

• • • • •  ØVELSE IKT 08



Crisis Management – Simulation and Training

Norwegian Exercise IKT 08

Sigtuna, 19th March 2008

Stein Henriksen

Executive secretariat

stein.henriksen@nsm.stat.no

IKT 08 – Exercise type

Was

- About Information and Communication Technologies (ICT) in Critical Infrastructures (CI)
- First exercise of this nature in Norway
- A co-operative effort among about 30 participants under the sponsorship of the DSB and the NSM
 - The DSB provided exercise planning expertise while the NSM provided ICT threat knowledge
- A distributed, multi-location table top exercise
- About communications between actors
- About shared, but differing responsibilities at agency level and including private actors
- A 2 –stage exercise, **IKT 08** was followed by **SNØ 08** (Civil National Exercise: a yearly cycle involving ministries), reusing the scenario

Was not

- A "live" technological exercise
 - No release of real malware
 - No dummy networks
 - Not an exercise on analyzing malware



Participation

- Ministries (Exercise SNØ 08)
- 30 odd central and important actors from private and public sectors, including planning groups
 - Banking and finance sector
 - Electric power supply sector
 - Oil and gas sector
 - Telecommunications sector
 - Justice and Police sector
- Planning in each group headed by relevant gov't agency
 - Management of sensitive information an issue
- Including national security related agencies



Main goals of exercise

- **The main goal of exercise IKT 08 was to gain experiences relevant to the development of the ability and capacity of society to manage the phases before, during, and after massive attacks on digital infrastructures**
 - **Target 1 - establishing an understanding of responsibilities and roles before, during, and after the event**
 - **Target 2 – exploring the suitability of existing emergency planning**
 - **Target 3 – testing vertical and horizontal information sharing between decision-making levels before, during, and after the event**
 - **Target 4 – testing media management and crisis communications before, during, and after the event**



IKT 08 Exercise play

- IKT 08: 1. – 3. December 2008
- SNØ 08 : 9. December 2008

Main focus for crisis management (IKT 08)

- Day 1: attempted bank Trojan attacks
- Day 2: attempts to disrupt power supply
- Day 3: attempted denial of service attacks against telecom sector

DISTAFF at DSB Tønsberg containing response cells, including sector experts and "the Bad Guys" (established in background scenario)

Media play from media cell in Oslo

All other players participating from their own premises



Crisis management by players

- DISTAFF deliberately stalled the question of "lead ministry", forcing participants to co-ordinate horizontally
 - - dirty trick, but realistic
- Initial confusion and lack of joint situational awareness
- All players were extremely busy
- NSM department NorCERT is nat'l CERT and assumed role of co-ordinating technological management
 - NorCERT ticketing system received average of 1 communication per 2 minutes throughout exercise & forwarded 7 SITREPs
- NSM SITCEN assumed role of policy co-ordinator vis a vis ministerial level; produced
 - 5 SITREPs with info from other agencies
 - 1 risk assessment
 - 1 nat'l security situation assessment (classified SECRET) jointly with other security agencies



Numerous lessons learned (1)

- Planning process exposed interdependencies and vulnerabilities
 - Security issue, led to "no observers" policy
- Planning process highlighted need for cross-sectoral co-ordination
- Sudden need for fast co-ordination is a challenge; pre-crisis networking is essential
- National CERT is crucial, fast-acting resource
- Nat'l CERT needs access to powers invested in other agencies, particularly Post & Telecom (legal powers to shut down IP addresses and .no domains controlling botnets)
- Nat'l continuity of gov't planning is not relevant for cyber crisis management
- Fast electronic info exchange is essential for early situation awareness



Numerous lessons learned (2)

- Sharing of classified information with private actors is a challenge
- Conflict of interest exposed between law enforcement and continuity of operations
 - Between law enforcement agencies, the Post & Telecom agency, and the NorCERT
- Actors are frequently not aware of their dependency on the Internet
 - Nasty surprises when Internet shuts down
- ICT is a cross-cutting issue; the establishment of lead ministry for crisis management cannot be presumed
 - Confirmed by inter-ministerial play in SNØ 08
 - Major outstanding issue
- Private public partnerships within sectors worked very well with complete mutual trust



Thank you for your attention !