Training for CSIRT staff

Andrew Cormack, Jacques Schuurman, Claudia Natanson, Wilfried Woeber, Gareth Price

TF-CSIRT

CSIRT staff are different

Not just sysadmins

Not just network techies

Though we take both of those for granted

- Or learn them elsewhere

Filling in the gaps is important

Target Audience

Members of new teams

New members of existing teams

Assumed already to know how the Internet works

- Course teaches how it breaks

Based in Europe

- CERT-CC series of 3&4 day courses in USA

Course Objectives

Students should learn

- Tasks involved in operating a CSIRT
- Skills needed by CSIRT staff
- Tools and techniques of incident response
- Need for links with other organisations

Course Modules

Legal Issues

Organisational Issues

Technical Issues

Market Issues

Operational Issues

Systems Issues

Legal Issues

Rules & laws

Harmonisation

Jurisdiction

Powers of investigation

Contacts with law enforcement

Access to and use of restricted tools

Organisational Issues

Your ISP

Your constituency

Assets and risks

Risk management

Security policy templates

- For your customers
- For your team

RFC2350

Public functions

Press contacts

Sister organisations

FIRST etc.

Staffing issues

Technical Issues

- Operating Systems
  - About the OS
  - Network stacks
  - Vulnerabilities & back doors
  - Integrity
- Forensics & Data mining
- Networks
  - IP/ICMP
  - TCP/UDP
  - Higher level protocols
  - Masquerading & hijacking
- Encryption
- Certificates & PKI

Market Issues

Vendors

Commercial teams

Security bulletins

Undisclosed vulnerabilities

Other sources of information

Operational Issues

An operational framework

Incident response

- Reporting templates
- Tracking & Bookkeeping
- Taxonomy

Management reports

Other activities

Trust brokers

Finding contacts

Other (reliable) sources of information

Systems Issues

Recovery

Monitor

Audit

Other activities

Back To Basics

e-mail address and telephone number

operating hours (9 to 5, 24 x 7 x 365)

publicity for these three items

guidance on what to do

somewhere for them to work

people to react to messages

a customer

Building

Access levels and hours of access

Access Control Locks

Alarm - intrusion, fire

Guard - access control and visitor management

Cameras

Power

Office

Lock

Alarm

Camera

Secured area

Separate area for servers, backups, forensic, secure store

Furniture

Locks - key, code or combination

Desks, workbenchs, racking

Pedestals

Filing Cabinets

Security tethers for expensive hardware

Welfare

Heating - working hours

Lighting - DSE

Health and Safety - arriving, working and leaving

Catering - canteen or machines

Cleaning - monitored or clear desk

E-mail

E-mail - access, using mail, using pgp

Multi-user access, audit

Connected to local network or standalone Internet connected

Telephone Number

Free or paid

Automatic Call Diversion

PBX, DEL backup

answer phone, divert

incoming and outgoing on separate lines

handsfree, wirefree, mobile

Reporting Templates

Paper for faxing or snail-mailing

Scripts/Forms for telephone calls

E-mail

Web-based - to e-mail

Web-based - direct into database

Work Management

Off the shelf or custom

Get as much automation as you can afford

Application - access, admin, using

Internet or Local Network only

Performance Monitoring And Reports

Terms of Reference/Charter/Contract (RFC2350)

Reporting agreements

Memos of Understanding

Service Level Agreements

Work monitoring

Reports

Quality related work

Finding Contacts

Regular

- TF-CSIRT
- FIRST

Per Incident

- ARIN, RIPE, APNIC
- TF-CSIRT
- FIRST

Trust Brokers

TI

FIRST

Transferring incident information

Reporting templates

Taxonomy

Reliable Information Sources

Other (reliable) sources of information

Course format

Modular to ease delivery and maintenance

Modules include

- Presentations
- Workshops
- Discussion

Full course takes two days

- Allows informal discussion in evening

Progress and plans

Initial development by TF-CSIRT sub-group

Draft syllabus for discussion in January 2001

Development of modules by community

- Perhaps professional advice for legal section!

Aim for delivery during 2001