DFN-CERT GmbH

German Research Network
Computer Emergency Response Team

Agenda

- Team history
- Portfolio
- Team structure
- Incident Handling at DFN-CERT
- Open issues
DFN-CERT History

In the beginning ...

• 1993:
  – Start of DFN-CERT Project at
  – University of Hamburg, Dept. of Computerscience
  – 2 FTE
  – FIRST membership

• July 1994:
  – 3 FTE

DFN-CERT History

More work – more projects

• 1995:
  – TERENA Task Force “CERTs in Europe”

• 1996:
  – DFN-PCA as additional project

• 1997:
  – DFN-FWL as additional project
DFN-CERT History

Now

- Jan. 1999:
  - Start of DFN-CERT GmbH
  - Non-profit

- End of 2000:
  - DFN-CERT: 3 FTE
  - DFN-PCA: 1 FTE
  - DFN-FWL: 1 FTE

The Constituency

Members of the German Research Network

- Deutsches Forschungsnetz - DFN /
  German Research Network
  - ATM network (B-WiN) migrating to
  - IP over SDH network (G-WiN)

- More than 400 members
  - Universities, libraries, schools, ...
  - Research institutions like GMD, Max-Planck, Fraunhofer, DLR
  - Public funded agencies
  - Industry (research only)
Coordination in Germany

Central role of DFN-CERT

CERT, CIAC

FIRST

CERT-NL

BSI

VTC

BKA

MVC

AUSCERT

Basic services

of DFN-CERT GmbH

- Information
  - Counselling
  - Public information services
  - Advisories, security bulletins, ...

- Emergency response
  - Support
  - Information and coordination

- Events
  - Workshops and Tutorials
  - Classes for students at University of Hamburg
Optional Services

of DFN-CERT GmbH

- Individual chargeable services
  - Risk analysis
  - Security concepts
  - Product evaluation
  - Individual employee training
  - Expertise
  - On-Site support
  - Help in establishing and operating of ERTs
  - Individual help in establishing and operating certification authorities (DFN-PCA)

Internal Structure

- DFN-PCA, DFN-FWL, DFN-CERT
  - Autonomous teams
  - Common infrastructure (network, servers)

- Common Helpdesk for DFN-CERT and DFN-PCA
  - ONE defined point of contact to constituency
  - Similar tasks supported by one tool
Internal Structure

Putting it all together

Incident Reports / Information Requests

DFN-CERT Helpdesk

Triage

Incident

Feedback

Announcement

Constituency

Site(s)
Reporter(s)
CSIRT(s)
Expert(s)

Requester(s)
Media
Management

Incidents

Statistic

© 1993-2000 DFN-CERT GmbH / TF-CSIRT / Incident Handling / 1
Incidents

Classification

- Incidents by operating system
  - 95 % Unix
  - 5 % Windows (and rising)
  - almost nothing else

- Incidents by report medium
  - 80 % reported by e-mail
  - 19 % reported by phone
  - 1 % Fax, walkin, postal mail

Incidents

Classification (2)

- Incidents by priority
  - Classification by severity
  - Simple numbering scheme

- Severity
  - Peoples health and lifes
  - Potential damage of attack
    - Rights gained by attacker
    - Number of hosts affected
Incidents

Classification (3)

- Incidents by type
  - For statistics
  - For correlation
  - Basis for priority classification
  - Work in progress

Incidents

Workflow

- First contact with: Helpdesk
- Weekly shifts for triage
  - Classifies incident
  - Handles incident or
  - Assigns incident to coordinator
- Final resolution of incident outside weekly shift
Problems
to be solved

- Legislation
  - Privacy issues
  - Anti-Crypto laws
- Common reference framework
- Databases
  - Trust
  - Completeness