SECUDE for mySAP.com

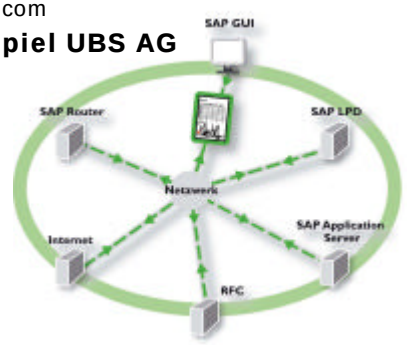
Secure Network Communication
Single Sign-On

SECUDE GmbH
Darmstadt
www.secude.de

Redner: Markus Nüsseler

Agenda

- **Statische Passworte**
  - Was sind die Probleme?
  - Wie sieht die Lösungen aus?
- **Secure Network Communication (SNC)**
  - SECUDE for mySAP.com
  - SECUDE SecurLogin for mySAP.com
- **Return on Invest am Beispiel UBS AG**



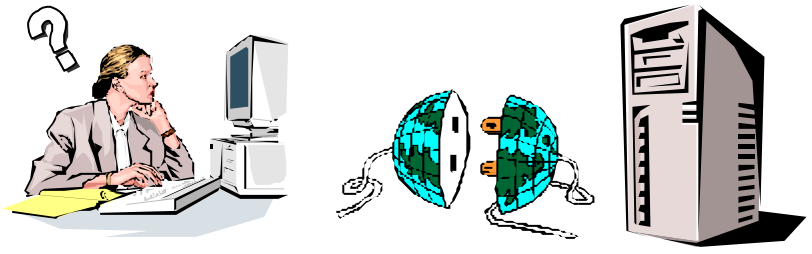
Probleme durch die Anmeldung mit Username und Passwort

3

Unsicherheitsfaktor Mensch

Passwortcontainer Mensch

- Vergessen von Passworten
- Wahl von einfachen Passworten
- Kein regelmässiger Wechsel der Passworte
- Vergabe von gleichem Passwort für verschiedene Systeme
- Erstellen von Spickzetteln

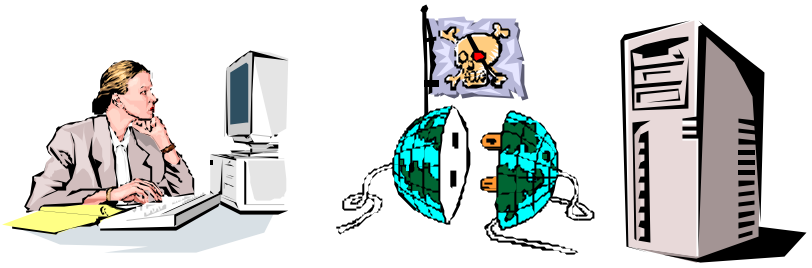


4

Unsicherheitsfaktor Netzwerk

Standard SAP: Unsicheres Netzwerk

- Benutzername und Passwort werden ungesichert übertragen.
- Alle Informationen sind unverschlüsselt auf dem Netzwerk.



SECUDE e-security for e-business

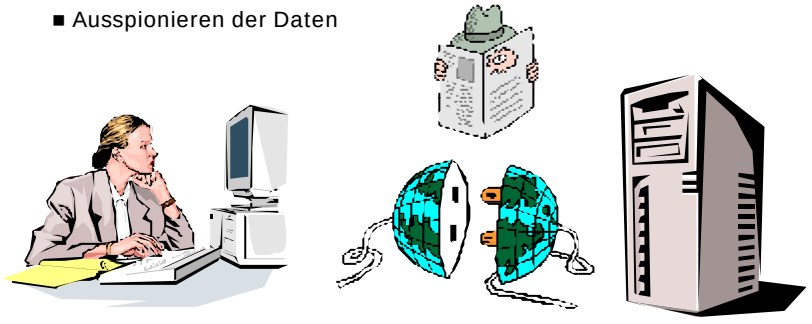
iTSEC

5

Angriff über das Netzwerk

Mögliche Angriffe

- Ausspähen von Anmeldeinformationen
- Unauthorisierte Änderung der Daten
- Nicht authentifizierbarer Absender der Daten
- Ausspionieren der Daten



SECUDE e-security for e-business

iTSEC

6

Rezept im Netz

1. Wie man ein SAP hacken kann und dabei seinen Spaß hat

1 Kids, don't do that at home. Allerdings benutzen wir nur Standardtechniken, die jedem Admin lange bekannt sind.

1.1. Hacken mit Unix/Netzwerk-Mitteln

Wir wissen nichts (außer, dass es ein SAP R/3 geben soll - die Chancen für eine Oracle-Datenbank sind gut) und haben einen Laptop dabei. Zufälligerweise finden wir eine beschaltete Netzwerkdose (oder klemmen uns mit einem Mini-Hub zusätzlich an). Und dann lauschen wir auf das, was da kommt.

SAP R/3 Systeme können auf vielen verschiedenen Ports verfügbar sein. In der Regel findet man die Applikationsserver auf einem Port zwischen 3200 und 3299, den Message-Server zwischen 3600 und 3699. Die letzten zwei Stellen sind üblicherweise die sogenannte Systemnummer. Man kann diese Ports zwar in den Profiles ändern, man kann aber davon ausgehen, dass die meisten Systeme in dieser Konfiguration betrieben werden. Die Abbildung 1 zeigt ein Beispiel für den Aufruf von **tcpdump**, es gibt aber noch andere Tools.

Abbildung 1. Packet-Sniffer

```
#!/bin/sh
tcpdump -n -i eth0 'tcp[13] & 3 != 0 and \
                   (( tcp[2:2] >= 3200 tcp[2:2] < 3300) or \
 5                  ( tcp[2:2] >= 3600 tcp[2:2] < 3700))'
```

Quelle: http://www.lan-ks.de/~jochen/sap-r3/ora-hack.html

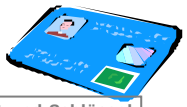
Single Sign-On via Smartcard

Single Sign-On

Zertifikat → Windows 2000 Netzwerk

Zertifikat → SAP R/3 Server

Freischalten über Passwort



Zertifikat und Schlüssel

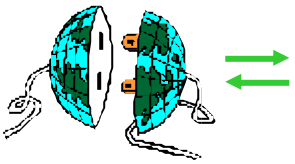
SECUDE e-security for e-business

ITSEC

9

Secure Network Communication

Tiefe Integration



Workprocess

Protocol

Compression

SNC

GSS API
Generic Security Services

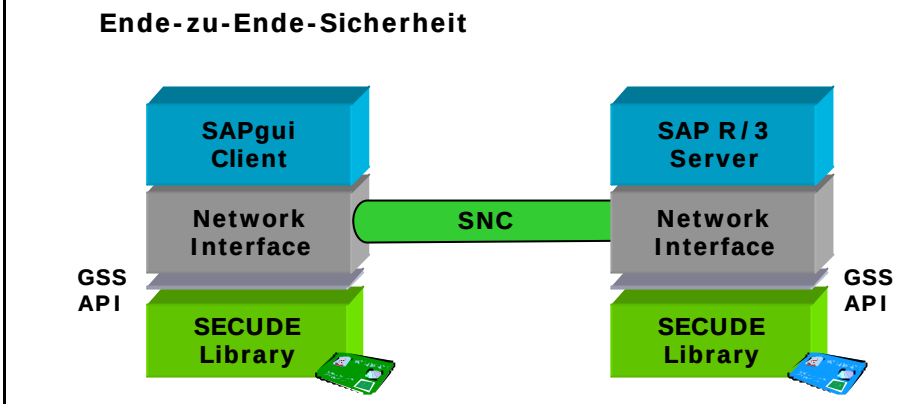
SECUDE Library

SECUDE e-security for e-business

ITSEC

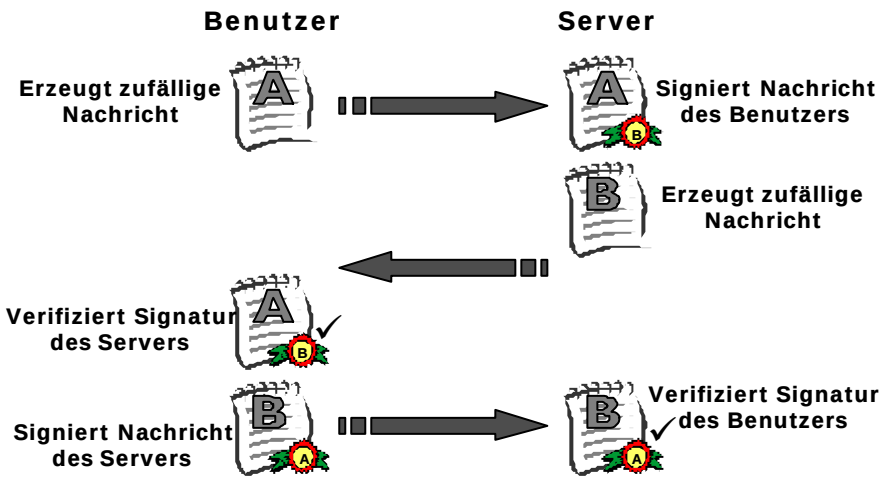
10

Sicheres SAP-Netz



11

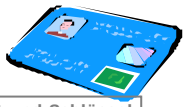
Starke Authentifikation



12

Single Sign-On

Freischalten über Passwort



Zertifikat und Schlüssel

App	User-ID	Passwort
1	xxx	xxx
2	yyy	yyy
3	zzz	zzz

Zertifikat → Windows 2000 Netzwerk

Zertifikat → SAP R/3 Server

User-ID/PWD → Windows NT Netzwerk

User-ID/PWD →
- Host
- Lotus Notes
- ...

SECUDE e-security for e-business

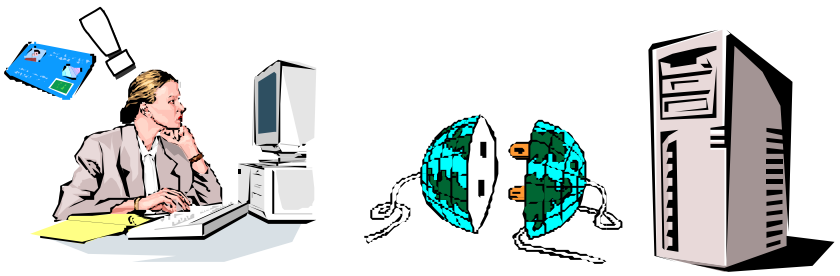
iTSEC

13

Sicherheitsfaktor Smartcard

Passwortcontainer Smartcard

- Kein Vergessen von Passworten
- Zufällige Wahl der Passworte
- Regelmässiger Wechsel der Passworte
- Vergabe von verschiedenen Passworten für verschiedene Systeme



SECUDE e-security for e-business

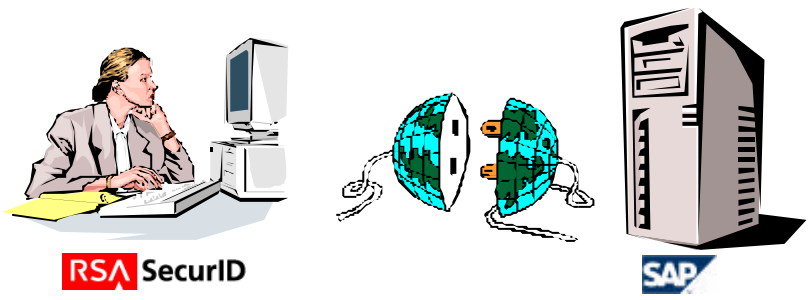
iTSEC

14

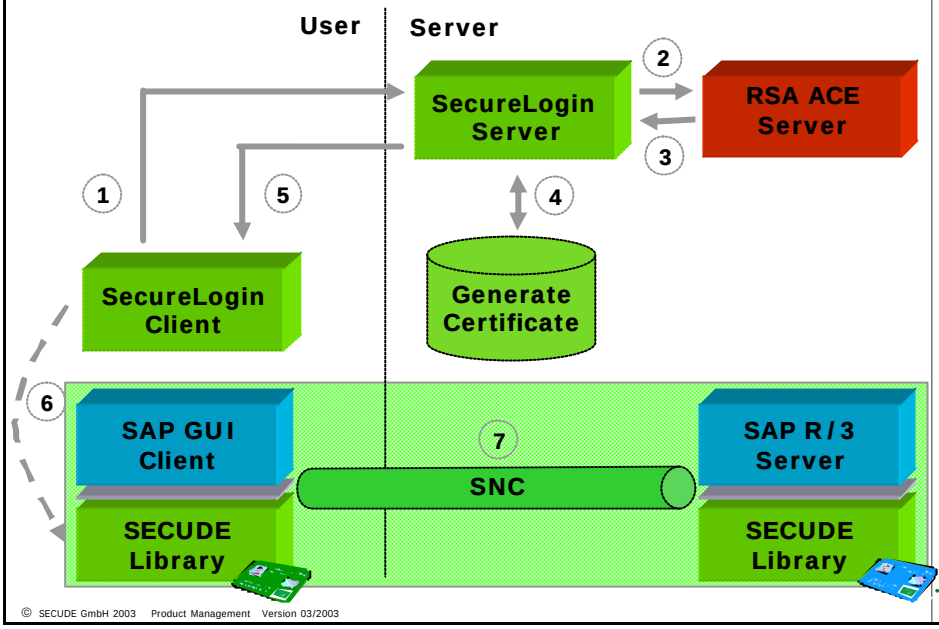
Single Sign-On
via RSA SecurID

Anforderung

- **Verwendung des bereits im Einsatz befindlichen Authentisierungssytems RSA SecurID zur Anmeldung am SAP R/3 Server.**



Architektur der SecurID-Lösung

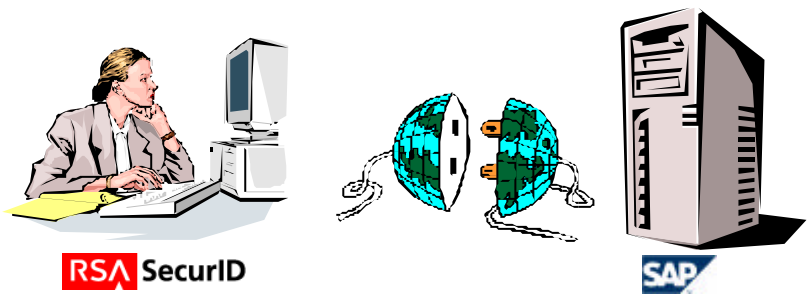


© SECUDE GmbH 2003 Product Management Version 03/2003

17

Vorteile

- Investitionsschutz durch Einsatz eines vorhandenen Authentisierungsverfahrens
- Rollout einer PKI nicht nötig
- Anmeldung mit dynamischen Passworten
- Benutzerakzeptanz bereits vorhanden
- Geringer Administrationsaufwand



© SECUDE GmbH 2003 Product Management Version 03/2003

18

Return on Invest durch Single Sign-On Lösung am Beispiel UBS AG

Studien

Kosten für vergessene Passworte

- Gartner Group:
  Jeder Anruf aufgrund eines vergessenes Passwortes kostet 20$.
- PriceWaterhouse Coopers:
  40% aller Helpdesk-Anrufe beziehen sich auf vergessene Passworte. Die Kosten liegen bei 210$ pro Benutzer und Jahr.
- Compaq:
  30% aller Helpdesk-Anrufe beziehen sich auf vergessene Passworte. Ein Anruf kostet zwischen 35$ und 75$.

Return On Invest: UBS AG

Ausgangssituation

- 300 unterschiedliche Applikationen sind bei der UBS im Einsatz.
- 8.700 von 10.000 Anrufen am Helpdesk pro Monat beziehen sich auf Passwortprobleme.
- 15min beträgt die Arbeitszeit für die Lösung eines Passwort-problems (HelpDesk und Mitarbeiter).
- Das verursacht 2 Mio € Kosten pro Jahr.

UBS

SECUDE e-security for e-business

ITSEC

21

Return On Invest: UBS AG

Umsetzung

- 40 Applikationen sind mit Single Sign-On ausgestattet, davon 50% zertifikatsbasiert.
- Nach 18 Monaten sind von 10.000 Anrufen am Helpdesk 5.080 passwortbezogen. Dies entspricht einem Rückgang von 40%.
- Eine Auswertung der UBS hat ergeben, dass im Jahr 2001 ca 2.4 Mio € Kosten eingespart wurden.

UBS

SECUDE e-security for e-business

ITSEC

22

Q & A

www.secude.com
info@secude.com

SOFTWARE SAP PARTNER

SECUDE e-security for e-business

.ITSEC

23