



# Information Security Authority: Actions and Targets

## - Network Vulnerabilities

Director Timo Lehtimäki FICORA



# Vulnerabilities?

# Vulnerabilities - Yes and No



Viestintävirasto

CERT-FI - 2011 - Windows Internet Explorer

http://www.cert.fi/haavoittuvuudet/2011.html

File Edit View Favorites Tools Help

Tämä sivusto on TURVALLINEN Ilmoita meille

Favorites Ehdotetut sivustot Hanki lisää lisäosia

CERT-FI - 2011 Suomen Erillisverkot Oy - Uut...

CERT-FI på svenska | in English Viestintävirasto

Etusivu Varoitukset Tietoturva nyt! Haavoittuvuudet Ohjeet Katsaukset Palvelut Esitykset

Kohde Etusivu > Haavoittuvuudet > 2011

Hyökkäystapa

Hyväksikäyttö

Ratkaisu

**2011**

2010

2009

2008

2007

2006

2005

2004

2003

2002

2001

Haku

Lisätietoa haavoittuvuuksista

**2011**

Päiväys	Numero	Otsikko
21.02.2011	025/2011	<a href="#">IBM Lotus Dominon LDAP-toteutuksessa haavoittuvuus</a>
17.02.2011	024/2011	<a href="#">Haavoittuvuus Microsoft Windows SMB-protokollassa</a>
16.02.2011	023/2011	<a href="#">Haavoittuvuus Oracden tietokantaohjelmistoissa</a>
16.02.2011	022/2011	<a href="#">Päivitys Oracle Java-ohjelmistoihin</a>
14.02.2011	021/2011	<a href="#">Adobe Shockwave Playerin päivitys korjaa kriittisiä haavoittuvuuksia</a>
10.02.2011	020/2011	<a href="#">Linksys WAP-610N WLAN-tukiaseman haavoittuvuus</a>
10.02.2011	019/2011	<a href="#">Realplayerin päivitys korjaa haavoittuvuuden</a>
10.02.2011	018/2011	<a href="#">Päivitys Google Chrome -selaimen</a>
10.02.2011	017/2011	<a href="#">Päivitys Adobe Flash Player -ohjelmistoon</a>
09.02.2011	016/2011	<a href="#">IBM Lotus Domino -ohjelmistossa useita haavoittuvuuksia</a>
09.02.2011	015/2011	<a href="#">Päivityksiä Adobe Reader- ja Acrobat-sovelluksiin</a>
08.02.2011	014/2011	<a href="#">Helmikuun Microsoft-päivityspaketti julkaistu</a>
08.02.2011	013/2011	<a href="#">BMG Patrol -ohjelmistojen haavoittuvuus</a>
03.02.2011	012/2011	<a href="#">Postgresql-ohjelmiston haavoittuvuus voi mahdollistaa koodin suorittamisen</a>
03.02.2011	011/2011	<a href="#">MediaWiki-ohjelmiston päivitys korjaa kaksi haavoittuvuutta</a>
31.01.2011	010/2011	<a href="#">VLC Media Player -ohjelmiston haavoittuvuudet</a>
31.01.2011	009/2011	<a href="#">Haavoittuvuus RealPlayer-ohjelmistoissa</a>
31.01.2011	008/2011	<a href="#">Microsoft Windows -käyttöjärjestelmän MHTML-haavoittuvuus</a>
27.01.2011	007/2011	<a href="#">Haavoittuvuuksia OpenOffice-ohjelmistossa</a>
27.01.2011	006/2011	<a href="#">Päivitys Opera-selaimen</a>
19.01.2011	005/2011	<a href="#">Oraclelta kriittisiä päivityksiä tammikuun päivityspaketissa</a>
11.01.2011	004/2011	<a href="#">Microsoftin päivitykset korjaavat kolme haavoittuvuutta</a>
06.01.2011	003/2011	<a href="#">Haavoittuvuus Internet Explorerin mshtml.dll-kirjastossa</a>

CERT-FI  
PL 313  
00181 Helsinki  
Puh: 00 6066 510



# Challenges?



- IPv4->IPv6
- IP-based networks
- R&D
- Ownership
- National know-how
- Network operation centers
- Cloud-computing, cross-border services
- ...



# Problems?

- Case Salla
  - "Asta, Veera, Lahja and Sylvi caused quite a mess"
  - Environmental stress
  - Human errors
  - Konfiguration problems
  - ...
- > Disruptions in information and communication infrastructure are threatening business-life, citizens and authorities



Cavalry is coming ;)

Actions and targets of  
authority:

Information security and  
situational awareness!

## What?

- Information about the status of communication networks and services
- Information is e.g. accessibility, functionality, capability or development of networks and services:
  - Functionality – faults and disturbances
  - Accessibility – network coverage, supply of serviceja
  - Capability – network capacity
  - Development – structural changes of network
  - Information security

- Situational awareness can be:
  - Proactive: information about upcoming events,
    - Service planning, network development and changes etc.
  - Real-time: information about current situation,
    - Faults and disturbances, fixing schedulehavaitut, network accessibility, etc.
  - Subsequent/reactive: information about history events,
    - Statistic follow-up
- Just on time, easily and usable format!



- Three entities, which each include several services:
  - Functionality
    - service 1: information on faults and disturbances to the public (web-based service)
    - service 2: collaboration tool for closed user-groups
    - service 3: situational reports, surveys, guidance
  - Accessibility and quality
  - Network structure



- Service 1 (faults and disturbances) design and implementation starts 2011
  - FICORA is collecting information about present practises and readiness of telecompanies
  - Requirements for telecompanies are included in regulation 57 – new working group will be established



## Service 2: collaboration tool for closed user-groups

- Centralized tool for information sharing and distribution is needed
- Scalability is needed in order to add users and services - services will be implemented one by one
- Planning, implementation and maintenance requires long-term commitment from both industry and authorities
- Feasibility study starts 2011



- Ability to detect information security threats or incidents targeted to own organization is limited
- Systems used to handle and deliver classified information and secure communication channels are very rare

## Needs:

- International cooperation network to handle information security incidents
- National monitoring system to detect information security incidents and anomalies
- Development of NCSA-operations: both national and international requirements handled by same criteria and same organisation

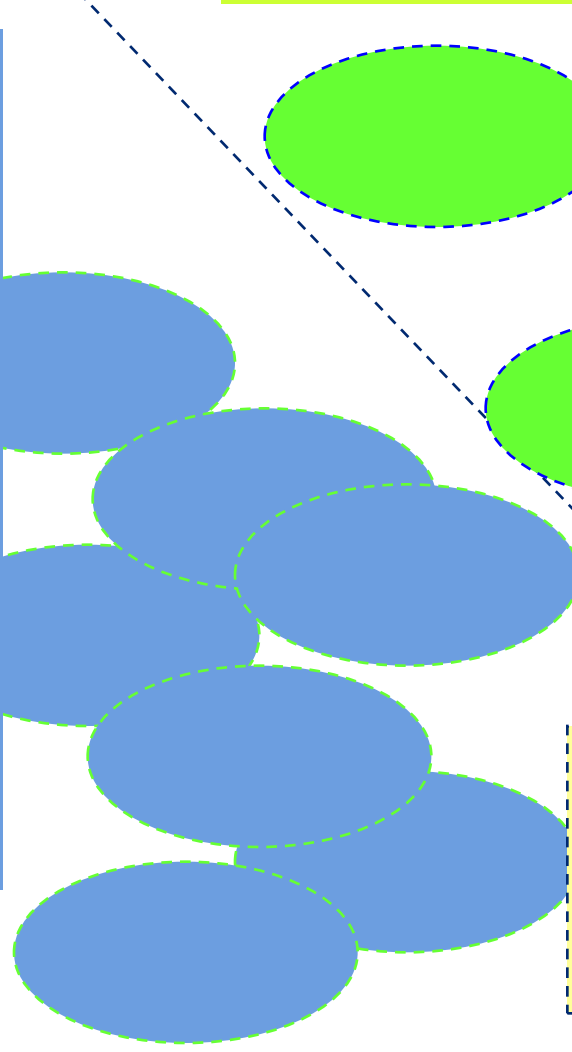
# Network and information security operation centre?



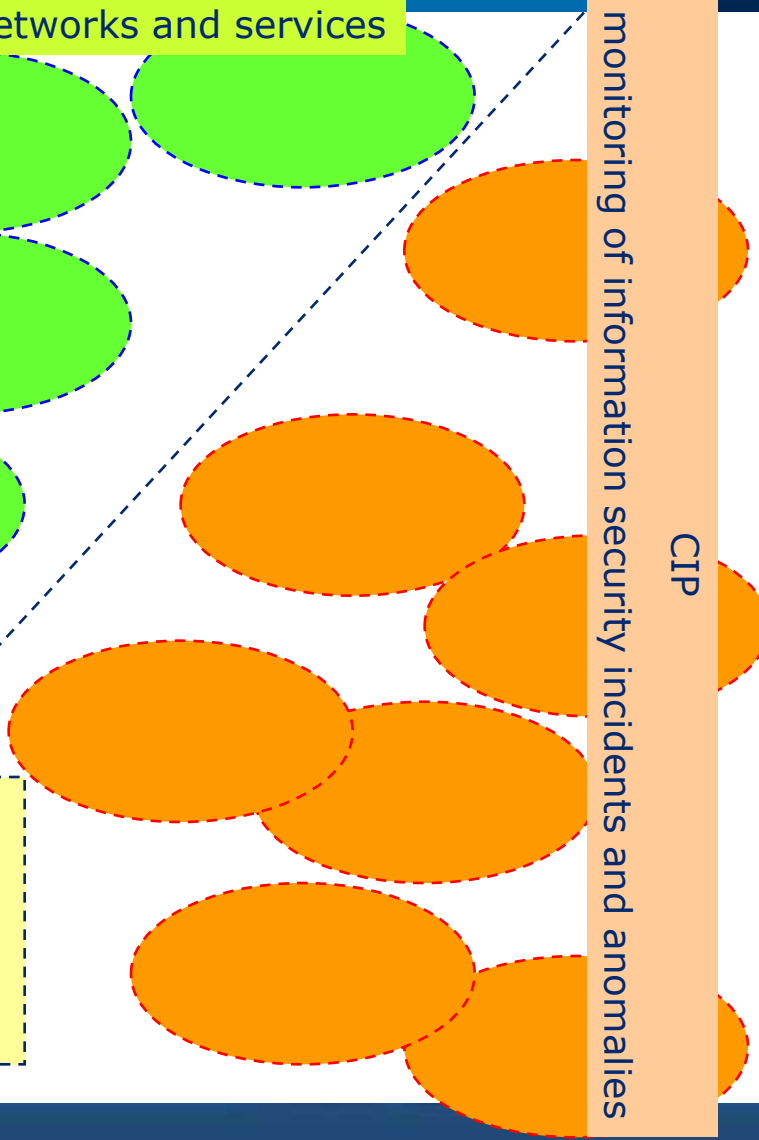
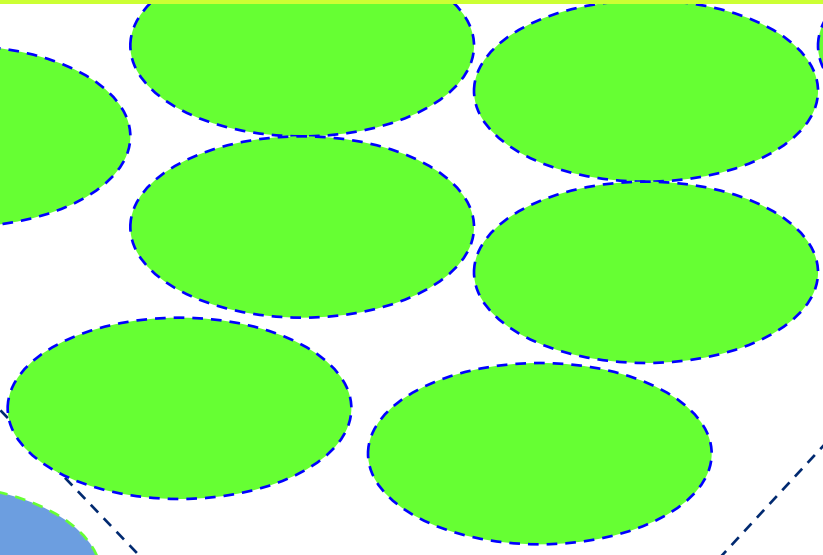
Viestintävirasto

Information security and functionality of public networks and services

Government ICT-environment  
monitoring of information security incidents



FICORA 24/7  
CERT-FI  
Faults/disturbances  
NCSA-FI  
.FI



monitoring of information security incidents and anomalies

CIP



**Questions!?**