IT-Security in Theorie und Praxis
–
Über „harmlose“ Geräte und andere Denkfehler

Jens Liebchen - RedTeam Pentesting GmbH
jens.liebchen@redteam-pentesting.de
http://www.redteam-pentesting.de

Security-Workshop
18. September 2008, Berlin

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004 in Aachen
- ★ Spezialisierung ausschließlich auf Penetrationtests
- ★ Weltweite Durchführung von Penetrationtests
- ★ Forschung im Bereich der IT-Sicherheit

Über diesen Vortrag

- ★ IT ist überall – IT-Sicherheit noch nicht
- ★ Gerade „harmlose“ Geräte beinhalten Risiken, die so oft nicht bewusst sind
- ★ Viele Angriffe werden als unrealistisch oder sogar unmöglich eingestuft, sind in der Praxis aber sehr einfach
- ★ $\Rightarrow$ Beispiele aus der Praxis

Definition: Physische Sicherheit

Physical Security

Physical security describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media.

(Wikipedia)

Fallbeispiel: Sicherheitsdienst

- Sicherheitsdienst bewacht Zugänge zum Gebäude
- „Sind Sie angemeldet? Dann brauche ich Ihren Namen!“
- Name wird auf der ersten Seite einer Zeitung notiert und Zugang gewährt

Fallbeispiel: Sicherheitsdienst

- ★ Sicherheitsdienst bewacht Zugänge zum Gebäude
- ★ „Sind Sie angemeldet? Dann brauche ich Ihren Namen!“
- ★ Name wird auf der ersten Seite einer Zeitung notiert und Zugang gewährt

Fallbeispiel: Sicherheitsdienst

- ★ Sicherheitsdienst bewacht Zugänge zum Gebäude
- ★ „Sind Sie angemeldet? Dann brauche ich Ihren Namen!“
- ★ Name wird auf der ersten Seite einer Zeitung notiert und Zugang gewährt

Hier kommt keiner rein...

Andere oft funktionierende Angriffe:

- ★ Passende Kleidung und entsprechendes Auftreten (Blackberry und Anzug, telefonierend am Sicherheitsdienst vorbeilaufen)
- ★ Interne Visitenkarte (evtl. als eigene ausgeben)
- ★ Rauchertüren/Notausgänge
- ★ Hilfsbereitschaft der Mitarbeiter nutzen

Technische Zugangskontrollsysteme

Technische Zugangskontrollsysteme

Definition Biometrie

Biometrie

[. . .] Heute definiert man Biometrie im Bereich der Personenerkennung auch als automatisierte Erkennung von Individuen, basierend auf ihren Verhaltens- und biologischen Charakteristika.

(Wikipedia)

Zugangskontrolle per Biometrie

- ★ Zugangskontrolle zu sensiblen Bereichen per Fingerabdruck
- ★ Zutrittsversuch mit gefälschtem Fingerabdruck funktionierte
- ★ Stopp des weltweiten Enrollments des betroffenen Fingerabdruckscanners

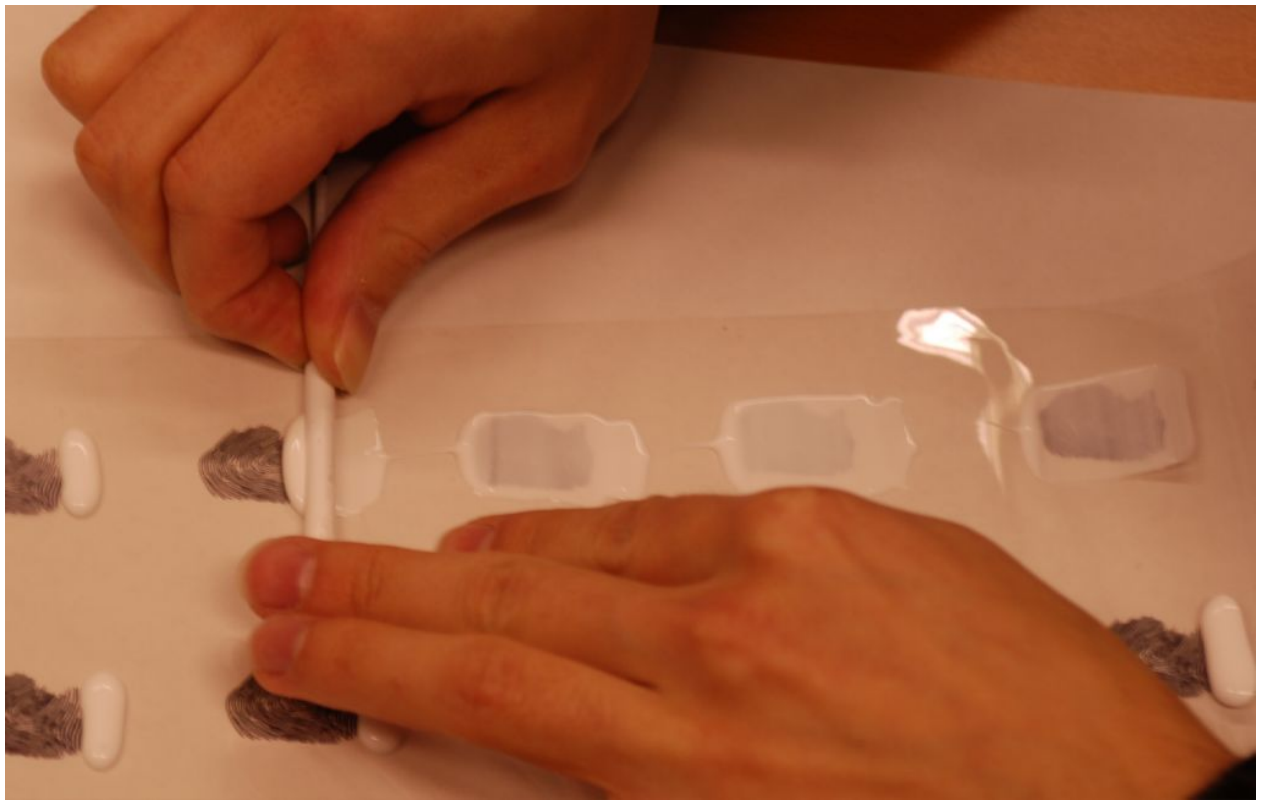
Zugangskontrolle per Biometrie

- ★ Zugangskontrolle zu sensiblen Bereichen per Fingerabdruck
- ★ Zutrittsversuch mit gefälschtem Fingerabdruck funktionierte
- ★ Stopp des weltweiten Enrollments des betroffenen Fingerabdruckscanners

Zugangskontrolle per Biometrie

- ★ Zugangskontrolle zu sensiblen Bereichen per Fingerabdruck
- ★ Zutrittsversuch mit gefälschtem Fingerabdruck funktionierte
- ★ Stopp des weltweiten Enrollments des betroffenen Fingerabdruckscanners

Replizieren von Fingerabdrücken



Replizieren von Fingerabdrücken

Risiken bei Biometrie: Was zu beachten ist

- ★ Abwägung zwischen Bequemlichkeit und Sicherheit
- ★ Kann das genutzte Merkmal erfolgreich kopiert werden, so steht oft kein neues (anderes) zur Verfügung
- ★ Biometrie kann Seiteneffekte haben (z.B. Zugangskontrolle BND Berlin)
- ★ Große Unterschiede zwischen Theorie und Praxis ⇒ Verlassen Sie sich nicht auf Werbeaussagen!

Risiken bei Biometrie: Was zu beachten ist

- ★ Abwägung zwischen Bequemlichkeit und Sicherheit
- ★ Kann das genutzte Merkmal erfolgreich kopiert werden, so steht oft kein neues (anderes) zur Verfügung
- ★ Biometrie kann Seiteneffekte haben (z.B. Zugangskontrolle BND Berlin)
- ★ Große Unterschiede zwischen Theorie und Praxis $\Rightarrow$ Verlassen Sie sich nicht auf Werbeaussagen!

Überwachungskameras

Überwachungskameras (CCTV)

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

Fallbeispiele Überwachungskameras

Aufgetretene Sicherheitsprobleme:

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

Fallbeispiele Überwachungskameras

Aufgetretene Sicherheitsprobleme:

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

Fallbeispiele Überwachungskameras

Aufgetretene Sicherheitsprobleme:

- ★ Kamera direkt auf Pinpad zur Zugangskontrolle gerichtet

Fallbeispiele Überwachungskameras

Aufgetretene Sicherheitsprobleme:

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

Überwachungskameras

Zu beachten:

- ★ Patchmanagement für Kameras sicherstellen
- ★ Physischen Zugriff auf Netzwerk unterbinden
- ★ Trennung CCTV-Netz und andere Netzwerke

Voice over IP

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

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

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: Neue Features, neue Risiken

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: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Fernsteuerung der Bedienelemente

- ★ Umleiten von Telefonaten

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Fernsteuerung der Bedienelemente

- ★ Umleiten von Telefonaten
- ★ Abhören per Konferenzschaltung

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Gute Mikrofone

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Gute Mikrofone

- ★ Einschalten der Freisprecheinrichtung
- ★ ⇒ Raumüberwachung per Telefon

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Anpassbare Bildschirmmenüs

- ★ „Phishing“ auf dem Telefondisplay

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Anpassbare Bildschirmmenüs

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

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Anpassbare Bildschirmmenüs

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

Was macht Ihr Telefon so, wenn Sie nicht hinschauen?

 Jean-Etienne Poirrier

Voice over IP: Zusammenfassung

- ★ Fehler herstellerübergreifend
- ★ Auch physische Trennung der Netzwerke hilft oft nicht
- ★ Fehler sind teilweise auch auf Nicht-VoIP-Telefone übertragbar

 Jean-Etienne Poirrier

Faxgeräte

Faxgeräte

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

Fallbeispiel Faxgerät

Fallbeispiel

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

Fallbeispiel Faxgerät

Fallbeispiel

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

Drucker / MFPs

Kopierer/MFPs haben

- Festplatten
- Netzwerkanschlüsse
- Betriebssysteme
- $\Rightarrow$ Drucker sollten wie Server behandelt werden

Drucker / MFPs

Kopierer/MFPs haben

- Festplatten
- Netzwerkanschlüsse
- Betriebssysteme
- $\Rightarrow$ Drucker sollten wie Server behandelt werden

Drucker / MFPs

- ★ MFPs in abgeschlossene (Server-) Räume?
- ★ Angreifer mit physischem Zugriff auf Drucker (Unzufriedene Mitarbeiter, Gäste und andere Personen)
- ★ ⇒ Manipulationen und Zugriff auf MFPs sehr einfach

Drucker / MFPs

- ★ MFPs in abgeschlossene (Server-) Räume?
- ★ Angreifer mit physischem Zugriff auf Drucker (Unzufriedene Mitarbeiter, Gäste und andere Personen)
- ★ ⇒ Manipulationen und Zugriff auf MFPs sehr einfach

Drucker / MFPs

- ★ MFPs in abgeschlossene (Server-) Räume?
- ★ Angreifer mit physischem Zugriff auf Drucker (Unzufriedene Mitarbeiter, Gäste und andere Personen)
- ★ ⇒ Manipulationen und Zugriff auf MFPs sehr einfach

Weitere Denkanstöße

- ★ Fremde Hardware an eigenem Rechner (USB-Sticks, Firewire, etc.)
- ★ Funkverbindungen (WLAN, Bluetooth, Funktastaturen, RFID, etc.), Clients beachten!
- ★ Besondere Situationen (z.B. Einreise USA)

Fazit

- ★ Angreifer handeln zielorientiert
- ★ Chancen eines erfolgreichen Angriffs bei „harmlosen“ Geräten ist wesentlich höher
- ★ ⇒ **Ubiquitous IT-Security**

Fazit

- ★ Angreifer handeln zielorientiert
- ★ Chancen eines erfolgreichen Angriffs bei „harmlosen“ Geräten ist wesentlich höher
- ★ ⇒ **Ubiquitous IT-Security**

Fragen?

Vielen Dank für Ihre Aufmerksamkeit