The DigiNotar crisis

Handling SSL-mageddon

Aart Jochem
Joint FIRST/TF-CSIRT technical seminar
Rome - 31 January 2012
First: What’s NCSC-NL?

- Dutch National Cyber Security Centre,
- Operational since Jan 12, 2012
- Already FIRST member, TI-accredited, TI-SIMM3-certified, fully 24x7 operational IRT, monitoring network….  
  
  ....We even have our own international symposium (13-14 nov 2012)

- The secret?
Agenda

- What happened?
- Building up a national crisis
- Crisis management in the Netherlands
- Organizational aspects
- Communication
- Lessons learned: ours and yours
What happened?

• A Dutch CSP was hacked and fraudulent certificates were stolen
• Two main CA’s were compromised and many sub-CA’s
  • DigiNotar Public CA
  • DigiNotar PKI Overheid CA
• Fraudulent certificates were being used as hits on the OCSP’s proofed
• Government seized DigiNotar to control a gracefull transition to other CA’s
Video’s

2011-08-04 04:00:00
Video’s

2011-08-04 04:00:00
Building up a crisis

- **June**: Hack
- **July**: Fact finding, etc
- **August**: IR
- **Sept**: Crisis
- **Oct**: Parliament, fact finding, etc

- **June**: No role yet
- **Sept**: Coörd
- **Oct**: Expert
Crisis management in The Netherlands

- National Crisis Coordination center
- Advise Team
- Interdepartmental Crisis Council
- Ministerial Crisis Council
Crisismanagement in The Netherlands

- Escalating and de-escalating during a crisis

Diagram showing the roles and stages of crisis management, with labels for MCCB, ICCB, AT, and NCC, along with timelines for analyses, reports, actions, results, and investigations.
Organizational aspects

- Staffing
  - Growing and shrinking
  - Shifts and roles
- Continuing normal operations
- Splitting the organization
- Facilities
- Tools
  - Mailinglists
  - Skype
  - Record keeping
Communications

- Mobiles are it
  - Spare batteries
  - Record keeping
- Mailbox explodes
- Handing over tasks and reporting results
- IWWN: thanks again, CERT-Bund
Lessons learned

- PKI has become a critical infrastructure in itself
- Never assume that obvious measures are obvious
- PKI has no adequate response to CA-failure
- The trustlists in browsers and OSses are an important factor in PKI
- Certificates should be managed as assets
  - Know where and how they are used
  - Why not keep a backup certificate?
- Communicate early
  - Every bit helps and later on it might be out of your hands
Lessons learned

- Remember the 4th Law of GOVCERT.NL

An incident is never as bad as it seems.......always worse
Your Lessons learned
Questions?

aart.jochem @ ncsc.nl/ a.j.jochem @ nctv.minvenj.nl
Protect against unauthorized access by physical and logical compartmentation.

Instruct clients to take measures to protect certificates and services.

General requirements to increase level of control.

New PKI policy released by PA last Friday.