Brainstorming & Saaldiskussion

Upcoming Security Nightmares

oder: worüber wir nächstes Jahr lachen werden…

Berlin, den 30.12.2004

Moderation
ron @ ccc.de
frank @ 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

Die Ironie des heise.de Banner-Servers…

Zum Aufwärmen… geplante Merchandise für die WM 2006

Die 2004 vorhergesagten Highlights aus diesem Jahr

Superworms, Bluetooth, Instant Messaging

Überwachungskameras / WLAN u.a. Funkschnittstellen

Vulnerabilities in Tools rücken in den Fokus

- Symantec, F-Secure, Tred-Micro, McAfee, Sophos, … (Buffer Overflows im Virenscanner)
- Adobe Reader (cross platform!), Winamp, Etherreal, RealPlayer, Backup-SW, ...

Erster Mobiltelefon / MMS Wurm (nagut, nur PoC)

MacOS X (erster Trojaner, nur PoC)

MSFT Fokus auf Security bringt Ergebnisse?!

- der Nachteil: Clippy hilft bald beim Beseitigen von Buffer Overflows in MS Visual C++
- Proteste des Süd-Koreanischen Dienstes weil MSFT Windows 98 nicht mehr patched

VoIP

OpenSource Produkte (Firefox usw.)

zlib everywhere

Kundendaten verloren haben dieses Jahr: Marriott (2k), ABN Amro (2m), Time-Warner (600k), Guidance (3.8k), ChoicePoint (35k), Bank of America (1.2m), RVI (1.4m), LexisNexis (310k)…

… und was (noch) nicht passiert ist

Mautsysteme

SSH wirds nochmal dick erwischen

Biometrie-Großprojekte

ZigBee (Hausautomation, 350m Reichweite, …)

mobile Bot-Netze / Würmer die Premium SMS verschicken

die Vernetzung von Autos / z.B. CAN Bus / RDS → CAN → Autoelektronik

- “Handy-Wurm Cabir soll keine Gefahr für Lexus-Fahrzeuge darstellen“ (heise)

…aber aufgeschoben ist nicht aufgehoben!

Was wir letztes Jahr (für dieses Jahr) vergessen hatten, bzw. was sonst noch war…

SPAM / Phishing wurde tatsächlich noch schlimmer…

- "So meldet die Paderborner Polizei einen Fall, in dem sich ein 20-jähriger Paderborner Anfang Dezember selbst anzeigte, da er sich ertappt gefühlt hatte." (heise)

Firmen greifen zu Rootkits

- Sony erhöht die Zombie-Population um 3-500.000 PCs bei 2.1m verkauften CDs

php ist immer noch nicht "sicher"

SHA-1 "geknackt" (2^80 → 2^69)

Default Passwörter sind immer noch nicht ausgestorben

Daten-Geiselnahme und Erpressung durch Virus (PGPcoder)

"Deutschland sicher ins Netz" Initiative

Vortrag über Cisco Sicherheit auf BlackHat Konferenz und Nachspiel…

Mastercard Europay → GCMS mit Standort USA

Phrack wurde eingestellt: So long and thanks for all the fish…

Stichworte für 2006

Weiter steigende Unentspanntheit bei Hinweisen auf Sicherheitslücken

WarDriving usw. ist Out, WarFlying ist In (LH Flynet machts möglich)

Blackberry

P2P Würmer mit anständigen Schadensroutinen z.B. share *.*

Firewall-Würmer

Die meisten Mobiltelefone können immer noch nicht vom User gepatched werden…

- Wir warten also auf den MobileAltertCon / GSM Threat Level / … Service

TupperWare bringt “Tin-Foil-Hat” Taschen & Dosen in jeder Größe auf den Markt

Fussball-WM: mehr Kameras als Zuschauer (“Du bist Krimineller”)

VoIP Spam? Mal sehen…

ELSTER und anders

Abwasserüberwachung zur Sicherung der nationalen Sicherheit?

Hinweise für 2006…

“When robbing bank, don't take your own laptop”

If you work for the US Navy, please remember to NOT

“use peer-to-peer (P2P) file sharing applications, such as Kazaa, Shareaza and OpenP2P without approval and only in support of Navy missions” !!1!

Einen guten Rutsch..!