Tidbits of Crisis Management in Sweden

Lars-Johan Liman
Senior Systems Specialist
Netnod Internet Exchange

Euro-IX Meeting Oslo 2010-09-27

The Beginning

- January 2005: the hurricane "Gudrun" hit southern Sweden.
- Took down 70 million m^3 of forrest.
- 340,000 people lost power,
- … and telephone,
- … and the cell phone system went down as well.

- That is what we call …

The Awakening

- The guys fixing the cellphone base stations needed power.
- The guys fixing the power systems needed cellphone coverage.
- People in general needed both power and cellphone coverage and were getting noticeably upset
- The days went by …
  - 40 days to restore power to all homes!

Aftermath

- The Swedish Post and Telecom Agency (PTS) decided:
    - Create new group for national communications cooperation (NTSG)
    - Create new central system for damage assessment and information (GLU)
    - Roaming SIM cards for key persons
    - Conduct crisis exercises for authorities and industry

NTSG

- High-level executives from industry and authorities who have been empowered to make decisions.
- Prepared communication systems.
  - … and meeting places.
- Decides on resource allocation during crisis, with main focus on quick over-all restoration of systems.

GLU

- Web system with maps that shows "current state of service" for involved operators.
  - POTS
  - Cell-phone
  - Power
  - (Where's the Internet?)
- Service operators have direct access
- Public and privat parts

Roaming SIM cards

- SIM cards to be used only in crises.
- Will use any available cell networks regardless of operator.
  - Similar to “112” service.
- To be used by selected service and repair personnel.

Telö-09

- National Telecoms Exercise 2009
  - 2 day event in May 2009
- 18 participating organisations:
  - Telecom operators
  - Power companies
  - Internet service providers
  - Government agencies
  - Defence agencies
  - City administrations
  - … and an Internet Exchange point called Netnod.

What’s a Crisis Exercise?

- It’s a “role play”
- A scenario is rolled out.
- Conducted by a central management group,
- … with small local “extensions” at the various organisations.

The Central Management Group

- Provides the scenario.
  - 13 events, 84 incidents, 697 injects
- Fills the roles of all players that don’t participate.
- Acts as media.
- Turns the system clock.
  - Software: Exonaut
- Security monitoring.

The Local Management Team

- Local staff.
- Provides input to the scenario.
- Creates injects based on scenario and local environment.
- Sets up the local environment.
- Executes the exercise locally.
  - Coordinates with the central team.
- Evaluates the result locally.
- Reports result back to the central team.

The Scenario

- Coordinated and orchestrated terror attack, e.g.,
  - Communications bunkers powerless and blocked.
  - Power stations taken out.
  - Bomb threat at major airport.
  - Vital fiber cross connect demolished.
  - Insider puts incorrect DNS data in .SE rendering local DNS useless.
  - Cracker attacks on routers.

Training What?

- Decision making
  - Technical decisions
  - Chain of command
- Cooperation between
  - Providers
  - Authorities
- Communication with the public
  - through press and other media

Preparations

- Go through entire Exonaut to see what affected us.
- "Fake" monitoring system.
- Normal ticket system with marked tickets.
- Special telephone numbers.
  - Note: the central team only thought of telephone and fax for communication!
- Food and drink!
- Logging.

Experiences

- Participate with a small organisation = problems.
  - Local team = me, myself, and I.
  - + one seriously qualified admin person thankfully provided by PTS.
- Regulators have limited understanding of how the Internet works.
  - I had to step into the central scenario group to help prevent some embarrassment.

Experiences/conclusions

- Technically our staff did very well.
  - Correct analysis and fault isolation.
  - Good prioritisation.
  - Proper actions.
- Interaction/cooperation with others
  - Did OK, but the scenario required only limited interaction from us.
- Sustainability is a problem for small organisations.

The grenade …

- “Other organisation” kicked in an inject that wasn’t sync:ed with me.
  - Improvised …
  - Staff drew unexpected conclusions.

Experiences/conclusions

- Senior staff at conference abroad. (Really!)
  - Deemed untrustworthy by local staff.
  - All their access to company systems revoked.
  - Telephone messages considered non-authoritative.
- Chain of command got really interesting…

Finally

- Good learning experience!
- Preparations = a lot of work.
- More process than technology.
  - … but that’s what you need to train. :-)
- The really good experiences come from the unexpected.
- Great fun!
- Next time – September 2011
  - Preparations underway …

Questions?