Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

CERT-FI
First 12 months

Kauto Huopio

FICORA

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

FICORA

Finnish Communications Regulatory Authority

- communications regulator
  - operating under the Ministry of Transport and Communications
- total staff ~230 persons
  - academic background ~100
- budgetary independence
  - all funding from fees collected from user organisations

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

FICORA operating areas

- Telecommunications
  - telecommunications regulation
  - inspection of operators
  - telecommunications standardisation
  - information security
- Radiocommunications
  - radiocommunicatons regulation
  - frequency management & surveillance
  - equipment market control

FICORA operating areas cont.

- Electronic media
  - monitoring on TV advertising
- Television fees
  - collection of television fees
- Postal operations regulator

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Information security

- FICORA's telecommunications regulator "traditional area": security issues regarding telecommunications networks and operators
- Present goverment program: "How to administratively organise security management issues regarding telecommunications networks" (..including data networks & Internet)
  - secure telecommunications seen as key issue
- TIHA –project result: COMSEC -> FICORA
  QCB -> commercial vendors
  CERT -> FICORA
- Information security unit formed 1.7.2001

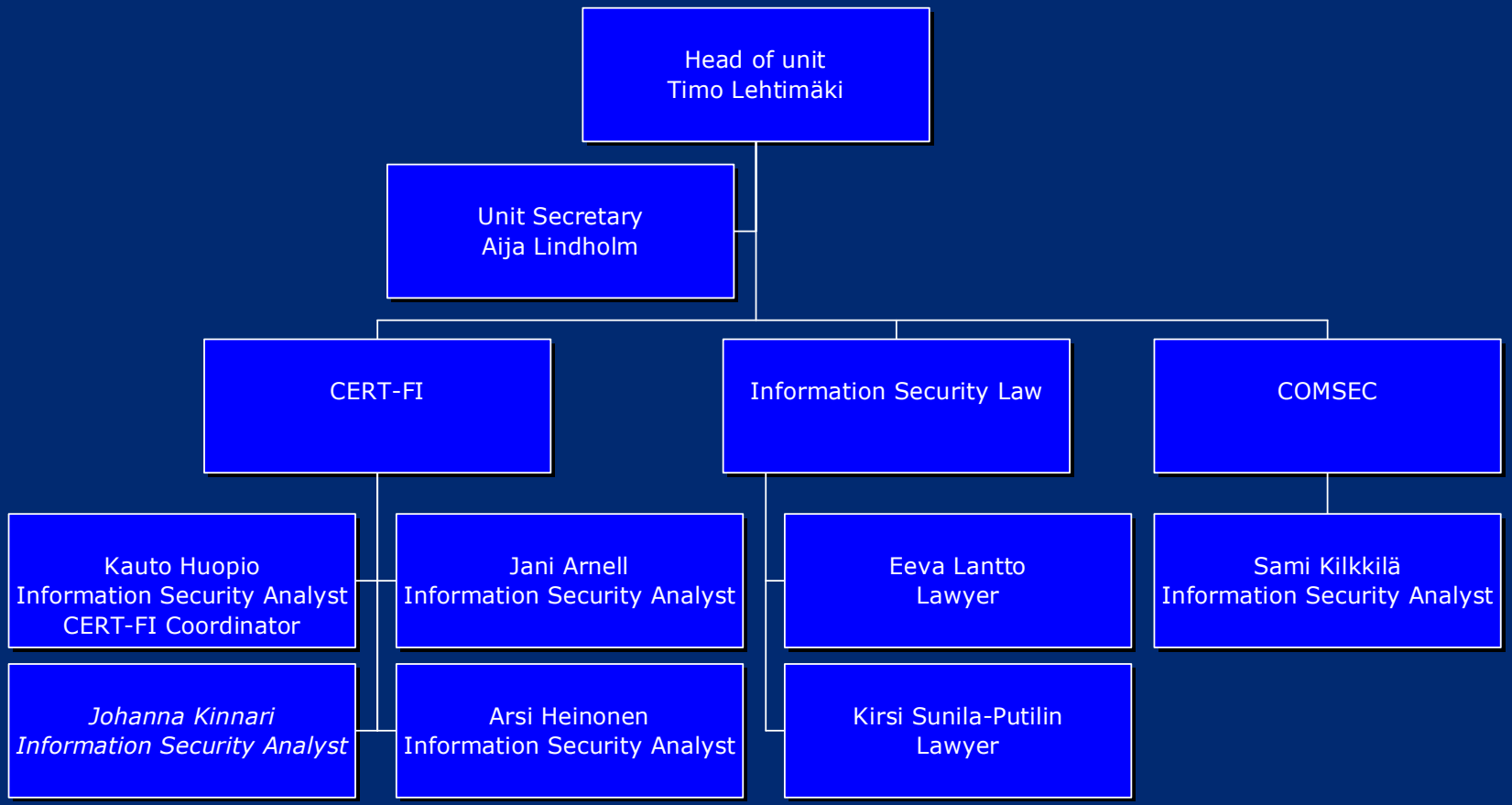
Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Information security unit: Key operating areas

- Telecommunications security (COMSEC)
- Privacy in telecommunications
- Electronic signatures / PKI
- E-commerce
- Observation and assistance of/to security incidents – CERT-functionality

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Unit personnel



Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

CERT FI – main tasks

- to observe and collect information on threats concerning telecommunications infrastructure
- prevent harmful effects caused by telecommunications security issues
- inform public on observed vulnerabilities and security issues
- give public advice on security incident response
- follow up international development in the area

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Target group

- Finland
- Telecommunications service providers
  - traditional telcos
  - data operators, ISP:s
  - value added service providers
- Public and private sector
- Individual citizens

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

CERT-FI timeline

- planning started 1.7.2001
- present personnel recruited 4Q/2001, 4Q/2002
- open for business 2.1.2002
- first major incident OpenSSH outbreak Jan/Feb 2002
- TERENA TI Level 2 application 1Q/2003
- FIRST membership application 1Q/2003

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

”CERT-legislation”

- Modifications to the Act on Telecommunications Security (1.9.2002)
- CERT function is given officially to FICORA
- telecommunications operators (including data carriers & ISP:s) are required to report significiant security events and network problems to FICORA
- operators are required to pay an administration fee to FICORA

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Significiant event?

- basic ideology: ”events that one should follow anyhow”
  - concentrated portscanning
  - significiant traffic anomalies
  - break-in –attempts
  - attacks that have an effect to usability
  - (naturally) successiful breakins
  - failures on basic services (SMTP,DNS, DHCP)
  - important routing mishaps
  - detected software vulnerabilities
  - social engineering attempts

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Partners - Finland

- Customers/other CERT:s participate in CERT working group
  - meets 4-5 times / year
- Other CERT groups inside Finland
  - FUNET CERT (academic research network)
  - operator CSIRT/abuse teams (Sonera, Finnet Group etc)
  - major IT outsourcing houses (TietoEnator, Novo etc)
- Police – various units
  - Central Criminal Police (KRP) Computer Crime Unit
  - Security Police (SUPO)
- Finnish Defence Forces

CERT-FI in figures - year 2002

- Recorded contacts: 285
- of which incidents 138
  - incident=event or related series of events affecting communications security

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

CERT-FI: warnings

- 93 compared to CERT/CC ~25
- European/Finnish software enviroment
  - no AOL Instant Messenger issues..
- slightly more relaxed warning release rules vs. CERT/CC
  - if public information, exploit exists and/or ”sensible” resolution possibilities -> release
- trying to limit the Microsoft warning flood
- subscribers to CERT-FI-ALERT mailing list: ~800

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Training & education

- WWW-site with general information on security issues
- general whitepaper –type documents on
  - personal firewalls
  - security issues with P2P networks
  - security issues with IRC / instant messaging software
  - WLAN security
- popular lectures / presentations in conferences

CERT-FI: vulnerability coordination

- no real cases leading to significiant vulnerability coordination activities..yet
- 8 cases raported directly to CERT-FI (cc:)
- policy on vulnerability information handling available (finnish)
- being a government organisation causes additional legal considerations

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Situational awarness

- all the traditional securityfocus mailing lists plus..
  - cisco-nsp, juniper-nsp,
  - full-disclosure, nsp-sec
  - NANOG, operator forums
  - virus bulletins
  - local finnish lists & newsgroups
  - N websites, traffic monitors
- all important finnish operators under speed dial
- getting distilled information is not enough, must read the anyway

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

CERT-FI as part of incident response process

- key questions: WHAT, HOW, TO WHERE
  - not so important: WHO
- Attacked enviroment in safe mode and prevention of further damage
- Can sanitize information
- Good experiences
- Protection of evidence
- Guidance to police contacts

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Incident highlights 2002

- OpenSSH breakin series Jan/Feb 2002
- Slapper/Scalper OpenSSL/Apache issue
- Many worm-related issues (getting distribution sites of exploit code used by the worm shut down – these not in Finland
- Assistance in the Sonera CDR case

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

A word on DDoS

- wasted bandwidth = money on IP capacity
- internal tracking / limitation resources vary from operator to operator
- ..not to mention inter-operator tools/processes
- It is not just IRC servers but
  - mail servers
  - core routers
- Top attacks we've observed are in the 1 Gbit/s range – this is costing operators money
- tools, resources, methods to combat DDoS available!

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Current/future concerns

- really nasty worms/viruses
- WLAN security
  - wardriving, warchalking, warspamming, war-whatever
- Attacks towards network infrastructure (routers, other active network elements)
  - first are out there
  - groups trying to specialise themselves on transforming Cisco boxes to DDoS generators
  - Juniper – BSD-enviroment
- Attacks towards M2M (machine-2-machine) communications
  - equipment with added IP connectivity

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

CERT-FI in 2003

- personnell 3 -> 4
- operational support systems development
  - incident handling system
  - IDS / attack data integration project
- CERT test enviroment
  - monitoring of ”internet baseline noise”
    - what is arriving into a empty IP connection
  - vulnerability evaluation platfoms (all major OS:s)

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Contact details

Telecommunicatons network –sector director

Mr. Tapani Rantanen

Head of Information Security Unit

Mr. Timo Lehtimäki

Information Security Analyst /
CERT-FI – coordinator

Mr. Kauto Huopio

tel. +358-9-6966772
mobile +358-50-5826131

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Contact information

Viestintävirasto / CERT-FI

http://www.cert.fi

cert@ficora.fi

duty desk +358-9-6966510 (office hours)

fax +358-9-6966515

PGP-fingerprint:

03B1 F7F0 6892 F27F 15D1

A98F D351 7DA8 3CDA 0200