



Ubiquitous IT Security – Warum die Firewall nicht schützen konnte

Patrick Hof – patrick.hof@redteam-pentesting.de
RedTeam Pentesting GmbH

Sicherheit 2008, Saarbrücken, 4. April 2008



Über den Autor

Patrick Hof

- ★ RedTeam Pentesting GmbH
- ★ Spezialisierung auf Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit





Penetrationstests

- ★ **Penetrationstest:** Sicherheitsüberprüfung eines IT-Systems durch einen kontrollierten Angriff
- ★ **Arten von Penetrationstests**
 - ★ *Produktpenetrationstests:* Überprüfung eines (sicherheitsrelevanten) Produkts auf Schwachstellen
 - ★ *Netzwerkpenetrationstests:* Kontrollierter Angriff auf ein Firmennetzwerk oder zumindest Teile davon



Ubiquitous IT Security

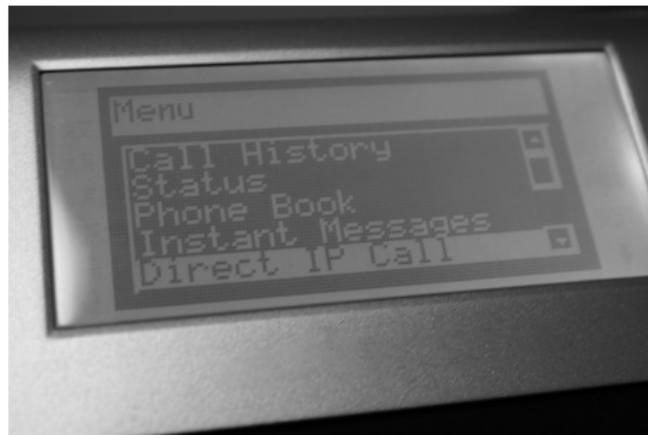
- ★ Ubiquitous IT Security – „Allgegenwärtige IT-Sicherheit“
- ★ Ein IT-System ist nicht nur der Inhalt des Serverraums
- ★ IT-Sicherheit muss für das Gesamtsystem gelten – die Firewall allein hilft nicht





Voice over IP

- ★ Viele Firmen setzen bereits VoIP ein
- ★ Die anderen migrieren gerade



Jean-Etienne Poirrier



Voice over IP

VoIP-Geräte haben neue
Funktionalitäten – und Risiken:

„Push Audio“

- ★ Senden von Audio-Daten
an die Endgeräte, welche
automatisch abgespielt
werden



Jean-Etienne Poirrier

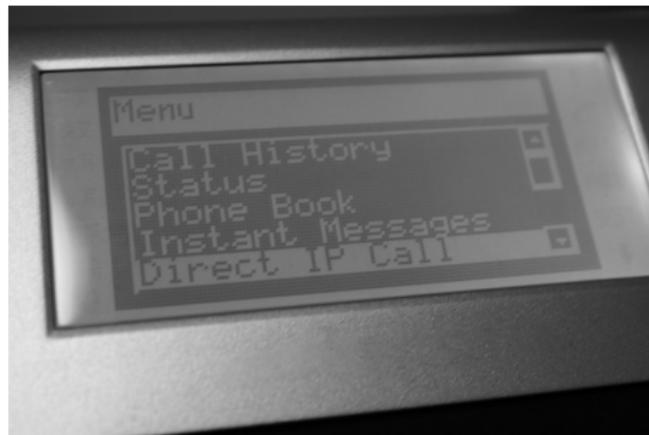


Voice over IP

VoIP-Geräte haben neue
Funktionalitäten – und Risiken:

„Push Audio“

- ★ Senden von Audio-Daten
an die Endgeräte, welche
automatisch abgespielt
werden
- ★ z.B. Feueralarm...



Jean-Etienne Poirrier



Voice over IP

VoIP-Geräte haben neue
Funktionalitäten – und Risiken:
Anpassbare Bildschirmmenüs



Jean-Etienne Poirrier

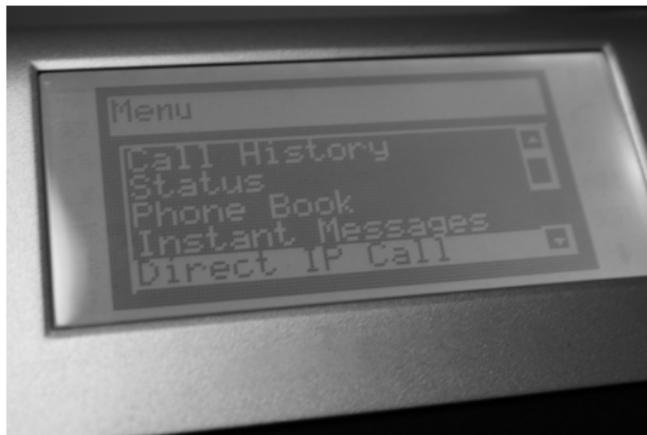


Voice over IP

VoIP-Geräte haben neue
Funktionalitäten – und Risiken:

Anpassbare Bildschirmmenüs

- ★ „Phishing“ auf dem
Telefondisplay
- ★ Rufumleitung aktiviert –
und wohin?



Jean-Etienne Poirrier



Voice over IP

VoIP-Geräte haben neue
Funktionalitäten – und Risiken:

*Fernsteuerung der
Bedienelemente*



Jean-Etienne Poirrier

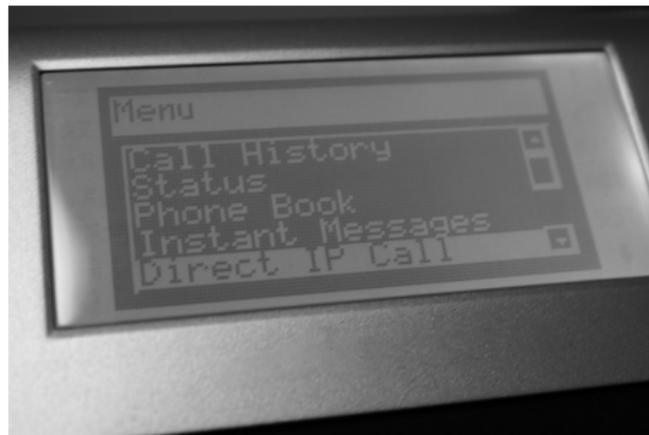


Voice over IP

VoIP-Geräte haben neue
Funktionalitäten – und Risiken:

*Fernsteuerung der
Bedienelemente*

- ★ Abhören per
Konferenzschaltung
- ★ Umleiten von Telefonaten



Jean-Etienne Poirrier



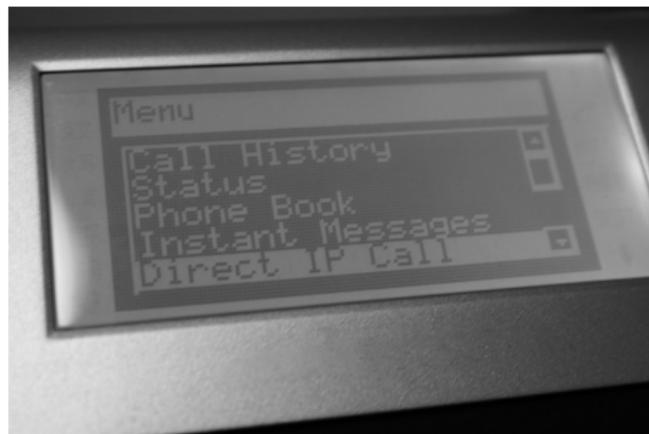
Voice over IP

VoIP-Geräte haben neue
Funktionalitäten – und Risiken:

Fernsteuerung der Bedienelemente

- ★ Abhören per
Konferenzschaltung
- ★ Umleiten von Telefonaten

Was macht Ihr Telefon so,
wenn Sie nicht hinschauen?



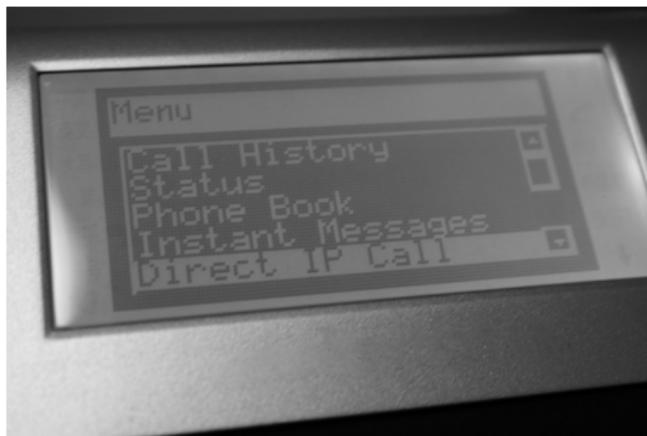
Jean-Etienne Poirrier



Voice over IP

VoIP-Geräte haben neue
Funktionalitäten – und Risiken:

Gute Mikrofone



Jean-Etienne Poirrier



Voice over IP

VoIP-Geräte haben neue
Funktionalitäten – und Risiken:

Gute Mikrofone

- ★ Einschalten der Freisprecheinrichtung
- ★ ⇒ Raumüberwachung per Telefon



Jean-Etienne Poirrier



Fax, Drucker & Co.

Faxgeräte

- ★ Gern genutzt zur „out-of-band“-Kommunikation
- ★ Sicheres Übertragungsmedium für sensible Daten?





Fax, Drucker & Co.

Fallbeispiel

- ★ Kunde mit großem SAP-System
- ★ Zugangsdaten werden zur Sicherheit per Fax versandt – handschriftlich eingetragen





Fax, Drucker & Co.

Fallbeispiel

- ★ Kunde mit großem SAP-System
- ★ Zugangsdaten werden zur Sicherheit per Fax versandt – handschriftlich eingetragen
- ★ Problem: Faxe werden automatisch gescannt und archiviert. . .





Überwachungskameras

Überwachungskameras (CCTV)

- ★ Gebäudesicherung
- ★ TCP/IP-basierte
Netzwerkcameras
- ★ Funktionalität z.B.:
 - ★ Webserver
 - ★ FTP-Server
 - ★ E-Mail
 - ★ SMS





Überwachungskameras

Sicherheitsproblem: Kameras oft
frei zugänglich

Fallbeispiel

- ★ Kamera in frei zugänglicher
Sicherheitsschleuse





Überwachungskameras

Sicherheitsproblem: Kameras oft frei zugänglich

Fallbeispiel

- ★ Kamera in frei zugänglicher Sicherheitsschleuse
- ★ direktes Kabel ins interne Netz





Überwachungskameras

Sicherheitsproblem: Kameras oft
frei zugänglich

Fallbeispiel

- ★ Kamera direkt auf Pinpad zur Zugangskontrolle gerichtet
- ★ Ausfall der Kamera nach Exploit wird tagelang nicht behoben





Überwachungskameras



Brett Taylor



Diskussion

Vielen Dank!