

“Bezpečnost na síti”

14. 11. 2005

CESNET z. s. p. o.

Přednášející

Andrea Kropáčová

Jana Jandusová

Pavel Vachek

Pavel Kácha

Seminář organizuje – Gábina Krčmařová

Program

- 09:30–10:10 Úvod do problematiky bezpečnosti sítí a služeb
(Andrea Kropáčová)
- 10:10–10:45 Incidenty, jejich charakter a řešení
(Andrea Kropáčová, Pavel Kácha)
- 10:45–11:30 Právní aspekty spojené s bezpečností sítí a služeb na ní
provozovaných *(Jana Jandusová)*
- 12:30–13:00 Vytvoření bezpečnostního týmu a jeho management
- 13:00–13:30 Představení CESNET-CERTS týmu a jeho cílů
(Andrea Kropáčová)
- 13:30–14:00 Spamming, phishing, pharming *(Pavel Kácha)*
- 14:20–14:50 Systémy pro detekci porušení bezpečnosti síťového provozu a služeb
(IDS, Audit) *(Pavel Vachek)*
- 14:50–15:15 Představa dalšího vývoje bezpečnostní strategie v
síti CESNET2 *(Andrea Kropáčová)*
- 15:15–??:?? Diskuse

Prezentace

Naleznete po skončení semináře zde:

http://www.cesnet.cz/csirt/20051114_prezetace/

Bezpečnost

Problém **technický** nebo **lidský**?



Zdroj: Pavel Kantorek, http://kantorek.webzdarma.cz/kantorek_f.htm

Trocha historie

Na počátku byl Arpanet ...

- **RAND Corporation** má za úkol vymyslet síť pro případ jaderné války:
 - bez centrálního prvku
 - provozuschopnou v případě zničení některé části
- první implementace v Británii, vzápětí v USA financováno **ARPA** (Advanced Research Projects Agency)

ARPANET

- **ARPANET měl za úkol:**
 - ověřit technologii přepínání paketů
 - připojit univerzitní superpočítače
- **první připojené university (1969)** – UCLA (University of California), UCSB (University of California Santa Barbara), Stanford (Stanford Research Institute, SRI) a univerzita v Utahu
- velice brzy vítězí **komunikace** nad “**počítáním na dálku**”, skupina **Vinton Cerf, Steven Crocker** a **Jon Postel**, RFC, tvorba protokolů TCP

První problémy

- 1980 první virus vyřadil celý Arpanet z provozu
- 1981 Ian Murphy (alias Captain Zap) - změna času
- 1988 (listopad) Morrisův červ
- 1990 Kevin Poulsen pronikl do telefonní sítě amerického rádia a vyhrál Porsche
- Kevin Mitnick a jeho “**socialengineering**”
- John Draper - “phreaker” a jeho píšťalka Captain Crunch
- od 90. let bezpečnostní problémy na denním pořádku

Proč není Internet bezpečný?

- nepočítalo se s tím, že by měl být **bezpečný**, měl sloužit "na hraní"
- nikoho to v 70. letech, kdy vznikaly protokoly TCP/IP, nenapadlo
- byl jiný požadavek - **robustnost a efektivnost**
- až uživatelé přišli s tím, že chtějí přes síť dělat všechno a pokud možno ani "nevylézt z postele"
- **bezpečnost** měly řešit až ty **aplikace**, které ji potřebují

Základní pojmy

- "hacker" versus "cracker"
- sociotechnika (Kevin Mitnick)
- podvržení identity
- identity theft (odcizení identity)
- phishing, pharming

Charakterizace hackerů ...

- **původní odrůda** – hackují pro radost ze svých dovedností, neničí a nezneužívají
- **“script kiddies”** – většinou mladí lidé, kteří mají vědomosti pouze na aplikování hackerských **nástrojů**
- **špióni** (střední třída) – solidní znalosti, nabourají, tiše sledují, žertovné změny v systému
- **elitní střelci** – zneužívají čerstvé díry, vyvíjejí hackovací a maskovací nástroje, finanční zisk

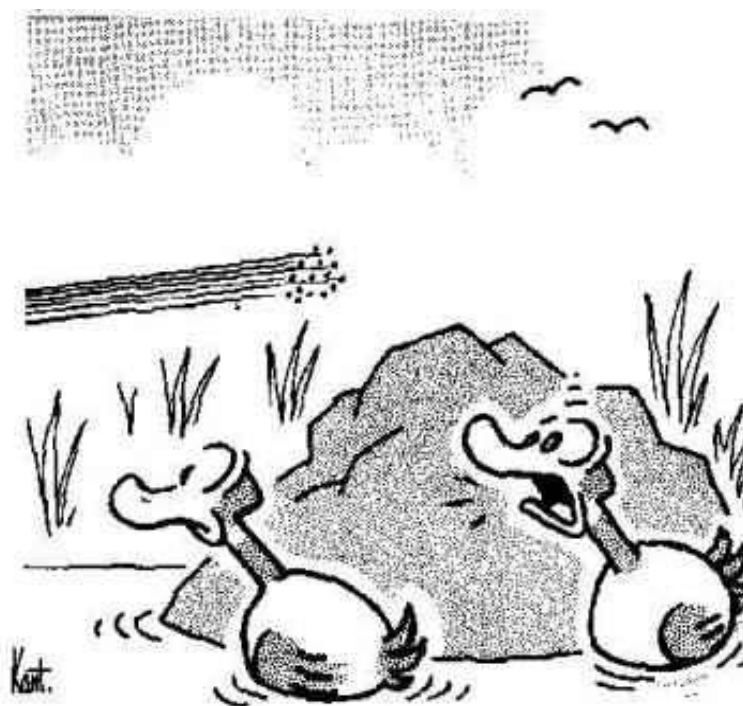
... a jejich motivace?:

- **snaha dobýt, zničit, zneužít, obohatit se, ublížit ...**

Proč se hackuje v akademických sítích?

Proč v akademických sítích?

- výkonná síť
- velké množství počítačů
- akademická povaha
- studenti



Neblázni! Jim je úplně jedno, že jsi hodná kachna.
Oni střílejí všechny kachny.

Mezinárodní spolupráce

- **FIRST (Forum of Incident Response Security Teams), <http://www.first.org/>**
- **Terena – TF-CSIRT, <http://www.terena.nl>**