Swedish IT Incident Centre

Pär Österberg
SITIC

SITIC’s task

Support society in the efforts against IT incidents by:

- Establishing a system for information exchange regarding IT incidents between community organizations and the team
- Being able to quickly communicate information to the community regarding new problems, potentially threatening to IT systems
- Aggregate and publish statistics as input to continuous improvement of the preventive work
- Providing information and advice regarding preventive efforts
Cooperation

- FIRST
- TF-CSIRT
- European Government CERT (GovCERTs in Finland, The Netherlands, UK, France, Germany, Norway and Sweden)
- Nordiskt CERT - forum (NCF)
- Sweden
  - SUNET CERT
  - TeliaSonera CERT

Constituency

According to the task from the government:
- Government agencies
- Regions
- Municipalities
- Companies
Watch & Warning

- Open Sources
- Subscribed Sources
- Other Sources

Collection tool (html, mail, rss)

Watch & Warning
*One scheduled staff responsible for watch & warning
*First filtering ("daily") published in-house
*Filtered data pushed through a vulnerability scoring system
*Decision on production in corridor

Production
*Daily (first filtering) to tight list of recipients
*Alert messages
*Advisories
*Messages to site-owners

Lab-verification (opt.)

Test your computer
- Nessus based
- Over 230 000 performed tests since April
- https://www.testadatorn.se
Internet traffic measure

- Probes on major ISP

Ongoing project

- Distributed IDS
- Log analyze (http, smtp and firewall)
  - send your log file and compare it with others
- Test your password
  - javascript for testing the complexity and strength of a password
Swedish IT Incident Centre

Swedish IT Incident centre
National Post and Telecom Agency
P. O. Box 5398
SE-102 49 Stockholm
Tel +46-8-678 57 99
Fax +46-8-678 55 05
sicit@pts.se
www.sitic.se