Dipl.-Kaufmann
Thomas R. Köhler

<aisys> Advanced internet Systems AG

Internetsicherheit 2003

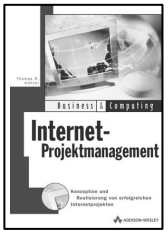
Zwischen "ScriptKiddies" und "Information Warfare"

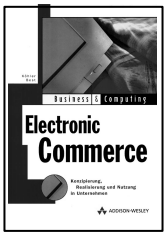
FH Ansbach 2003-04-03

Thomas R. Köhler - zur Person

- 1995 Mitarbeit am ersten Telekom-Internetauftritt www.dtag.de
- 1995 "Uni-Spin-Off"-Firmengründung
- 1998 erstes Buch: Electronic Commerce
- 2000 Gründung AISYS AG mit externem Kapitalgeber
- 2002 neues Buch: Internet-Projektmanagement
- 2002 - Lehrbeauftragter "WI-Info" FH Ansbach

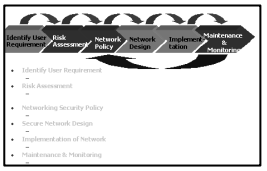
- Aktuelle Firmenprojekte für:
  -Europäische Zentralbank
  -Württembergische Versicherung
  -DeTeMedien
  -Deutsche Telekom AG
- -[…]





Was kostet Sicherheit ?

Hostinggebühren: ?1.000 monatlich



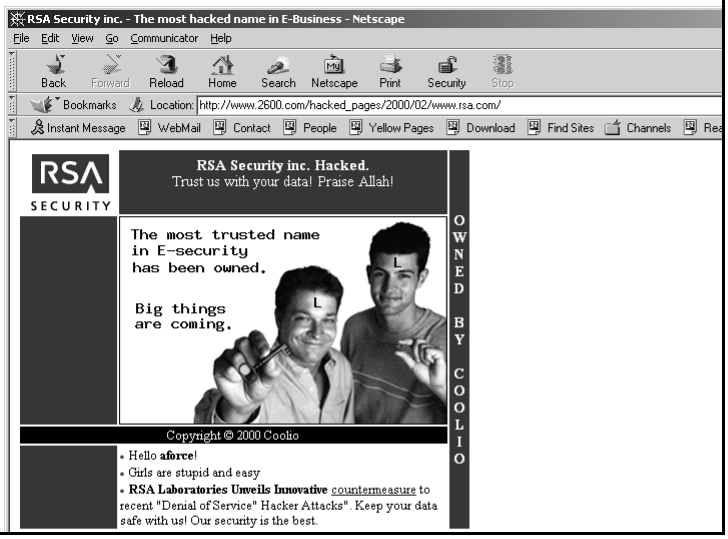
SecurityAudit: ?25.000

alld as.org defacement archive > ©

Kosten für Speicherung der gehackten Site: ?0.05

Imageverlust: einfach unbezahlbar

Defacements: Auch Sicherheitsfirmen werden gehackt



Ist die Bedrohung real ?

- Zahlen zum Thema (IDC 5/2002):
  - 51,7 % der Großunternehmen in D waren Opfer von "Cybercrime-Angriffen"
  - 50% davon: mehr als 5x Ziel von Hackern
- Schwierigkeiten bei der Bewertung:
  - nicht alle Angriffe werden bemerkt
  - nur wenige werden gemeldet / zugegeben
  - Bezifferung des "Schadens" schwierig
  - ca. 2/3 der Angriffe durch Insider (!)

Welche Kosten entstehen durch Sicherheitsverletzungen ?

Wie hoch ist der finanzielle Verlust, den Sicherheitsverletzungen im letzten Jahr hervorriefen?

	weltweit	USA	Deutschland
Kein Verlust	24	20	44
bis zu 1000 Dollar	8	8	10
bis zu 10000 Dollar	11	12	10
bis zu 500000 Dollar	8	10	3
bis zu einer Million Dollar	1	1	1
mehr als eine Million Dollar	1	1	0
Nicht bekannt	47	48	33

Alle Angaben in Prozent. Basis: Weltweit: 1910 Antworten, USA: 1020 Antworten, Deutschland: 229 Antworten
Quelle: PricewaterhouseCoopers/InformationWeek

Einige wesentliche Risiken des Internet

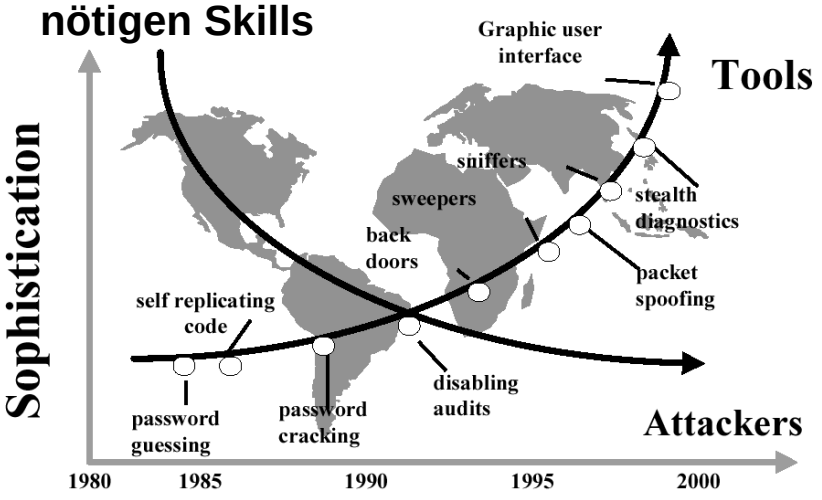
- Viren und Würmer
- Trojanische Pferde
- IP Spoofing
- Umleitung von Serverzugriffen
- Pufferüberläufe
- DoS, DDoS-Attacken
- gefälschte Mailnachrichten
- ...

Abb.: petroleumplace.com

Hackertum als Teil der Populärkultur

- Filme, Romane
- "how-to"-Guides
- weltweite Verbreitung

Entwicklung von Tools und nötigen Skills

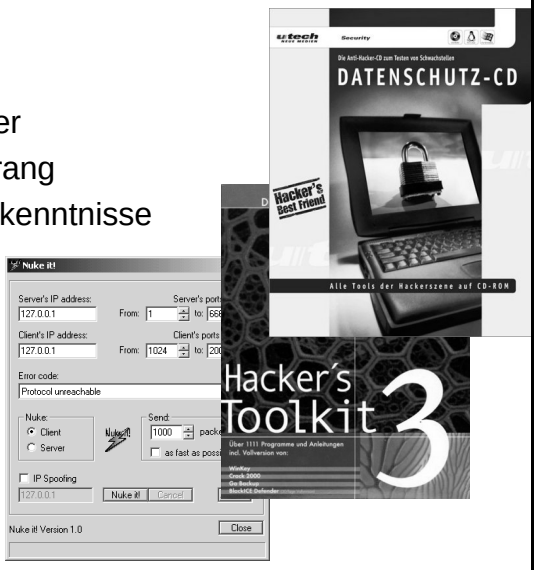


Quelle: Don Obert

Skriptkiddies

- (Jugendliche) Anfänger
- Neugierde/Geltungsdrang
- Keine / wenig Systemkenntnisse
- PC + Internet genügt

➡ für erfahrene Administratoren: KEIN PROBLEM



Andere Gruppen von Cyberkriminellen

- Hacktivisten
- (Cyber-)Terroristen
- Wirtschaftsspione

Hacktivismus

- Cyberprotest unter Nutzung von Hacking
- Protestgegner:
  - Staat
  - Unternehmen
  - Supranationale Organisationen
- Extremform: Cyberterrorismus

Mögliche Protestgründe:
-Kriege
-Unabhängigkeit
-Politik
-Atomwaffen
-Menschenrechte
-Tierrechte
-Umweltschutz
-Globalisierung
-Kapitalismus
-Recht und Gesetze
-Kinderpornographie
-Hackerinhaftierung
-Überwachung
-(…)

Cyber-Terrorismus

- Verwenden Terroristen das Internet ?
- Nutzen Terroristen "HackerTechniken" ?
- Bestehen Kontakte zwischen Hackern / Hacktivisten und Terroristen ?
- Gibt es den "Informationskrieg" ? !

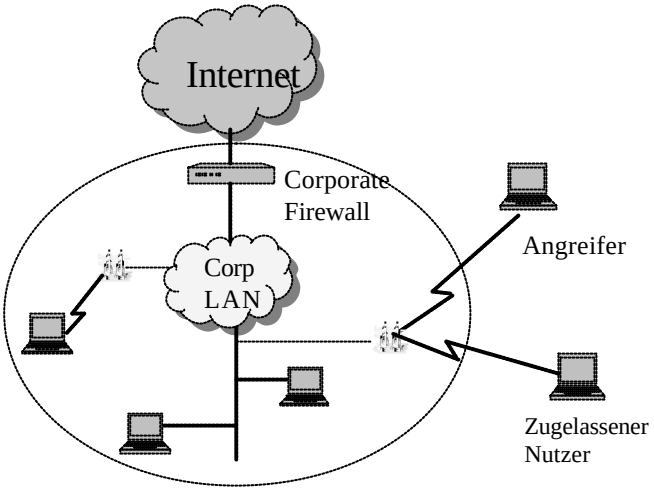
Wirtschaftsspionage

- Nutzung des Internet zum Ausspionieren fremder Unternehmen
- "Competitive Intelligence" wird salonfähig
- Bewusste Inkaufnahme von Grauzonen
- "Competitive Intelligence" bringt Geld in die Hackerszene

Problemfeld: Wireless LAN

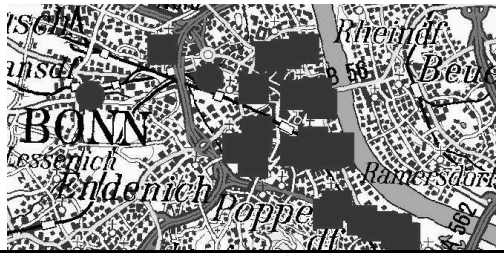
- Einfache Installation
- Preiswert
- Weitverbreitet
- Geringe Sicherheit bei Standardinstallation

Problemfeld: Wireless LAN

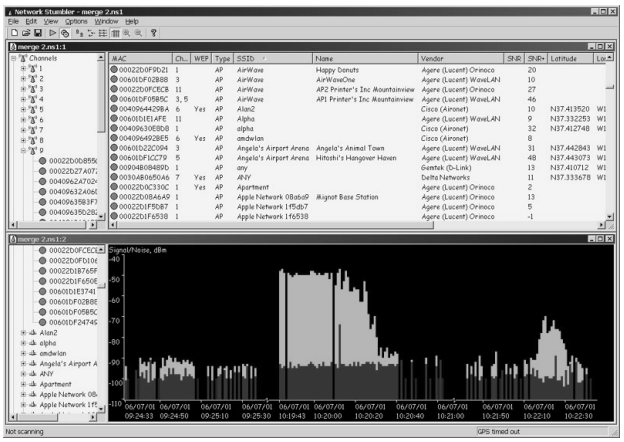


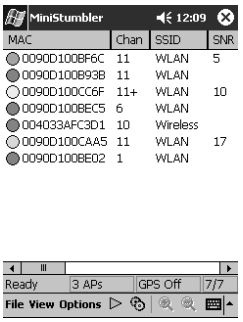
Wardriving

- Neuer Trend"sport" in Hackerkreisen
- Aufspüren und knacken von WLANs
- Kartenmaterial im Netz
- "WarChalking" auf der Strasse



Wardriving - Software frei im Internet verfügbar





Sicherheitsproblematik im Betrieb

- Systemadministrator ist mit Tagesgeschäft ausgelastet / Security steht hintenan
- Sicherheitsexperten sind teuer
- **Wer überwacht die Wächter ?**

Was tun ?

Optionen für den Umgang mit dem Faktor Sicherheit

- Systemadministratoren trainieren
- Hacker anheuern (?)
- Sicherheitsfirma mit Audit beauftragen
- [...]
- **Kurzfristig beste Lösung: Outsourcen !**

- **Wichtig:**
  Auch bei Lieferanten auf Sicherheit achten

Internetsicherheit 2003

Q&A

Kontakt: **mail@thomaskoehler.de**