



# IT-Security aus dem Nähkästchen – oder – „Das kann mir nicht passieren. . . “

Jens Liebchen - RedTeam Pentesting GmbH  
[jens.liebchen@redteam-pentesting.de](mailto:jens.liebchen@redteam-pentesting.de)  
<http://www.redteam-pentesting.de>

14. DFN-Cert Workshop – Sicherheit in vernetzten Systemen  
7.-8. Februar 2007, Hamburg



## Über den Autor

- ★ Jens Liebchen
- ★ RedTeam Pentesting
- ★ Gründung 2004
- ★ Durchführung von Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit



## Über diesen Vortrag

IT-Sicherheit ist mehr als die neuesten Exploits und Patches. Dieser Vortrag zeigt Fehler, von denen die Verantwortlichen meistens nicht dachten, dass solche Fehler (bei ihnen) vorkommen.

- ★ 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!



Über den Autor  
Über diesen Vortrag  
**Incident Response**  
Administratoren  
Auffälligkeiten  
Suchmaschinen  
Der Blick auf das Ganze  
Fazit

## 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

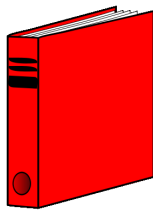
- ★ Administrator beauftragt Penetrationstest
- ★ Nach 24h Kompromittierung des Corerouters (von innen) durch die Pentester
- ★ Administrator so unter Stress, dass er nicht in der Lage ist, die aufgefallene Kompromittierung mit dem selbst beauftragten Pentest in Verbindung zu bringen





## 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)

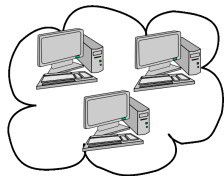
- ★ Viele Administratoren erledigen seit langer Zeit Alltagsaufgaben
- ★ Schulungen und Konferenzen werden häufig nicht bezahlt oder es fehlt die Zeit („Dann fällt der Administrator für diese Zeit aus...“)
- ★ Administratoren entwickeln „ungewöhnliche“ Lösungen für ihre Probleme





## 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 Penetrationstests: „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?

- ★ 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!





## Der Blick auf das Ganze

- ★ Als Techniker wird man leicht technikgläubig
- ★ Hierdurch werden schnell entscheidende Kleinigkeiten übersehen



## Der Blick auf das Ganze





Über den Autor  
Über diesen Vortrag  
Incident Response  
Administratoren  
Auffälligkeiten  
Suchmaschinen  
**Der Blick auf das Ganze**  
Fazit

## Der Blick auf das Ganze





## Der Blick auf das Ganze

Druckerkonfiguration:

### Incoming e-mail (not required for E-mail Alerts)

Set incoming e-mail server values to enable remote requests and commands to be sent to the device.

Enable Incoming E-mail

POP3 Server

Device POP3

Username

Password



## Der Blick auf das Ganze

Kopierer:

- ★ Festplatten
- ★ Netzwerkanschlüsse





## Der Blick auf das Ganze

Andere Beispiele:

- ★ Richtfunkverschlüsselung nur auf der Funkstrecke, Kabel mit unverschlüsselten Daten leicht erreichbar
- ★ Windows Vista: Speech Recognition



## Der Blick auf das Ganze

Was man tun kann:

- ★ Sicherheitsrisiken überall vermuten
- ★ Gerade bei scheinbar unwichtigen Geräten genauer schauen
- ★ Mehrstufige Sicherheitskonzepte





## Fazit

- ★ Sicherheit hört nicht bei der Technik auf
- ★ Viele Probleme sind leicht identifizierbar
- ★ Regelmäßig nach neuen „Fehlern“ suchen
- ★ Administratoren die nötige Zeit zur Verfügung stellen





Fragen?

Vielen Dank für Ihre  
Aufmerksamkeit.