Incident Management Process: Strategies, tools and techniques

Jacques Schuurman – jacques.schuurman@surfnet.nl

Riga, LV

14 April, 2008
Agenda

- Introduction into Incident Management
- How to devise a strategy for incident management?
- Tactical considerations
- Operational remarks
- Incident management in practice: SURFcert
- Questions and (hopefully) answers

IMP: strategies, tools, techniques
Incident management (1/3)

- Definition of an incident:

A breach or violation of any legislation, rule or policy (commonly: regulation) pertaining to the use of ICT facilities such as computer systems, applications, networks and their devices, appliances and/or (web) applications

- Laws come from “above” (government), rules and policies come from within (organisation, provider, etc.)
Incident management (2/3)

- These regulations must be:
  - clear;
  - unambiguous;
  - well understood;
  - known;
  - fair and equal to all equivalent users;

- ... in order to be:
  - enforceable
  - explicable
  - defendable

IMP: strategies, tools, techniques
**Incident management (3/3)**

- Once an incident is detected (reported, monitored), it needs to go through the five steps of Incident Management Process (**IMP**):
  1. analysed for relevance  
     (are we the correct party to solve it?)
  2. triaged  
     (what is its form and/or appearance?)
  3. assessed  
     (what is the violation, and what is the impact?)
  4. mitigated, solved and or ignored  
     (what steps to undertake)?
  5. analysed and reported  
     (lessons learned and statistics)

**IMP:** strategies, tools, techniques
All IMP tasks in one team

- Notion of a CSIRT: Computer Security Incident Response Team
- Operational and tactical approach of the IMP
- Coherent approach of the IMP
- Strategic considerations have a consistent implementation path:
  - mission
  - vision
  - strategy
  - tactics
  - operational implementation
All IMP tasks in one team

- Embedded in the functional context of the parent organisation:
IMP Strategy ("why?")

Depends on your mission/vision:

- Prevention vs. reaction
- Financial vs. reputation
- Labour intensive vs. labour extensive
- Liberal vs. restricted

All of this to be reflected in policies:

- Security Policy
- Acceptable Use Policy
- Service Level Agreement / Specification

IMP: strategies, tools, techniques
Tactical aspects ("what?")

- What service to offer?
  - Incident Management (MUST)
  - Optional:
    - Alerts & Warnings
    - Vulnerability Handling
    - Artefact Handling
    - Announcements
    - Technology Watch
    - Audits/Assessments
    - Configure and Maintenance
    - Education/Training
    - Security Tool Development
    - Intrusion Detection
    - Information Dissemination
    - Risk Analysis
    - Business Continuity Planning
    - Security Consulting
    - Awareness Building
    - Product Evaluation
    - List from CERT-CC (www.cert.org/csirts/)
Operations ("how?")

- Intrinsic vs. extrinsic
- Prevention vs. reaction
- Aggressive vs. loose
- Paid-per-service vs. all-inclusive
- Money vs. reputation
- Repressive vs. tolerant
- In-house vs. outsourced
SURFcert (1/2)

- Context:
  - 175 institutes, 1M end users
  - Academic in history and nature
  - Trend: centralised services in service centres
  - Trend: more financial awareness

- Choices:
  - Incident handling in-house
  - Advisories outsourced
  - Flow monitoring partly in-house developed, partly acquired commercial product
SURFcert (2/2)

- Operational parameters:
  - 10 members
  - 6 SURFnet staff. 4 institute based staff
  - Avg. total workload incident response: 1.5 fte
  - Avg. total workload other services: 1.0 fte
  - Ordinary services inclusive, specials to be charged additionally

- Tools:
  - Flow monitoring (SURFflow / Peakflow / NfSen)
  - Workflow management: AIRT
  - Encryption: PGP (GPG) and X.509
  - Sinkhole alert subscription
  - At the side: Intrusion Detection (SURFids)
Questions (and answers?)

- Anything you always wanted to ask....