Siemens CERT

Stockholm, 24.01.2002
Udo Schweigert

Udo.Schweigert@siemens.com

http://www.cert.siemens.de

cert@cert.siemens.de
Siemens - Facts

- more than 450,000 employees
- more non-German employees than German
- 250,000 IP addresses
- approximately 600 externally visible Web-servers
- approximately 150 "gateways" from the intranet to the internet
Siemens CERT - Facts

• Founded April 1st, 1998 as a „corporate service“

• Started with 5 members

• At the moment:
  • 10 members doing the „basic services“
  • 4 (+ x) doing added services (to be paid for separately)
  • 1 Team assistant
  • Always one team member located in North America

• Full FIRST member since May 1998

• TI Level 2 Team since March 2001 (first german L2, first commercial L2)
### Overview of the basic services

#### Information
- App. 200 websites, app. 50 mailing lists and newsgroups
  - Follow, analyze, filter
  - Test information on reference systems
  - Issue warnings (Security Telegram)
  - Maintain Siemens CERT web server

#### Contacts
- App. 400 contact persons, app. 4000 subscribers to Security Telegram
  - Request handling (app. 200 / month)
  - Maintain subscriber list
  - Workshops, presentations, visits, NA
  - Contributing to FIRST and I4

#### Tools
- App. 28 tools, app. 250 000 IP addresses
  - Analyze, test, evaluate, provide tools and patches
  - Scanner: Licensing, managing licenses
  - Operation concepts, policies
  - Checklists

#### Ready to Use Information

#### Security Tools for the Company

#### Emergency Management
- App. 30 incidents / month
  - Emergency planning, recommendations for Administrators in case of an emergency
  - On call 24h / 365d
  - Detection, Eradication, Recovery

#### Containment

---

Stockholm January 2002

---

© Siemens AG 2002, CT IC 3
All rights reserved. Siemens CERT
Siemens CERT basic services

- Does NOT include handling of virus incidents!
  This is done by another corporate service called “Virus Competence Center” (5 members)

- Close cooperation with the Siemens-internal IS organization

- There is at least one workshop per year for the IS organization

- Corporate license for ISS (Internet Security Scanner)
Advisories

• Advisory Capability is part of Siemens-CERT's „basic service“

• Reading of important mailing lists
  • bugtraq
  • bugtraq-nt
  • FIRST
  • vendor mailing lists (SUN, Microsoft, ...)

• Status of Security-Telegrams since 2001 (2000):
  • PC (Windows-NT/2000): 77 (124)
  • UNIX (including Linux): 128 (62)
  • Net (CISCO, etc): 11 (6)
  • Misc 27 (21)
Measureplans

• Regularly updated (4 times a year) documents to advise administrators how to setup a secure system

• Four flavors:
  • UNIX/Linux
  • Windows-NT (US-English and German)
  • Windows 2000 (US-English, Siemens uses the MUI)
  • Windows XP (US-English, same as with Windows 2000)

• Tightly bound to Siemens-internal „Scan Process“ (ISS)

• Additionally available
  • Apache
  • Microsoft IIS
Siemens CERT – added services

Consulting on IS

- DMZ audits
- e-business processes
- secure system administration
- forensics
- research projects
- EU funded project(s)