Penetration Testing – Praxis and Beyond

Jens Liebchen – jens.liebchen@redteam-pentesting.de
RedTeam Pentesting GmbH

Berufsakademie Mannheim, 10. April 2008

Über den Autor

Jens Liebchen

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

Penetrationstests

Penetrationstest

Ein *Penetrationstest* bezeichnet die 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

Penetrationstests

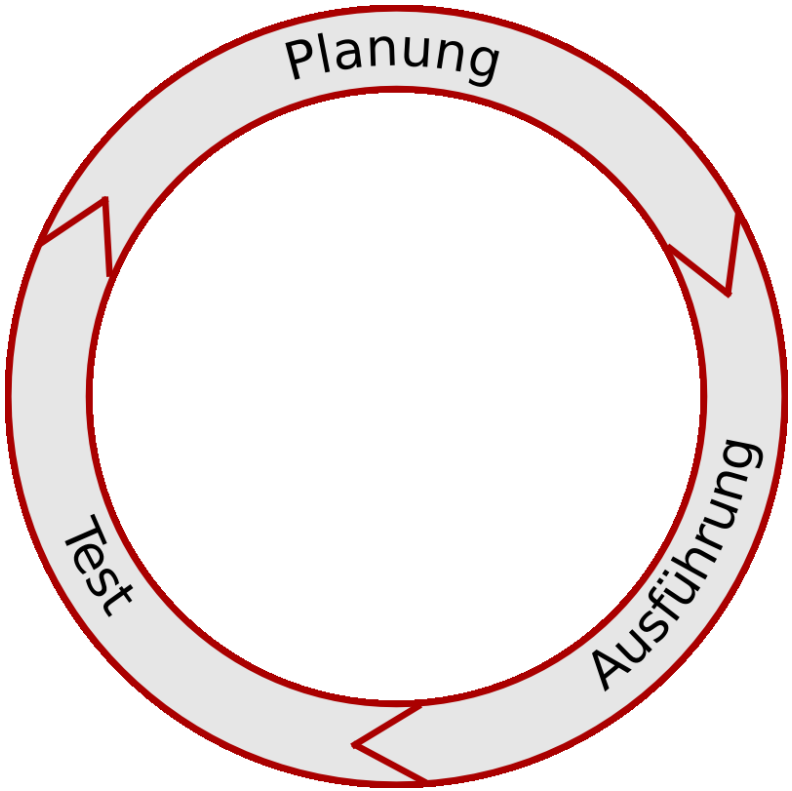
Penetrationstest

Ein *Penetrationstest* bezeichnet die Sicherheitsüberprüfung eines IT-Systems durch einen kontrollierten Angriff.

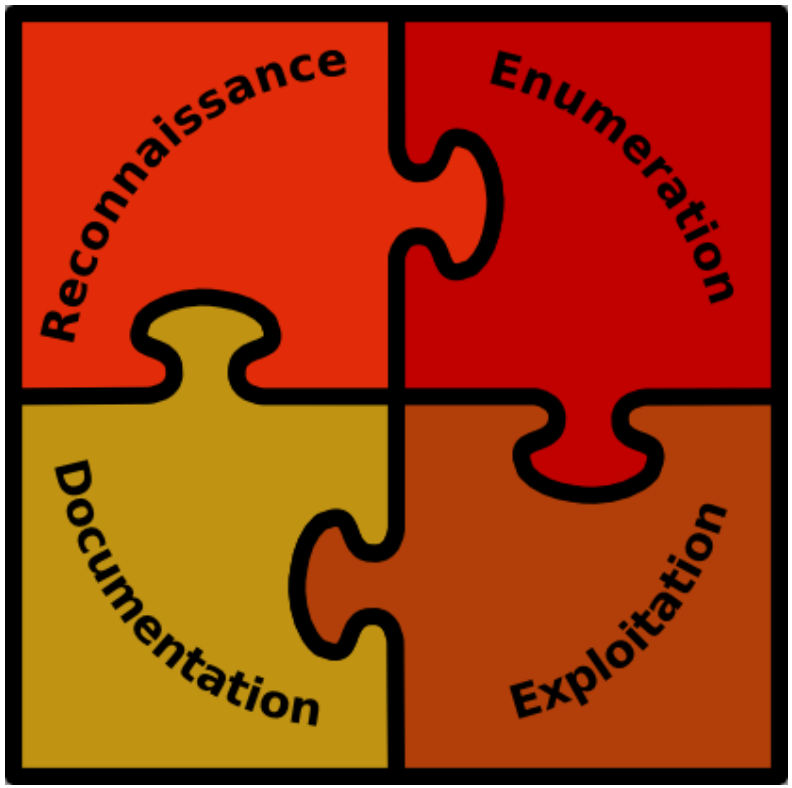
Arten von Penetrationstests

- ★ *Produktpenetrationstests*: Überprüfung eines (sicherheitsrelevanten) Produkts auf Schwachstellen
- ★ *Netzwerkpenetrationstests*: Kontrollierter Angriff auf ein Firmennetzwerk oder zumindest Teile davon

Einordnung Penetrationstests



Phasen eines Penetrationstests



Aus der Praxis...

IT-Sicherheit ist mehr als die neuesten Exploits und Patches.

- ★ Fallbeispiele aus der Praxis von Pentests
- ★ Keine typischen technischen Fehler (Buffer Overflows, SQL-Injections, XSS, ...)
- ★ Stattdessen: Ungewöhnliche, aber häufig vorkommende und leicht zu behebende Fehler
- ★ Ziel: Erkennen solcher Fehler!

Aus der Praxis...

IT-Sicherheit ist mehr als die neuesten Exploits und Patches.

- ★ Fallbeispiele aus der Praxis von Pentests
- ★ Keine typischen technischen Fehler (Buffer Overflows, SQL-Injections, XSS, . . .)
- ★ Stattdessen: Ungewöhnliche, aber häufig vorkommende und leicht zu behebende Fehler
- ★ Ziel: Erkennen solcher Fehler!

Die Sache mit dem Stress – Incident Response

Die Sache mit dem Stress – Incident Response

- ★ Erschreckend wenig standardisierte Abläufe in der Praxis
- ★ Stress ist unglaublich hoch, sofern man nicht täglich mit (erfolgreichen) Angriffen zu tun hat

Die Sache mit dem Stress – Incident Response

- Administrator beauftragt Penetrationtest
- Nach 24h Kompromittierung des Corerouters (von innen) durch die Pentester
- Administrator so unter Stress, dass er nicht in der Lage ist, die aufgefallene Kompromittierung mit dem selbst beauftragten Pentest in Verbindung zu bringen

Die Sache mit dem Stress – Incident Response

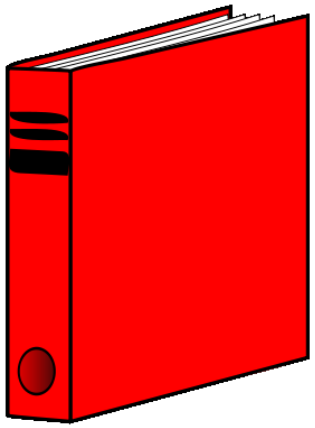
- ★ Administrator beauftragt Penetrationtest
- ★ Nach 24h Kompromittierung des Corerouters (von innen) durch die Pentester
- ★ Administrator so unter Stress, dass er nicht in der Lage ist, die aufgefallene Kompromittierung mit dem selbst beauftragten Pentest in Verbindung zu bringen

Die Sache mit dem Stress – Incident Response

- ★ Administrator beauftragt Penetrationtest
- ★ Nach 24h Kompromittierung des Corerouters (von innen) durch die Pentester
- ★ Administrator so unter Stress, dass er nicht in der Lage ist, die aufgefallene Kompromittierung mit dem selbst beauftragten Pentest in Verbindung zu bringen

Die Sache mit dem Stress – Incident Response

- Roter Ordner
- Zumindest erste Handlungsmöglichkeiten beschreiben
- Rechte genau definieren:
  - Darf ein Administrator das Netzwerk abschalten?
  - Darf der Geschäftsführer an Weihnachten um Mitternacht angerufen werden?
  - ...

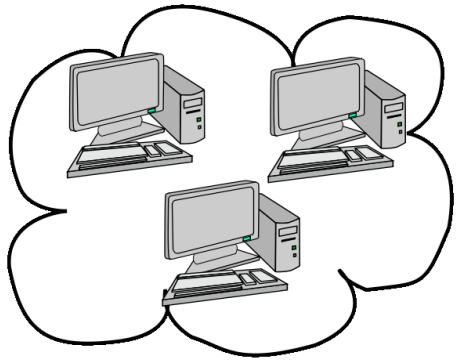


Administratoren können mehr. . . (als man glaubt)

- ★ Viele Administratoren erledigen seit langer Zeit Alltagsaufgaben
- ★ Schulungen und Konferenzen werden häufig nicht bezahlt oder es fehlt die Zeit („Dann fällt der Administrator für diese Zeit aus. . . “)
- ★ Administratoren entwickeln „ungewöhnliche“ Lösungen für ihre Probleme

Administratoren können mehr. . . (als man glaubt)

- ★ Administrator mit $>$ 10 Jahren Unixerfahrung
- ★ Entwickelt „Reimplementierung“ von NIS, um Passwörter auf Workstations zu verteilen
- ★ Leider nicht wirklich sicherer als das Original



Administratoren können mehr. . . (als man glaubt)

- ★ Betrachtet man den Entwicklungsaufwand, so wäre eine regelmäßige Schulung und ein Austausch mit Kollegen billiger gewesen
- ★ Standardfehler wären vermieden worden
- ★ Faktor Administratoren für Betriebserfolg leider häufig unterschätzt

Auffälliger geht's nicht?

- ★ Einer der meist gehörten Sätze in Besprechungen von Penetrationtests: „Aber das fällt doch auf?“
- ★ In der Praxis fällt leider nur sehr wenig auf
- ★ Häufige Reaktion auf technische Auffälligkeiten: Reboot

Auffälliger geht's nicht?

- ★ Sommer, knapp 30°C: Drei Pentester im Auto mit Laptops, direkt vor dem Firmeneingang
- ★ 2 Stunden später: Zahlreichen Mitarbeitern der Firma ist das Auto aufgefallen, niemand meldet es (wohin auch?); bei der Firma auf der gegenüberliegenden Seite sammeln sich auffällig viele Mitarbeiter auf der Dachterasse
- ★ Nach 3 Stunden ist der WLAN-Scan abgeschlossen. Die IT-Abteilung oder die Sicherheitsbeauftragten haben keinen Hinweis über das auffällige Verhalten bekommen

Auffälliger geht's nicht?

- ★ Sommer, knapp 30°C: Drei Pentester im Auto mit Laptops, direkt vor dem Firmeneingang
- ★ 2 Stunden später: Zahlreichen Mitarbeitern der Firma ist das Auto aufgefallen, niemand meldet es (wohin auch?); bei der Firma auf der gegenüberliegenden Seite sammeln sich auffällig viele Mitarbeiter auf der Dachterasse
- ★ Nach 3 Stunden ist der WLAN-Scan abgeschlossen. Die IT-Abteilung oder die Sicherheitsbeauftragten haben keinen Hinweis über das auffällige Verhalten bekommen

Auffälliger geht's nicht?

- ★ Sommer, knapp 30°C: Drei Pentester im Auto mit Laptops, direkt vor dem Firmeneingang
- ★ 2 Stunden später: Zahlreichen Mitarbeitern der Firma ist das Auto aufgefallen, niemand meldet es (wohin auch?); bei der Firma auf der gegenüberliegenden Seite sammeln sich auffällig viele Mitarbeiter auf der Dachterasse
- ★ Nach 3 Stunden ist der WLAN-Scan abgeschlossen. Die IT-Abteilung oder die Sicherheitsbeauftragten haben keinen Hinweis über das auffällige Verhalten bekommen

Auffälliger geht's nicht?

- ★ Nachts, kurz nach Mitternacht: Pentester mit Laptop auf dem Firmengelände
- ★ Sicherheitsdienst greift ihn auf
- ★ Einzige Befürchtung des Sicherheitsdienstes: Laptop könnte gestohlen worden sein
- ★ Am nächsten Tag: Es wurde kein Laptop gestohlen gemeldet ⇒ Vorfall wird überhaupt nicht gemeldet

Auffälliger geht's nicht?

- ★ Nachts, kurz nach Mitternacht: Pentester mit Laptop auf dem Firmengelände
- ★ Sicherheitsdienst greift ihn auf
- ★ Einzige Befürchtung des Sicherheitsdienstes: Laptop könnte gestohlen worden sein
- ★ Am nächsten Tag: Es wurde kein Laptop gestohlen gemeldet ⇒ Vorfall wird überhaupt nicht gemeldet

Auffälliger geht's nicht?

- ★ Nachts, kurz nach Mitternacht: Pentester mit Laptop auf dem Firmengelände
- ★ Sicherheitsdienst greift ihn auf
- ★ Einzige Befürchtung des Sicherheitsdienstes: Laptop könnte gestohlen worden sein
- ★ Am nächsten Tag: Es wurde kein Laptop gestohlen gemeldet ⇒ Vorfall wird überhaupt nicht gemeldet

Auffälliger geht's nicht?

- ★ Nachts, kurz nach Mitternacht: Pentester mit Laptop auf dem Firmengelände
- ★ Sicherheitsdienst greift ihn auf
- ★ Einzige Befürchtung des Sicherheitsdienstes: Laptop könnte gestohlen worden sein
- ★ Am nächsten Tag: Es wurde kein Laptop gestohlen gemeldet ⇒ Vorfall wird überhaupt nicht gemeldet

Auffälliger geht's nicht?

- Nicht erwarten, dass Auffälliges bemerkt wird
- Stelle einrichten, wohin Auffälliges gemeldet werden soll
- Auffällig ist z.B.:
  - Unbekannte Personen im Firmengebäude
  - Auffällige Veränderungen am Netzwerk („Der Accesspoint hing da gestern noch nicht“)
  - Auffällige Emails (beliebt im Rahmen von Pentests: Scheinbewerbungen an HR mit „defektem Lebenslauf“ o.ä.)

Wer weiß, was Google weiß?

- ★ Suchmaschinen indizieren fast alle Daten
- ★ Viele Daten sind vertraulicher Natur
- ★ Einmal ins Internet geratene Daten sind kaum noch zu entfernen

Wer weiß, was Google weiß?

Im Rahmen von Pentests wurde unter anderem gefunden...

- ★ Ein Counterstrike-Server, der durch alle Firewalls hindurch erreichbar im internen Netz stand
- ★ Interne Datenbanken inkl. gültiger Logins
- ★ Interne Sicherheitsrichtlinien (z.B. Aufbau der genutzten Passwörter)
- ★ „Versteckte“ Webapplikationen und nicht mehr genutzte veraltete Skripte

Wer weiß, was Google weiß?

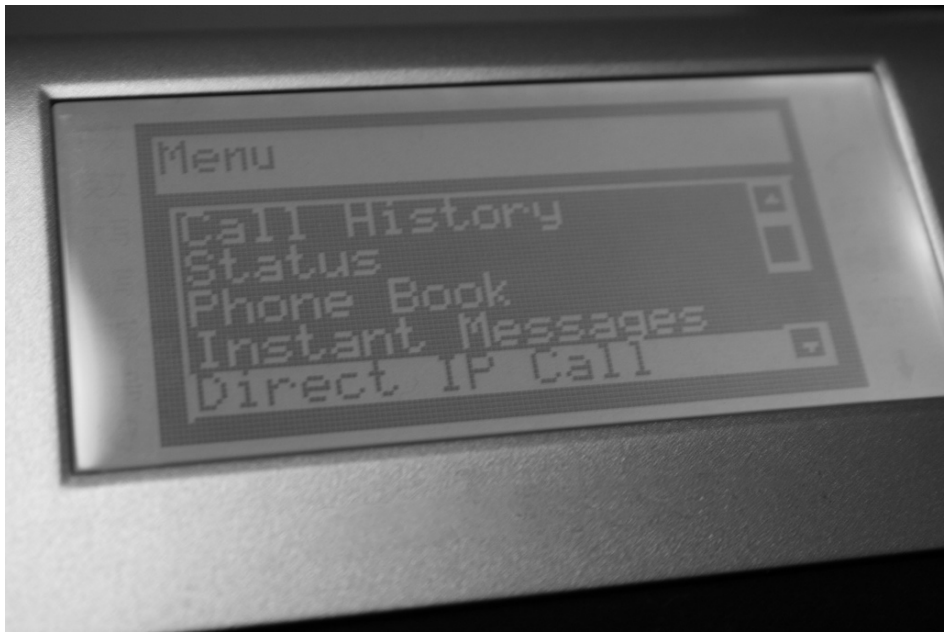
- ★ Regelmäßig nach eigenen IP-Adressbereichen und Domainnamen suchen
- ★ Lesenswert: `http://johnny.ihackstuff.com`
- ★ Überraschungen garantiert!

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



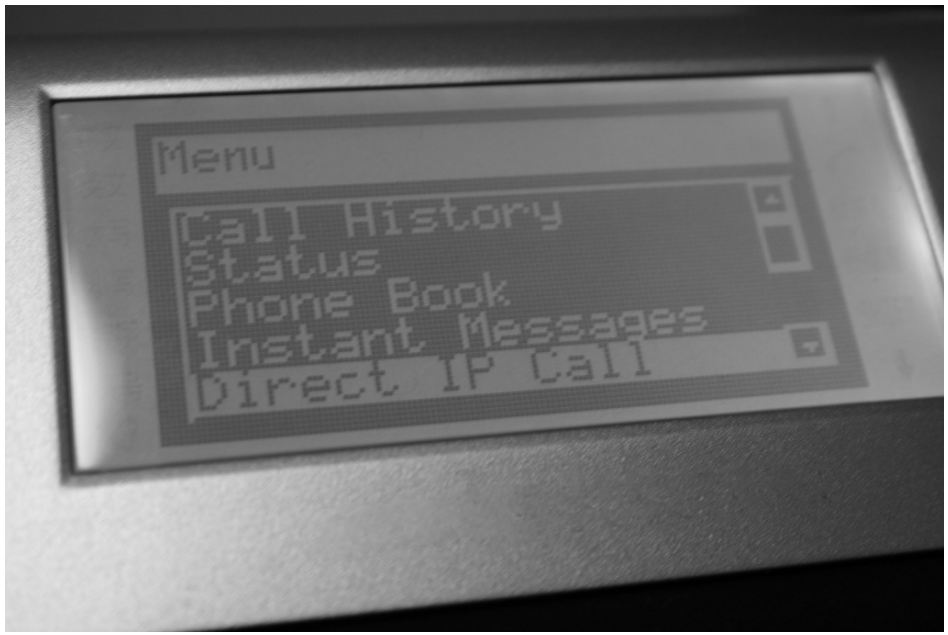
 Jean-Etienne Poirrier

Voice over IP

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

„Push Audio“

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



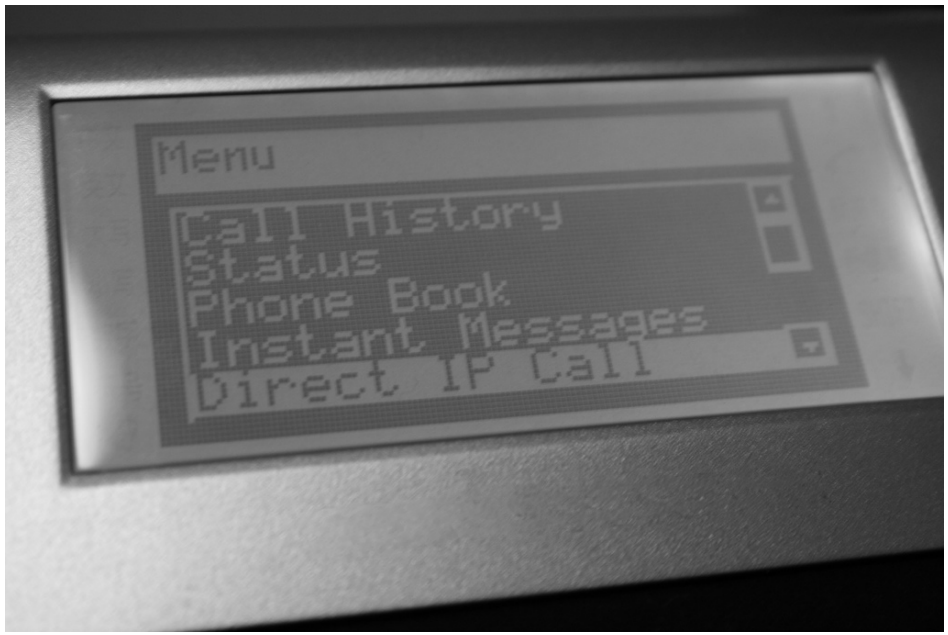
 Jean-Etienne Poirrier

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. . .

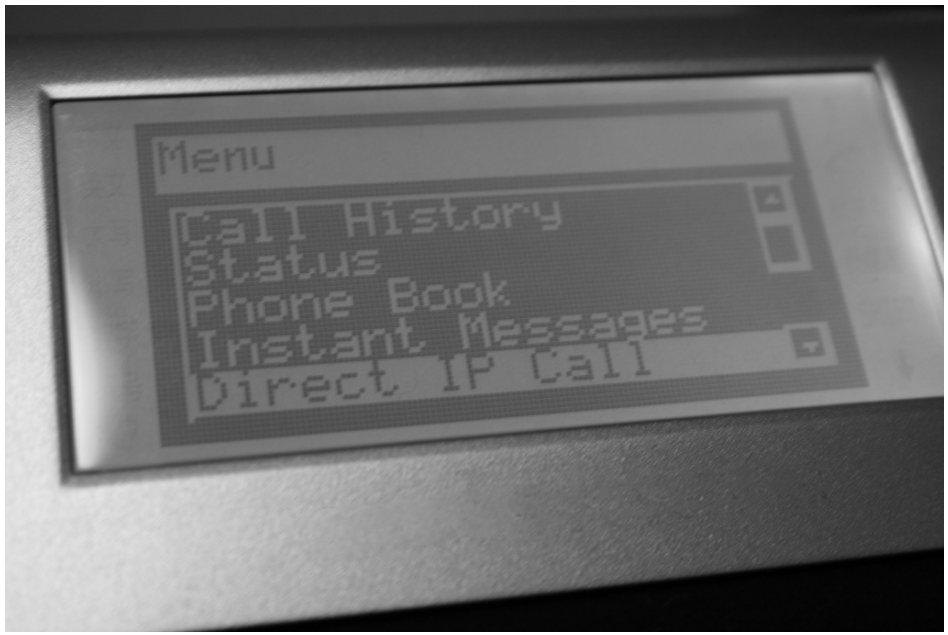


 Jean-Etienne Poirrier

Voice over IP

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Anpassbare Bildschirmmenüs



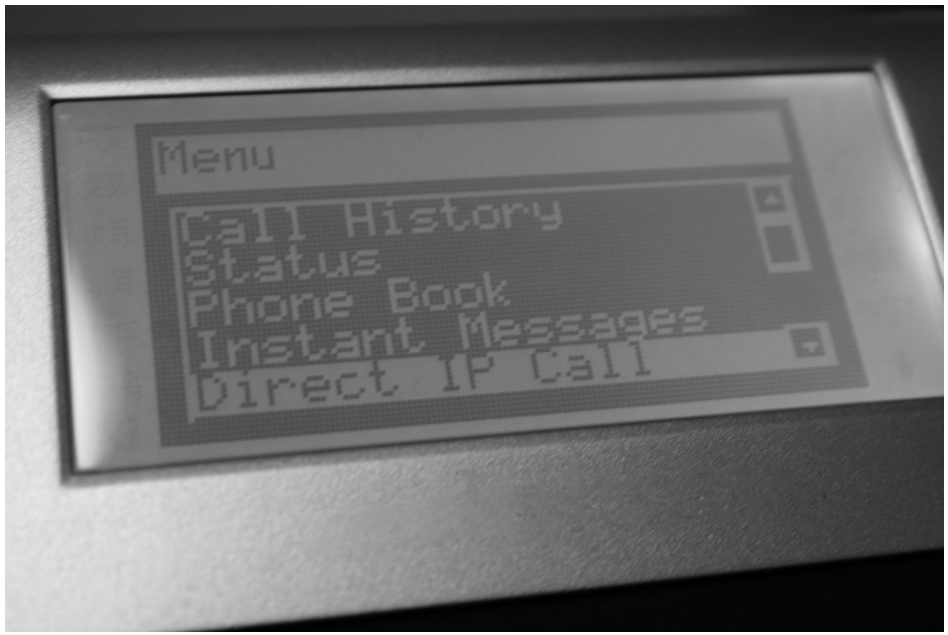
 Jean-Etienne Poirrier

Voice over IP

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Anpassbare Bildschirmmenüs

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

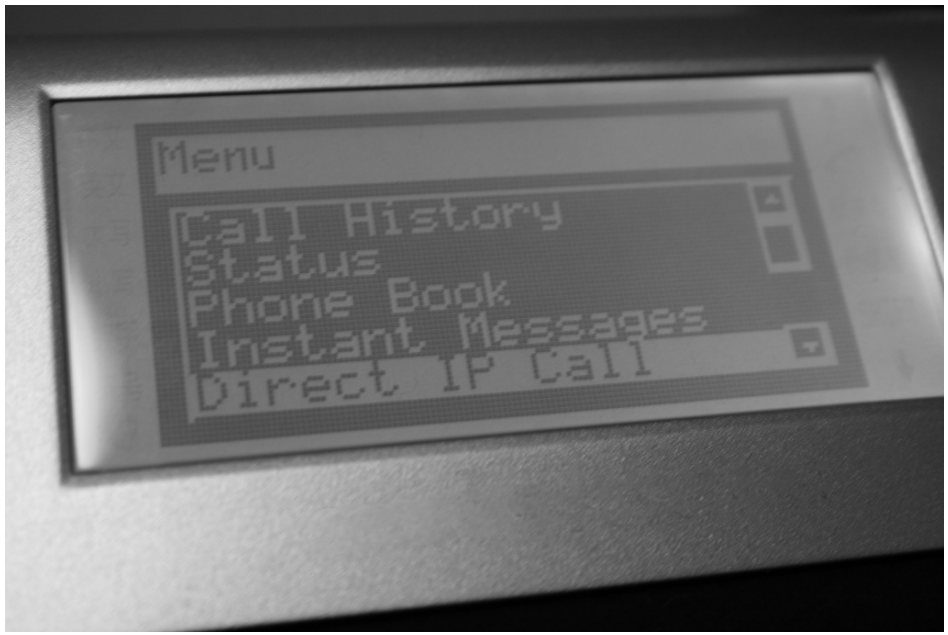


 Jean-Etienne Poirrier

Voice over IP

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Fernsteuerung der Bedienelemente



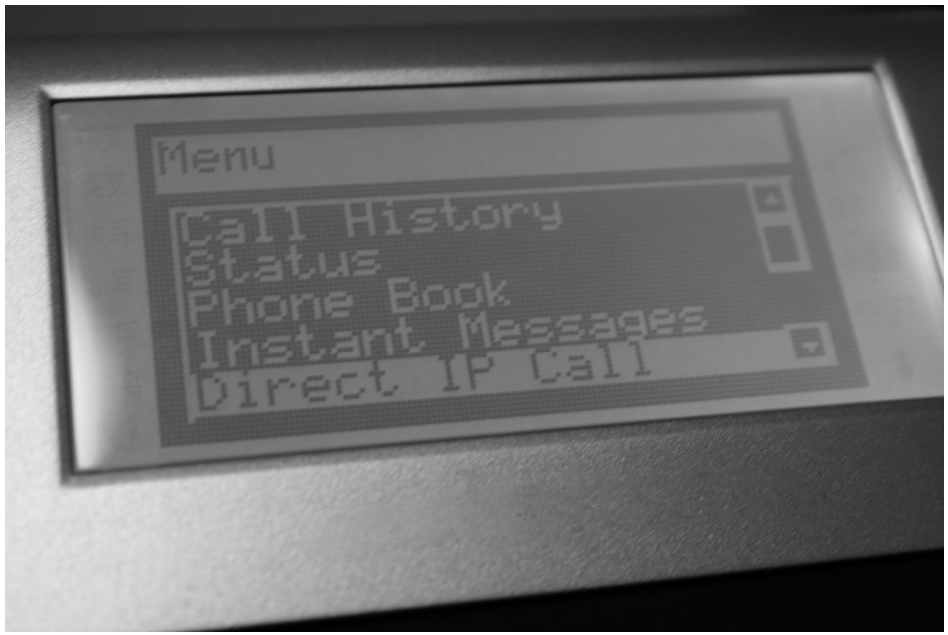
 Jean-Etienne Poirrier

Voice over IP

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Fernsteuerung der Bedienelemente

- ★ Abhören per Konferenzschaltung
- ★ Umleiten von Telefonaten



 Jean-Etienne Poirrier

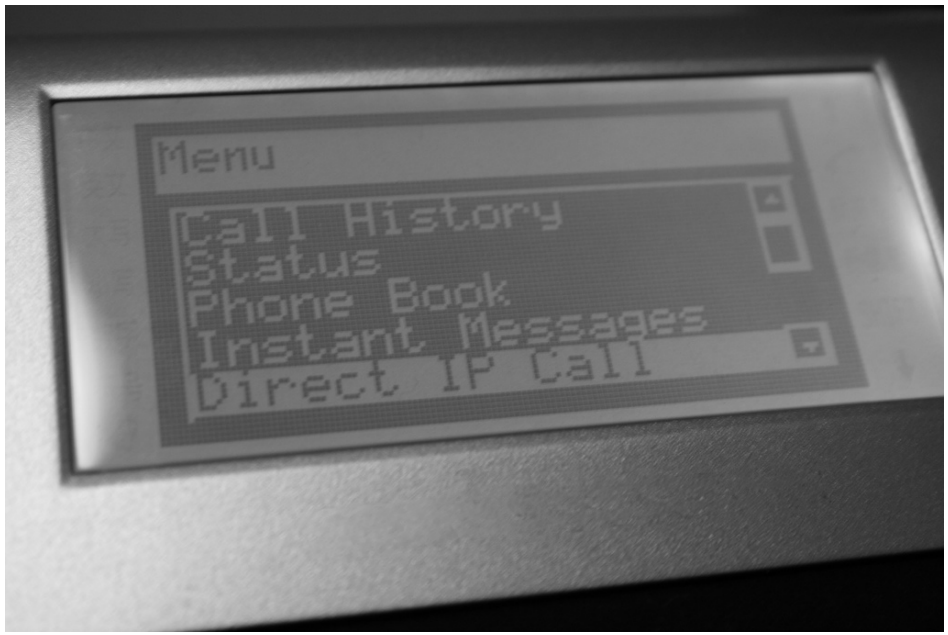
Voice over IP

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?

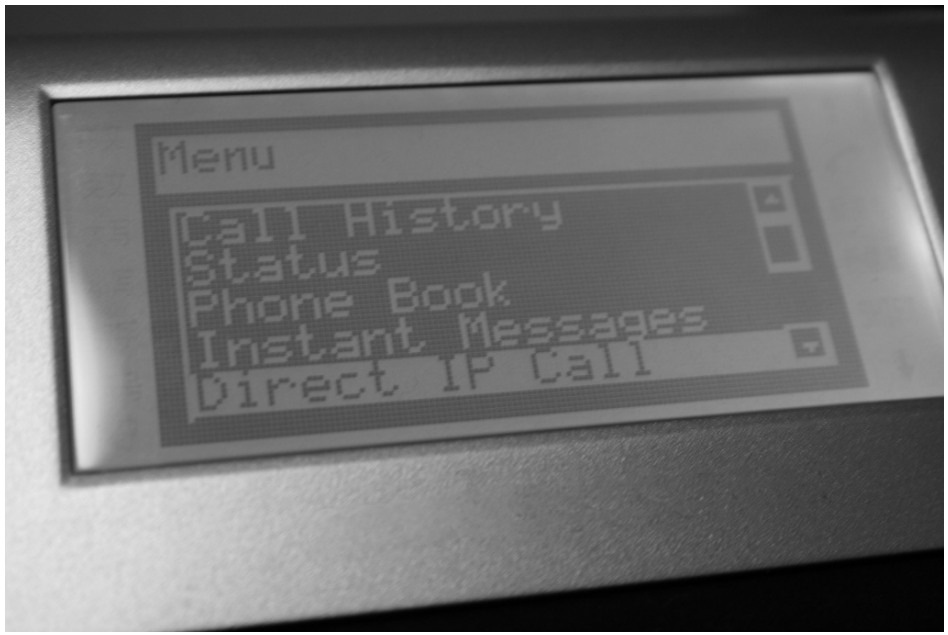


 Jean-Etienne Poirrier

Voice over IP

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Gute Mikrofone



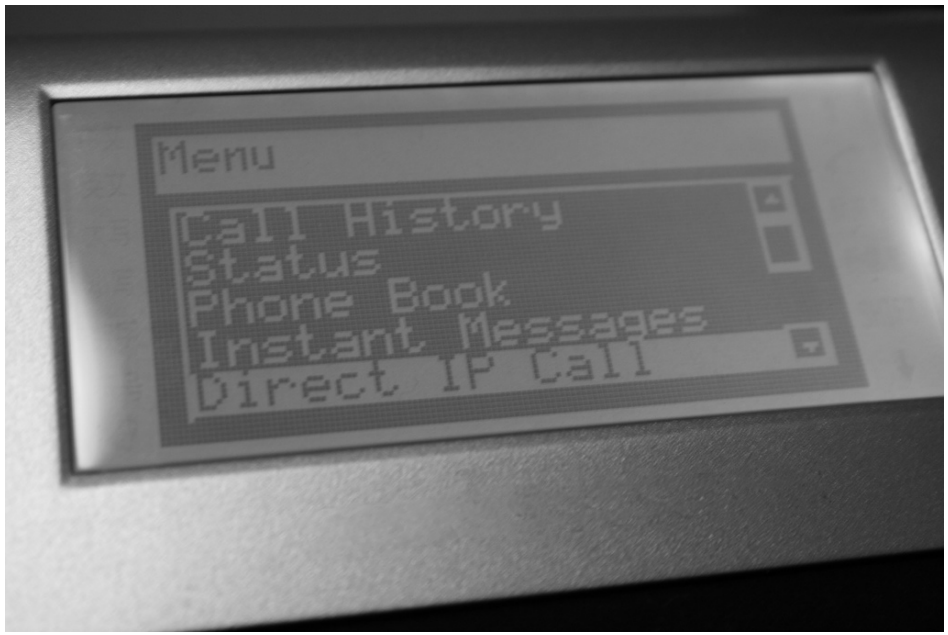
 Jean-Etienne Poirrier

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 Netzwerkkameras
- 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

Fazit

- ★ Sicherheit hört nicht bei der Technik auf
- ★ Viele Probleme sind leicht identifizierbar
- ★ Kreativität ist Voraussetzung für guten Pentester

Diskussion

Vielen Dank!