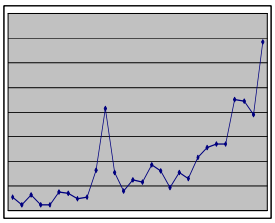
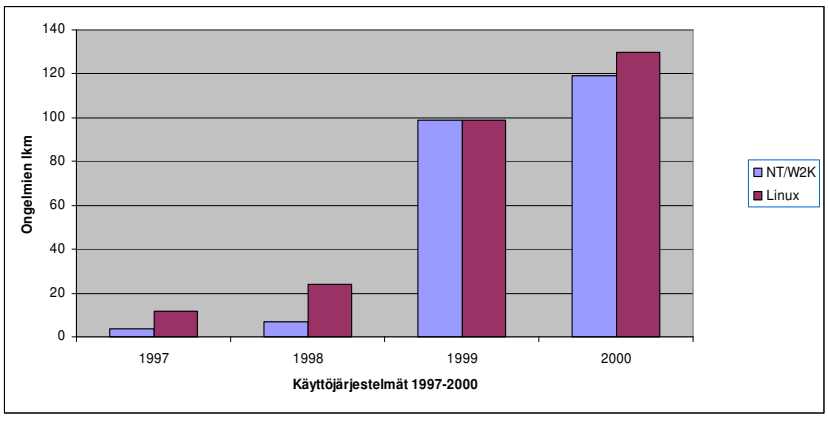
Tietoturvatrendejä ja uhkakuvia

Tietoturva ry
30.5.2001
Jari.Pirhonen@atbusiness.com
Senior Security Consultant, CISSP
AtBusiness Communications Oyj
www.atbusiness.com

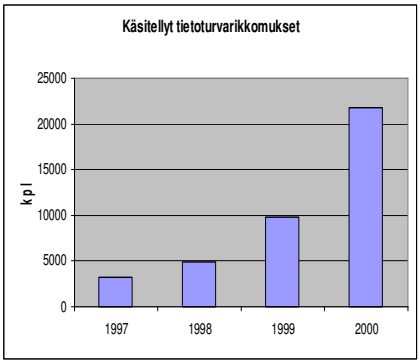


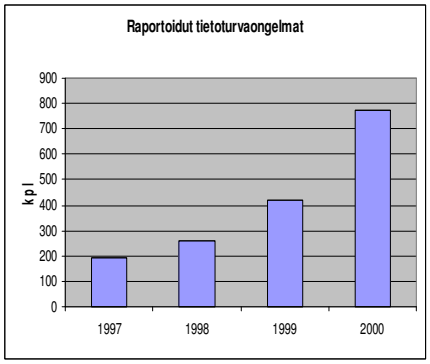
Käyttöjärjestelmien ongelmat



lähde: Securityfocus/Bugtraq

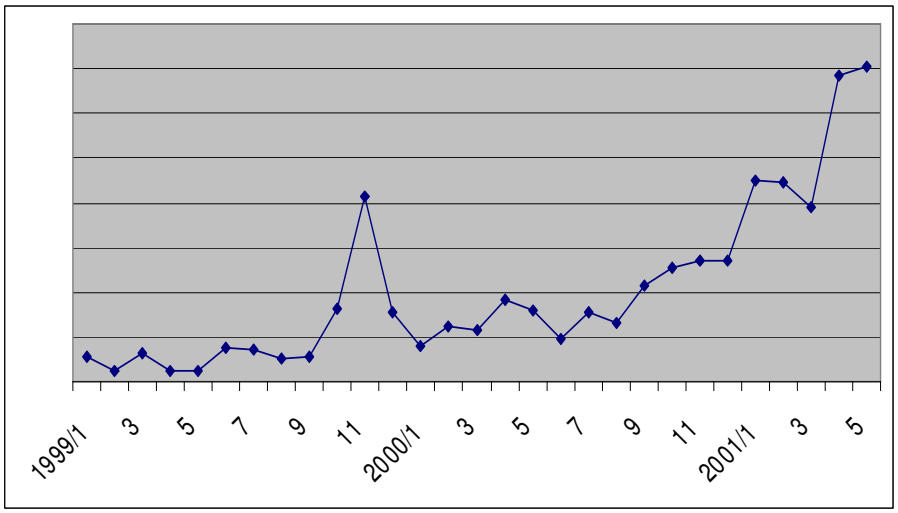
CERT / CC





lähde: Carnegie Mellon University, http://www.cert.org/stats/cert_stats.html

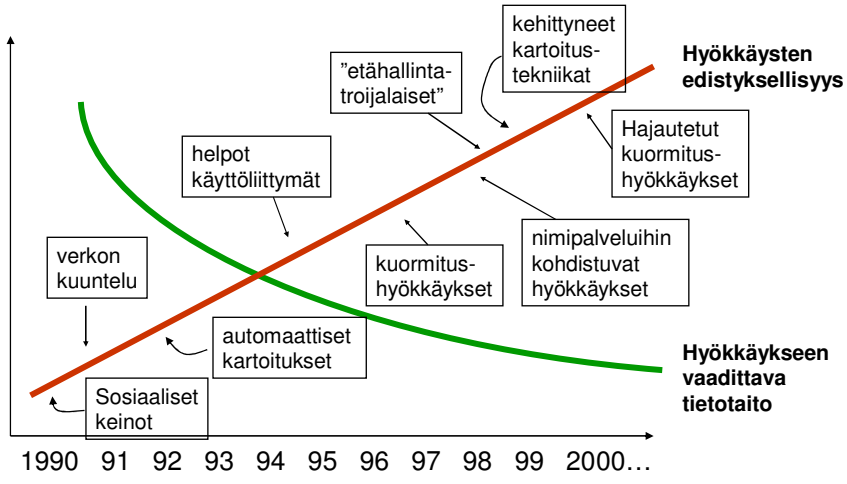
Skannaukset (lkm/kk)



Attrition.org 21.5.2001

One of the most predominant sections of Attrition has been the defacement mirror. What began as a small collection of web site defacement mirrors soon turned into a near 24/7 chore of keeping it up to date. **In the last month, we have experienced single days of mirroring over 100 defaced web sites**, over three times the total for 1995 and 1996 combined. **With the rapid increase in web defacement activity**, there are times when it requires one of us to take mirrors for four or five hours straight to catch up. Add to that the scripts and utilities needed to keep the mirror updated, statistics generated, mail lists maintained, and the time required for basic functionality is immense. A "hobby" is supposed to be enjoyable. Maintaining the mirror is becoming a thankless chore.

Hyökkäysten uhka kasvaa



lähde: Carnegie Mellon University

Yleisimmät ongelmat

- BIND
- CGI -ohjelmat ja web-palvelinten laajennokset
- Remote Procedure Call (RPC)
- MS IIS-palvelin ja Remote Data Services (RDS)
- Sendmail ja MIME puskurin ylivuoto,
- sadmind ja mountd
- Tiedostojen jako, NFS ja SMB/CIFS
- Huonot salasanat, ei salasanoja
- IMAP ja POP puskurin ylivuoto
- Oletusarvoinen SNMP ”community string”

Lähde: www.sans.org

Eniten ”koputellut” portit

- 0
- 53 (dns)
- 21 (ftp)
- 111 (sunrpc)
- 515 (lpr)
- 80 (http)
- 137 (netbios)
- 1 (tcpmux)
- 27374 (SubSeven)
- 109 (pop2)

Lähde: www.incidents.org

Keväällä 2001

- Linux-madot (Lion, Ramen)
- Sadmind/IIS mato
- Cheese – Lion-madon poistava mato
- ”Hakkerisodat”
  - Kiina <> USA
- Henkilökohtaiset palomuurit
- Yrityksen palomuurin kiertäminen
  - www.firethru.com
  - www.gotomypc.com
- Open Source <> Microsoft
- Langattomien ja mobiililaitteiden tietoturva
- Viranomaisten järjestäytyminen
  - Suomi Tietoturvakeskus

Suuntauksia

- Käyttäjien ja palvelujen määrä kasvaa
- Käyttäjät entistä ”yksinkertaisempia”
- Protokollat ja sovellukset entistä monimutkaisempia
- Sovellusten tietoturvaongelmien määrä kasvaa
- Hyökkäykset entistä kehittyneempiä, helppo-käyttöisempiä ja tehokkaampia
- Tietoturvaratkaisut entistä vaativampia
- Pula tietoturva-ammattilaisista
- Tietomurtojen ja kiusanteon määrä kasvaa
- Ammattihakkerit: yritysvakoilijat,terroristit, rikolliset
- Puolustautuminen: puolustusvoimat,poliisi
- Hactivism – mielenosoitukset verkossa