



## **T.I.S.P. Community Meeting**

**Berlin, 02. - 03.11.2015**

# **SAP Live Hacking**

**Christian Thiemann**

**Atos IT Solutions and Services GmbH**

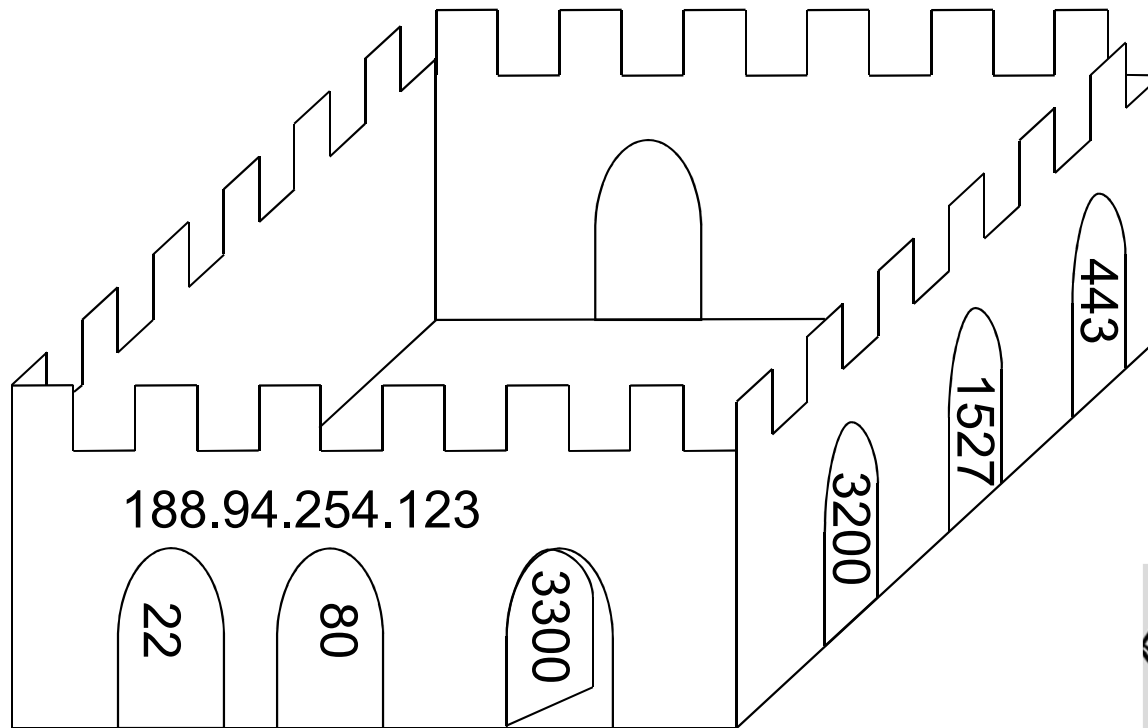
# Top 11 SAP Schwachstellen

## Top problems by BIZEC

- BIZEC TEC-01: Vulnerable Software in Use
- BIZEC TEC-02: Standard Users with Default Passwords
- **BIZEC TEC-03: Unsecured SAP Gateway**
- BIZEC TEC-04: Unsecured SAP/Oracle authentication
- BIZEC TEC-05: Insecure RFC interfaces
- BIZEC TEC-06: Insufficient Security Audit Logging
- BIZEC TEC-07: Unsecured SAP Message Server
- BIZEC TEC-08: Dangerous SAP Web Applications
- BIZEC TEC-09: Unprotected Access to Administration Services
- BIZEC TEC-10: Insecure Network Environment
- BIZEC TEC-11: Unencrypted Communications

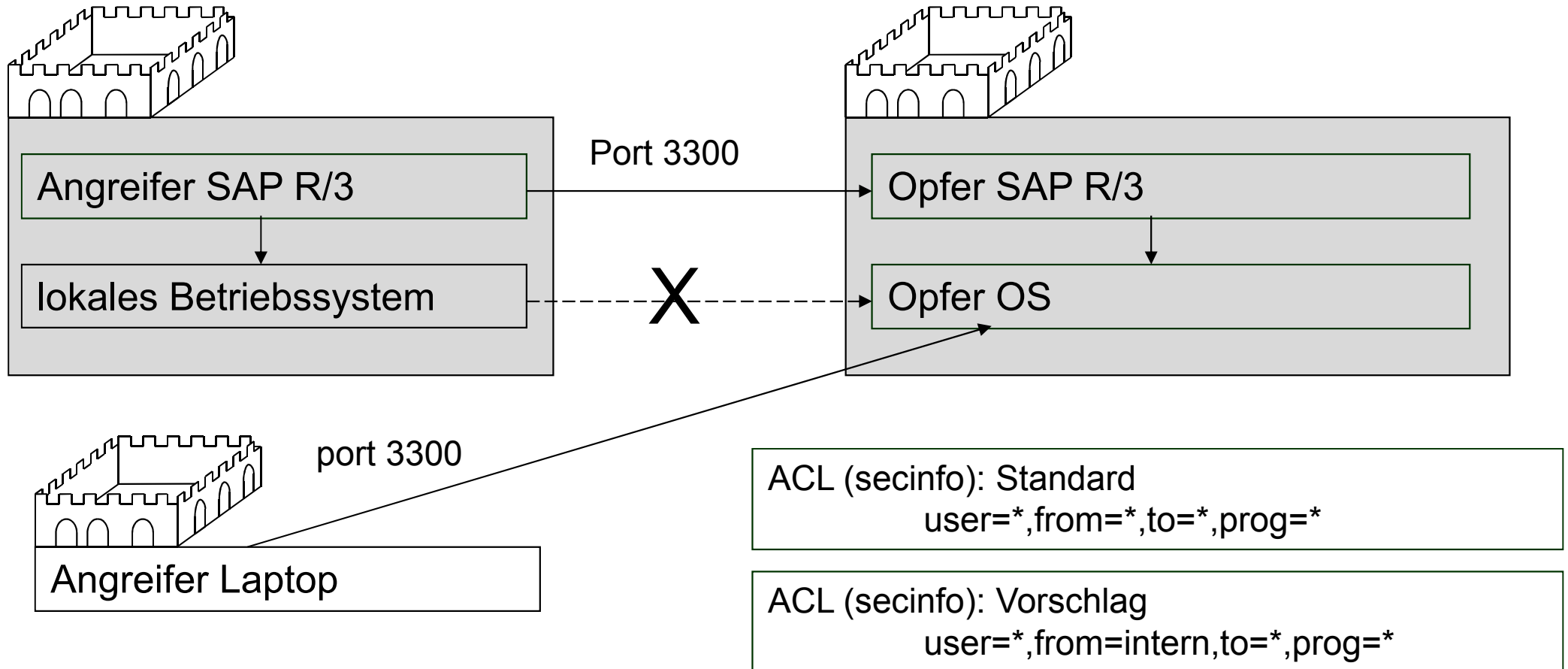
Quelle: <http://www.bizec.org>

# Angriff auf ein System



# Start externer Programme

via RFC



# Test mit R/3 – Transaktion SM59

The screenshot shows the SAP transaction SM59 configuration for an RFC destination. A context menu is open over the 'Gateway options' field, with an arrow pointing to the 'Gateway options' field in the main configuration window. The 'Gateway options' field is highlighted in yellow. The 'Gateway options' dialog box is also open, showing the 'Gateway service' field highlighted in yellow. The 'Gateway service' field contains the value '3300'. The 'Gateway host' field contains the value 'victim'. The 'RFC destination' field contains the value 'ZVICTIM'. The 'Type' field contains the value 'TCP/IP connection'. The 'Start on' section has 'Application server' selected. The 'Explicit host' section has 'Program' set to 'sapxpg', 'Target host' set to 'localhost', and 'Save as' set to 'IP address' with the value '127.0.0.1'.

Destination System information Test System Help

Other destination  
Change Ctrl+S  
Create  
Copy  
Delete Shift+F2  
Gateway options  
IRFC options  
MQS options  
SNC options  
Exit Shift+F3

CTIM Gateway

Connection type T TCP/IP connection

Activation Type Start Registration Trace

Start on  
Application server Explicit host Front-end workstation

Explicit host  
Program sapxpg  
Target host localhost  
Save as HostName IP address 127.0.0.1

RFC Destination ZVICTIM

RFC destination ZVICTIM

Type T TCP/IP connection

Gateway host victim

Gateway service 3300

O.K. Delete

## Test mit rfcsdk

```
#include <stdio.h>
#include <saprfc.h>
int main()
{
    RFC_HANDLE rfc_handle;
    RFC_ERROR_INFO_EX error_info;
    rfc_handle = RfcOpenEx ("TYPE=E GWHOST=victim GWSERV=3300
                            TPHOST=localhost TPNAME=sapxpg", &error_info);
    if (rfc_handle == RFC_HANDLE_NULL)
    {
        printf ("Key          %s\n", error_info.key); */
        printf ("Message       %s\n\n", error_info.message);
    }
    else
    {
        printf ("Secinfo not restrictive. Start of arbitrary external
programs possible.\n");
        RfcClose(rfc_handle);
    }
}
```

## Start externer Programme

- Start beliebiger Programme
- Stop von SAP
- Mandanten löschen
- Umgehung des SAP Transportsystems
- Export und Veränderung von Daten
- Erstellen neuer R/3 Benutzer
- Ändern von R/3 Passwörtern
  
- keine Spuren

## Exploit via RFC

---

# ■ DEMO



# Risikobehandlung

- Prüfen



Existiert das Risiko

- Akzeptieren



Geringes Restrisiko

- Transferieren



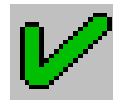
Versicherung

- Ignorieren



es ist uns egal

- Beheben



---

# Christian Thiemann

christian.thiemann@atos.net