

# Siemens CERT

Stockholm, 24.01.2002

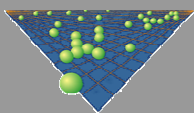
Udo Schweigert



<http://www.cert.siemens.de>

[cert@cert.siemens.de](mailto:cert@cert.siemens.de)

[Udo.Schweigert@siemens.com](mailto:Udo.Schweigert@siemens.com)



Information &  
Communications  
Security  
Siemens CERT

## Siemens - Facts

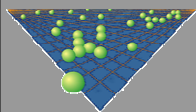
### Overview

### Basic Services

### Advisories

### Added Services

- 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

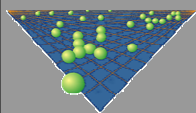
### Overview

### Basic Services

### Advisories

### Added Services

- 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

Overview

**Basic Services**

Advisories

Added 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*

*Ready to Use Information*

### 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*

*Trust and Acceptance*

### Tools

app. 28 tools, app. 250 000 IP addresses

- *Analyze, test, evaluate, provide tools and patches*
- *Scanner: Licensing, managing licenses*
- *Operation concepts, policies*
- *Checklists*

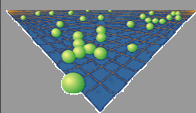
*Security Tools for the Company*

### Emergency Management

app. 30 incidents / month

- *Emergency planning, recommendations for Administrators in case of an emergency*
- *On call 24h / 365d*
- *Detection, Eradication, Recovery*

*Containment*



Information &  
Communications  
Security  
Siemens CERT

## Siemens CERT basic services

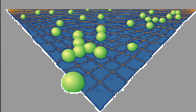
Overview

**Basic Services**

Advisories

Added Services

- Does NOT include handling of virus incidents!  
This is done by an other 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)



Information &  
Communications  
Security  
Siemens CERT

# Advisories

Overview

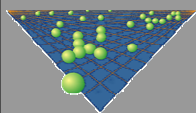
Basic Services

**Advisories**

Added Services

- 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)  |



Information &  
Communications  
Security  
Siemens CERT

# Measureplans

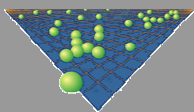
Overview

Basic Services

Advisories

Added Services

- 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



Information &  
Communications  
Security  
Siemens CERT

# Siemens CERT – added services

Overview

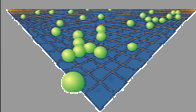
Basic Services

Advisories

**Added  
Services**

## Consulting on IS

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



Information &  
Communications  
Security  
Siemens CERT