Ihrer Portallösung im Internet

### Verschiedene Maßnahmen zur Erhöhung der Systemsicherheit

#### Absichern der Netzwerke

- Separieren der Netzwerksegmente
- Einsatz von Next Generation Firewalls
- Einsatz einer DMZ
- Einsatz SAP Webdispatcher als Proxy- und Contentfilter

#### Patchen, Patchen und Patchen!

- Betriebssysteme
- Firewalls
- SAP-Applikationen
- SAPRouter
- SAP Webdispatcher

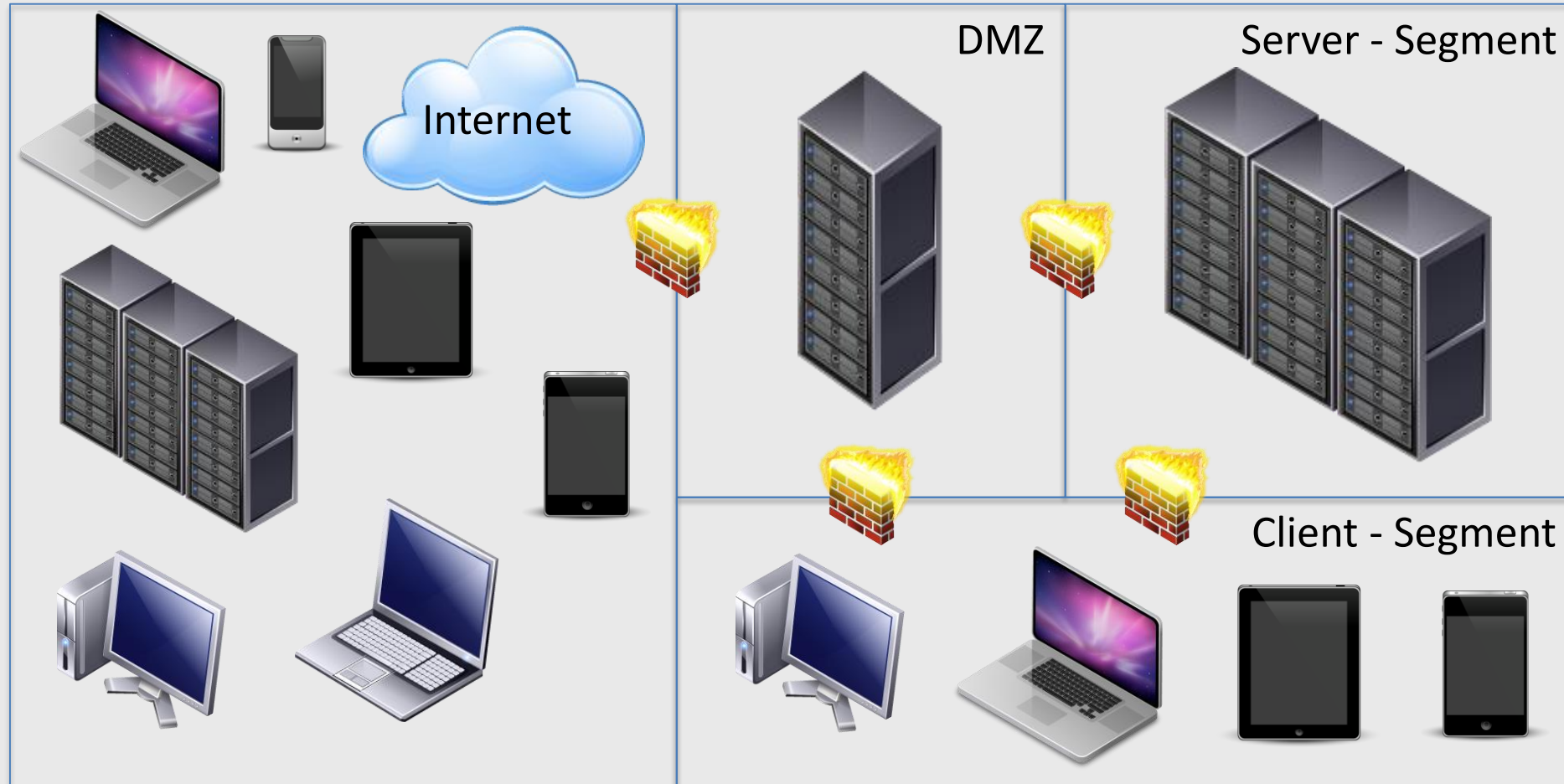
#### Verschlüsselung der Kommunikation

- Absichern der SAPGui und RFC-Verbindungen mit SNC
- Absichern Webservices mit SSL/TLS
- Absichern Mail mit TLS



## 5. Sicherer Betrieb Ihrer Portallösung im Internet

### Absichern des Unternehmensnetzwerkes



## 5. Sicherer Betrieb Ihrer Portallösung im Internet

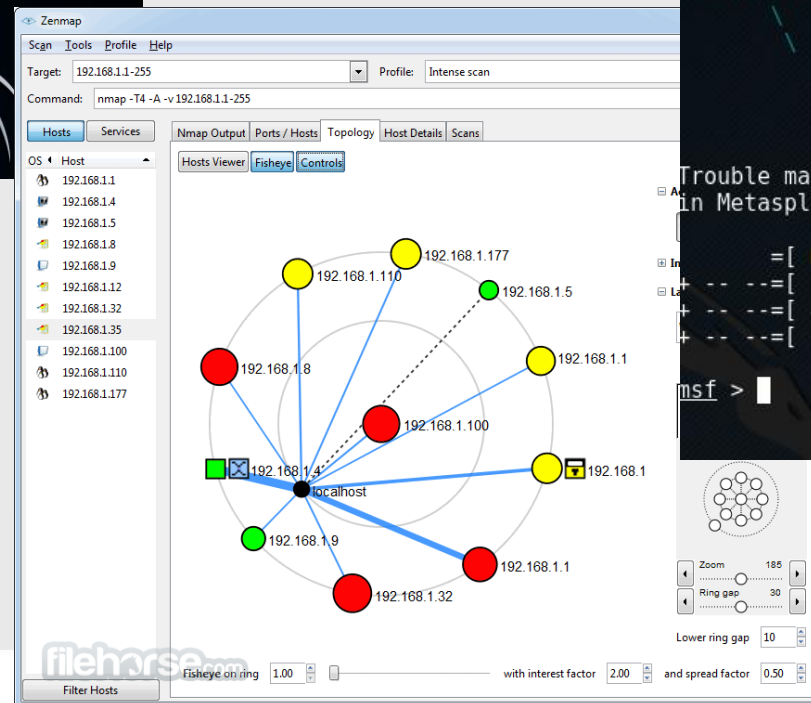
### Verschiedene Maßnahmen zur Erhöhung der Systemsicherheit

- Implementieren eines Honeypot mit Vorgaukeln von SAP-Services
- Testen Sie Ihr Netzwerk mit bekannten Hacker-Tools durch Unternehmens-IT
- Lassen Sie einen Penetrationstest durch externen Dienstleister durchführen



No.	Time	Source	Destination	Protocol	Length
708	13.650579	192.168.1.77	173.194.33.6	TCP	54
709	13.662945	173.194.33.6	192.168.1.77	TCP	60
710	13.995895	Actionte_d8:a3:88	Msi_74:82:e6	ARP	60
711	13.995922	Msi_74:82:e6	Actionte_d8:a3:88	ARP	42
712	15.030559	fe80::bdca:e67b:5eb7::ff02::c		SSDP	200
713	15.058140	192.168.1.76	239.255.255.250	UDP	50
714	15.123002	192.168.1.74	239.255.255.250	UDP	56
715	17.628874	192.168.1.77	208.43.115.82	TCP	60
716	17.711021	208.43.115.82	192.168.1.77	TCP	60

Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)  
 Ethernet II, Src: Msi\_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte\_d8:a3:88 (08:00:27:08:00:27)  
 Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 72.165.67.144 (72.165.67.144)  
 User Datagram Protocol, Src Port: 53691 (53691), Dst Port: 27017 (27017)  
 Data (84 bytes)



```
A database appears to be already configured, skipping initialization

# cowsay++
< metasploit >

Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.12.41-dev ]
-- ==[ 1597 exploits - 912 auxiliary - 274 post ]
-- ==[ 458 payloads - 39 encoders - 8 nops ]
-- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On

## Inhalt

1

Bedrohungen für Ihr SAP-HR-System

2

Einsatz des richtigen Berechtigungskonzeptes

3

Revisionssicheres Notfall-User-Konzept

4

Effektives Implementieren von SAP-Security-Hinweisen

5

Sicherer Betrieb Ihrer Portallösung im Internet

6

Einsatz von Single Sign-On



## 6. Einsatz von Single Sign-On

### Was ist Single Sign-On?

- Nutzung von mehreren IT-Diensten ohne sich mehrfach registrieren bzw. anmelden zu müssen
- Anmeldung erfolgt nur einmal an einem dedizierten Anmeldesystem
- Nutzung erfolgt über verschiedene Technologieansätze

### Beweggründe für die Einführung

- Vielzahl von verschiedenen IT-Systemen, Benutzernamen und Passwörtern
- Erhöhte Sicherheit vs. Anwenderproduktivität
  - Reduktion Zeitaufwand für Benutzer (Passwortwechsel, Login-Probleme)
  - Reduktion Zeitaufwand Support
- Erhöhung der Sicherheit durch Verschlüsselung
- Anwenderzufriedenheit

## 6. Einsatz von Single Sign-On

### Vorteile

- Mehrere Passwörter verleiten Anwender zur Nutzung eines „General“-Passwortes
- Beschränkte Gültigkeitszeiträume erhöhen das Verwenden von ausrechenbaren Passwortlogiken
- Erhöhung der Anwendungsakzeptanz durch vereinfachten Zugriff
- Verringerung der Ausspähmöglichkeit von Kennwörtern im Netzwerk
- Kostenersparnis durch wegfallenden Administrationsaufwand für Benutzermanagement
- Erhöhung der Produktivität durch Verringerung von Zugangsbeschränkungen durch vergessene, verlorene Passwörter, Sperrungen etc.
- Einsatz von SSO erzwingt Verschlüsselung des Kommunikationsweges – dies erhöht die Datensicherheit

## 6. Einsatz von Single Sign-On

### Nachteile

- Schwache SSO-Implementierungen erlauben den Verlust des „Master“-Passwortes, was den missbräuchlichen Zugriff auf alle beteiligten IT-Systeme erlaubt

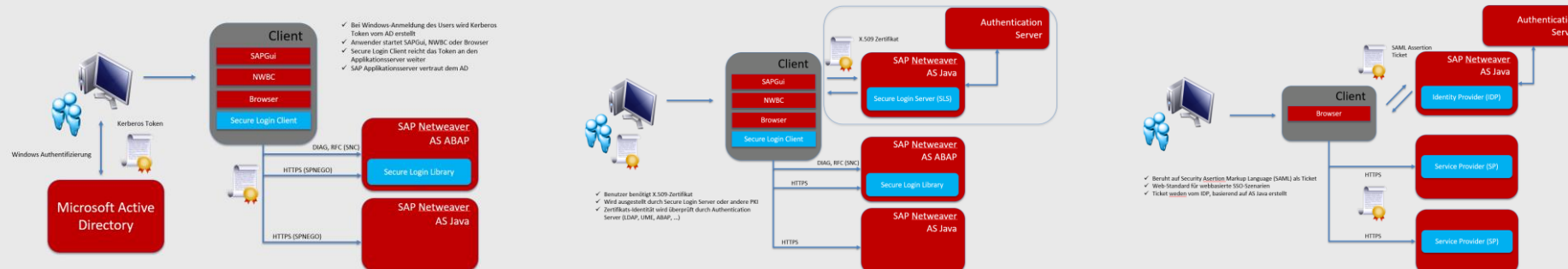
## 6. Einsatz von Single Sign-On

### Verschiedene SSO-Methoden

Single Sign-On mit Kerberos

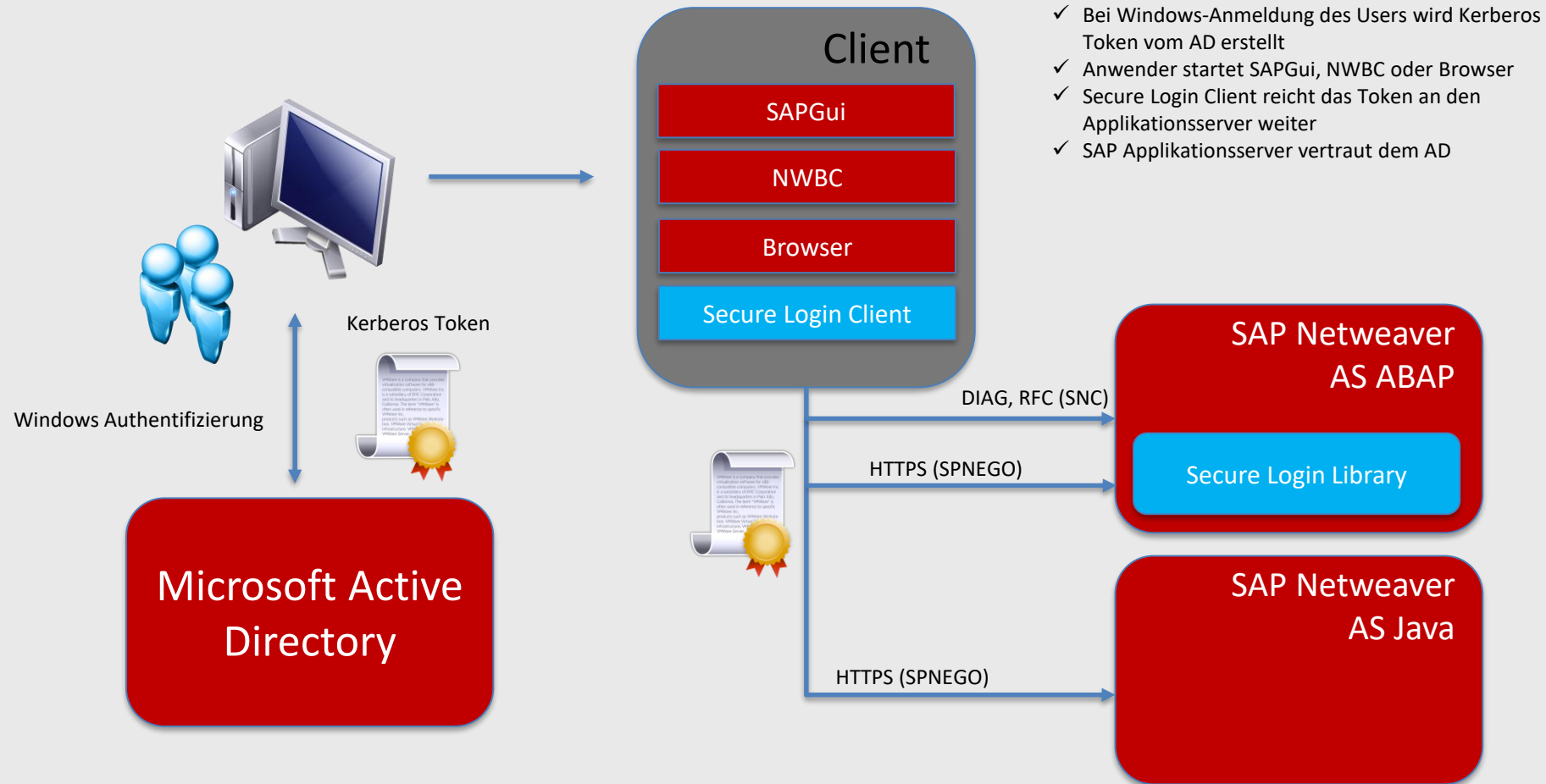
Single Sign-On mit X.509-Zertifikat

Single Sign-On mit SAML 2.0



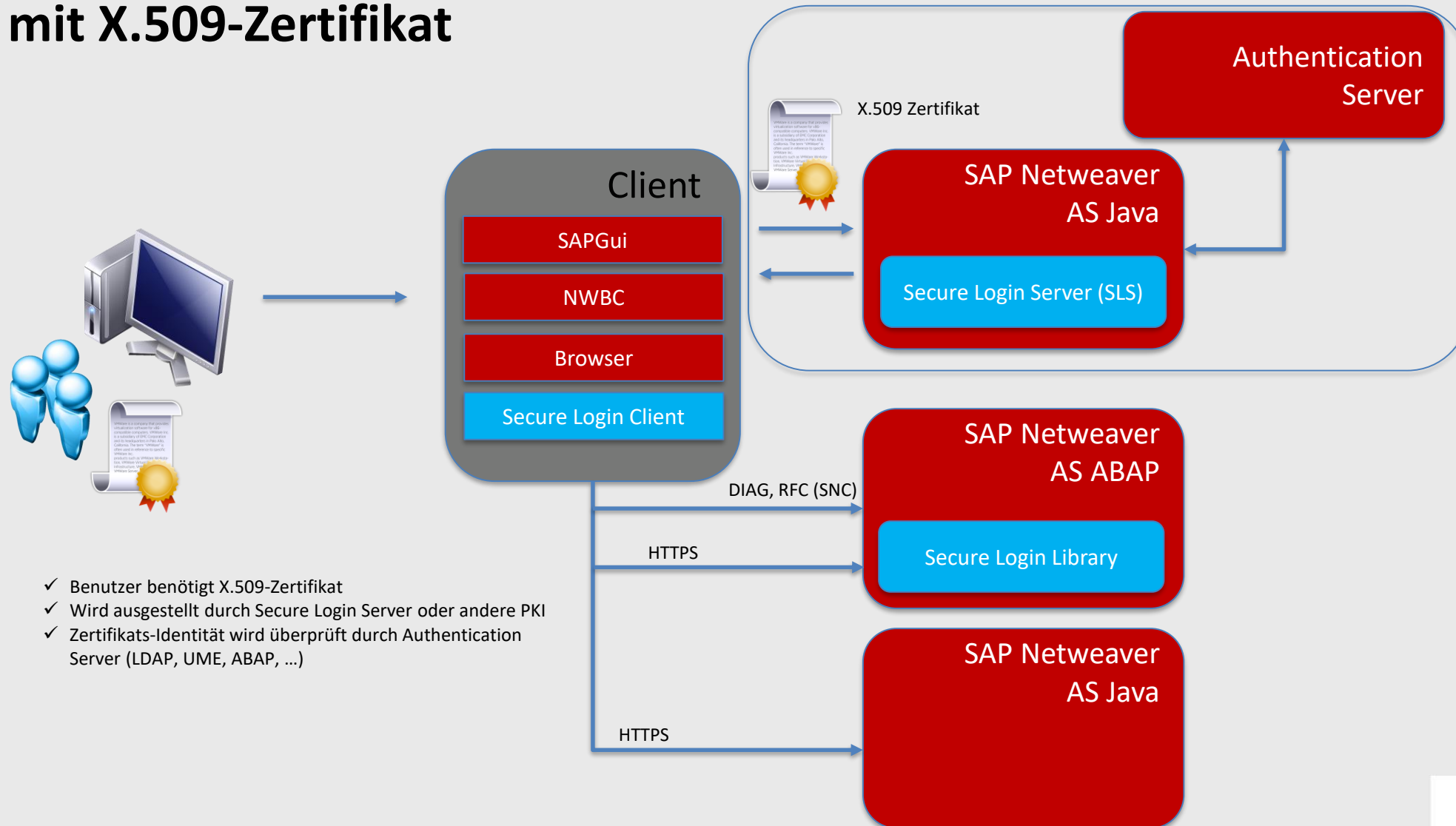
## 6. Einsatz von Single Sign-On

### SSO mit Kerberos



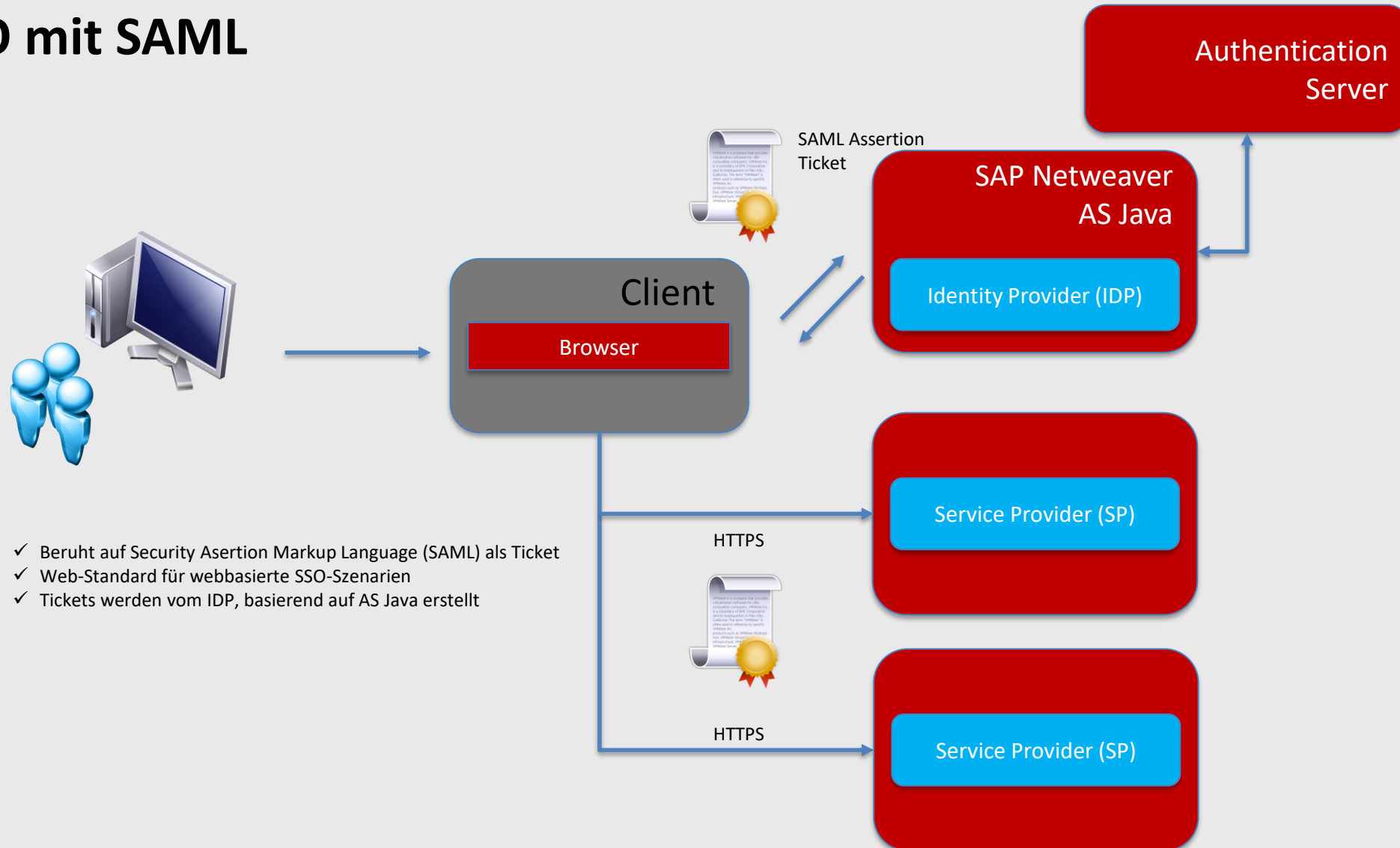
## 6. Einsatz von Single Sign-On

## SSO mit X.509-Zertifikat



## 6. Einsatz von Single Sign-On

### SSO mit SAML



Wie geht es weiter?

## Sie haben Fragen oder möchten mehr Details?

Danke für Ihre Aufmerksamkeit!

Bitte sprechen Sie mich nach Ende des Vortrags im Laufe der Praxistage gerne an. Ich stehe zu Ihrer Verfügung!

Mehr Informationen auch im Web unter [hoelterhoff.info](https://hoelterhoff.info)

