



Brainstorming & Saaldiskussion Upcoming Security Nightmares III

**oder: worüber wir nächstes Jahr lachen
werden...**

Berlin, den 29.12.2002

*Moderation
ron @ ccc.de*



Agenda

Security Nightmares, die wir haben wollen... (weil sie vielleicht was ändern)

Security Nightmares, die wir nicht haben wollen...

... to be forewarned is to be forearmed



Stichworte, die wir uns letztes Jahr für dieses Jahr gemacht hatten...

SSHD, die Fortsetzung

Multi-OS Würmer / Scripte etc.

**Noch mehr automatisierung bei Viren, Wurmern,
... Schadenfunktionen?**

**Linux. Die Schonzeit ist vorbei. Man sieht es an
der Qualität der rootkits... „You can be lazy on any
plattform“**

**Kompromittierte Update-Mechanismen (Update
Server / Update Agent ...)**

**Strafverfolgungsbehörden hacken für
Gerechtigkeit (FBI „Magic Latern“)**

Basel II und Operational Security

**Es liegt in der Luft dass eine wesentliche
Datenbank „wegkommt“. Laptop Klau beim BKA
Kontaktbeamten des FBI?**

Biometrie vs. entfernte Fingerkuppen

**Wer wird DBA für Inpol Neu DB? Und reicht eine
Bezahlung nach BAT 5 (oder so) oder macht man
das nur, wenn man sich mindestens einen 4GH
Code einrichten kann.**

DRM OS, PC wird „Secure Perimeter Device“?

**Kompromittierte Kühlschränke, die zu viel Milch
bestellen**

Fernabfrage Heizungsablesegeräte

Kopierer als Wurmverteiler

Spasige Schadensfunktionen

Funkuhren “überschreiben”

**Navigationssystem-Updates selber bauen um
Ruhe zu haben**

OnlineBanken, SCHUFA oder DATEV Hacks...

**Die hier angekündigte Hackbahn hat übrigens
stattgefunden...**



Stichworte, die wir uns letztes Jahr für dieses Jahr gemacht hatten...

Insecurity goes Mobile / Wireless / etc.

- Mobiltelefone mit „richtigen“ Betriebssystemen
- Mobiletelefone mit MS Stinger
- und always on werden sie auch sein...

- Location Based Services? Bewegungsprofile? Location Based Spam?
- Kleine Dinge mit WaveLAN und 360 Grad Fischaugen-Optik kaufen?
- Wired Equivalent Privacy (WEP) 2
- Bluetooth Headsets... Spam im Ohr?
- PDA Viren



Was wir dieses Jahr (2002) so hatten...

**Es war noch Code Red übrig vom letzten Jahr...
ein bisschen Apache**

Php 4

Kerberos Buffer Overflow

**Immer noch keine Virens Scanner beim Otto
Normalverbraucher...**

Privacy & Datenschutz?

- Kennzeichenerkennung in Bayern und bald bundesweit wegen LKW-Maut

**Viele, viele IE Bugs (bis hin zum
Plattenformatieren) und Wmplayer nu auch...**

KDE mit MS Symptomatik

Ein bisschen MacOS X

**Bugs in Web Servern (IIS, ...), ftp-Servern (wu-
ftpd), sonstigen Servern, ...**

Und bind mal wieder, wer hätte das gedacht...

**Wireless LAN, mehr Wireless LAN und dann noch
Wireless LAN, aber nur 802.11b...**

- Wardriving
- Warflying
- Warchalking
- Warharharhar

Mobile Issues

- Einmalklingelnlassen aus Nauru (AP), bei Rückruf Freizeichensimulation
- SMS Spam / "Premium SMS"
- WAP Push Bug bei Panasonic GD87 (keine Rückfrage bei WAP Push Befehlen)
- Orange SPV (Stinger) Geld zurück möglich
- LBS Push Start durch... die Strafverfolgungsbehörden
- Bluetooth Pins festverdrahtet



Und die Highlights...

Bill Gates startet Trustworthy Computing Initiative!

- Auswirkungen sicherlich schon in den nächsten Jahren!

Es war noch ssh / openssl vom letzten Jahr übrig... und zwar viel davon

- Wurm Apache / OpenSSL

Trojaner in libpcap, tcpdump, sendmail

DoS, DDoS „nur“ auf DNS und keiner hats gemerkt

Schadensroutinen

- BugBear schaltet PFWs aus
- NN schaltet AV aus

S/O/N/Y Versteckt instabile API's hinter Sicherheitsbedenken

Mehr private / silent Bugfixes als wir je wissen werden

- Und natürlich die Diskussion um die Disclosure Policy zu Sicherheitslücken, die dieses Jahr weiter ging...

TCPA, Palladium, DRM Diskussion

- Windows Mediaplayer Update mit DRM

Windows/NetBIOS Popup Spam

PGP.com ist wieder da!

Sicherheit aus Hollywood...

- Minority Report
- James Bond



Was wir vergessen hatten...

0190er Dialer und Artverwandtes

- Snail Mail SPAM mit 0190...

Mehr und mehr SPAM

- Das Deutsch der Spammer wird auch immer besser...

Es heisst jetzt nicht mehr Orange Book sondern Common Criteria...

High Tech Fallen für Autodiebe



Stichworte für das nächste Jahr

Wireless...

- Tastaturen... hatten wir dieses Jahr schon, da kommt aber noch mehr...
- mehr Handies mit OS kommen jetzt aber real soon now...
- ...aber sind ferngesteuerte Handykameras echt ein Problem? Naaaaajaaaaa

... embedded Systems

- hatten wir schon angesagt, da kommt aber noch mehr...
- Es gibt bestimmt bald Viren, die auch einen Benz fahren wollen...

Handies: Wireless embedded Systems...

- Jetzt aber! Nun endlich! Mit OS!
- d.h. der Patch Wahnsinn ist in unserer Hosentasche angekommen, aaaaber....

UMTS / GPRS

- weiterhin GPRS Paranoia?
- Operator Equipment vs Netztrennung?

Videüberwachung mit Gesichrererkennung könnte einen neuen Sport starten

- Politiker-Gesichtsmasken werden wieder Mode...

Premiere stellt Crypto um... vielleicht ... real soon now...

Biometrie-Studie des Bundesinnenministeriums läuft. Das Ergebnis ist...

- und gibt es da nicht noch ganz viele kommerzielle Möglichkeiten?

Webservices?

- Remember the Credit Card Verification Game

Achja und die Konsolenflut wird uns viele, viele Zombies bescheren...

and remember, parts of iptables are still experimental...



Nach Veranstaltungsende

Die Lufthansa Miles&More Datenbank könnte man fast als “wesentliche Datenbank” bezeichnen – jedenfalls hat es für ein paar Politiker gereicht...