4. Exercise: Developing CERT Infrastructure

Main Objective	To learn what kind of software and hardware solutions could be used to provide a particular CERT service for a constituency.	
Targeted Audience	Technical and management CERT staff.	
Total Duration	Roughly 3 hours	
Time Schedule	Introduction to the exercise	15 min.
	Task 1: Incident handling – incident analysis	45 min.
	Task 2: Further 3-5 services	90 min.
	Summary of the exercise	15 min.
Frequency	The exercise should be carried out when a new team is being established or plans to expand its services.	

4.1 GENERAL DESCRIPTION

The purpose of this exercise is to learn what kind of software and hardware solutions could be used to provide a particular CERT service for a constituency. By doing this exercise, students will learn about the connection between a set of services defined for their team and available IT solutions. This will help them to provide their services more easily and more effectively.

As a trainer, you should become familiar with the CERT services base, listed by the CERT/CC CERT at http://www.cert.org/csirts/services.html. This will be the basis of the discussion. It is recommended that for every service, the trainer should compose a list of freely available (as well as commercial, if needed) software solutions needed to provide the service.

All discussions should be moderated by the trainer.

4.2 EXERCISE COURSE

The course of this exercise is as follows.

4.2.1 Introduction to the exercise

At the beginning, introduce students to the exercise, outlining what its main tasks are and how the exercise will be carried out. This exercise consists of two main tasks:

TASK 1: Step by step example: Incident handling – incident analysis; and

TASK 2: A further 3-5 scenarios.

At the beginning the students should receive a short introduction to the CERT services base, listed by the CERT/CC CERT on the website: http://www.cert.org/csirts/services.html. The next

task would be to challenge the students to create a concept for providing these services using a proposed hardware and software infrastructure. You should give an example of a step-by-step exercise to get the students to understand how to proceed. In this exercise, the *incident handling – incident analysis* service is chosen. Further scenarios will depend on what you and the students agree upon.

4.2.2 Discuss the proposed infrastructure for the *incident handling – incident analysis* service

Hand out the two diagrams shown below to the students. Your goal is to discuss them with the students, asking the students to point out the strengths and weaknesses of the proposed solutions. You should lead the students by asking them questions, and step by step bring them closer to possible answers. Note, that the answers do not have to be same as in this example, but should cover a similar set of aspects. The questions are presented below.

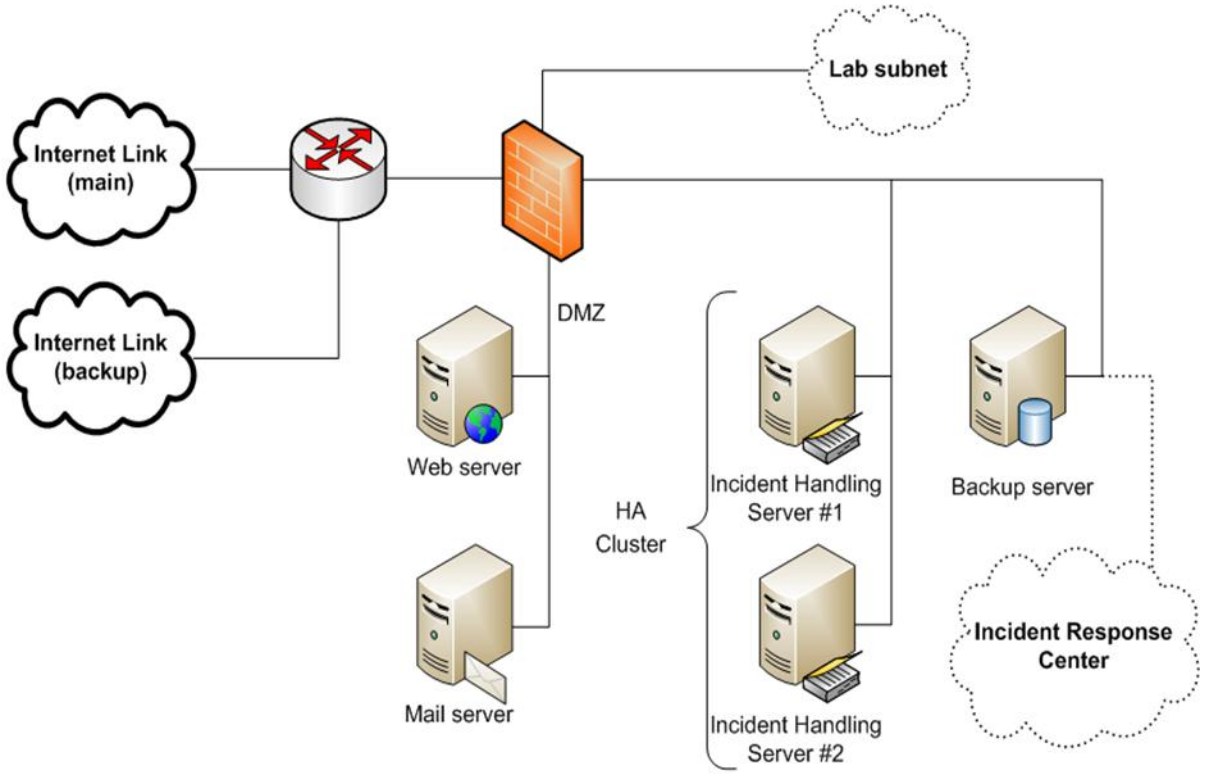

Figure 1: Sample CERT network infrastructure

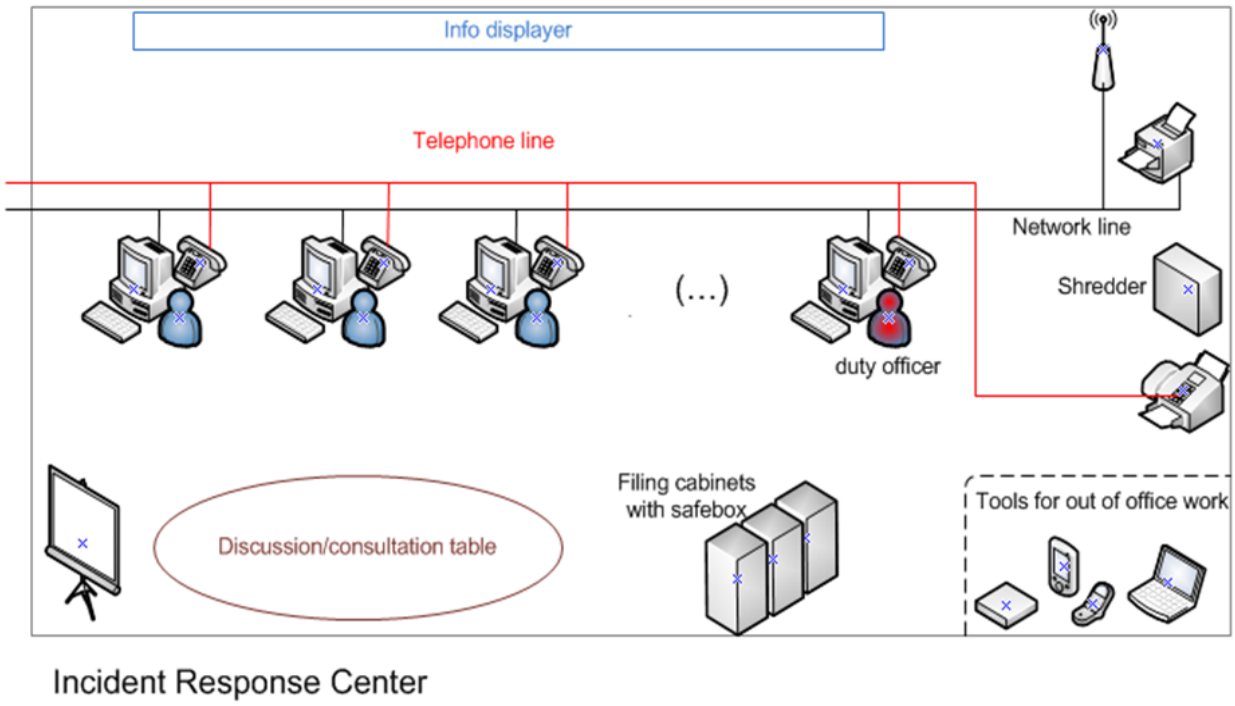

Figure 2: Incident Response Center

Listed below are possible questions that could be asked regarding the incident handling service. Note that these are just suggestions and not an attempt at enumerating every possible issue. The answers are just examples as well and may not cover every issue. You should carefully think through the issues below and come up with additional answers or answers of your own, so that you will be able to moderate the discussion accordingly.

- Incidents could be reported via several ways or channels. Which of them should be maintained by CERT teams as a minimum?
  - The most basic channel is via the Internet. Usually CERT teams use e-mail or/and web-page forms. Also telephone and fax should be available as a minimum. Every team should have a publicly available PGP key.
- What tools can be used to better organize teamwork and information flow – especially for incidents reported via the Internet?
  - A possible open source incident handling system that could be used is Request Tracker for Incident Response (RTIR: http://bestpractical.com/rtir/). If students do not know about RTIR, you could give a short overview of this tool. Look at the RTIR requirements.
  - A mail server is needed. If you use Linux, free ones include Postfix or Sendmail.

  - All mails targeted at the incident response centre should be passed through – no anti-spam or anti-virus rules should block traffic, or if they do, they should do it in a manner that enables the analysis of such traffic (*look also at the question: how to secure CERT infrastructure?*).
  - A web server will be useful: Apache is a possible choice.
  - A large information display in the incident response centre, which everyone can see, is a good idea: it could be a projector which projects information onto a wall or screen or LCD/plasma displays. Information about current threats could be displayed here. What are the possible sources of such information?

- How to better organize teamwork in respect of telephone and fax?
  - There should be an established position of 'duty officer of the day'. Every team member should hold this position interchangeably. The duty officer is responsible for, amongst other things, answering calls and faxes.
  - How phone calls are to be handled outside working hours should also be addressed.
  - Some new fax-machines can turn faxes into documents and send them via e-mail.
- Where to store incident reports and why is this so important?
  - Every result of incident handling could be potential evidence. Every incident (report, analysis and the effect of the investigation) and information gathered should be documented and safely stored. Every e-mail or other electronic data must be stored in a safe way on server(s) (with backup and HA cluster). All faxes must be stored in a safe place (for example in a safe-box). If you have the means, you should record your calls. 'This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evid;ence'[1].
- How to prevent a failure or outage of Internet or telephone connections and servers (hardware)?
  - There should be a backup Internet connection (via another autonomous ISP).
  - A backup telephone line (for example via GSM operator) is also a good idea.
  - To eliminate single points of failure, failover clusters should be deployed (critical services such as incident handling servers should consist of redundant nodes).
  - To minimize downtime and maximize availability, servers should be equipped with hot-swap RAID arrays and be connected to a UPS system.
  - Making regular backups is extremely important. Automatic backup system/scripts can be used. Created copies should be periodically verified to see whether they are usable.

- How to monitor your network for the failure or outage of servers, internet connections, etc?
  - A network monitoring system should be deployed to warn about failures or service status changes (open source solutions such as Nagios, Argus, Munin, and OpenNMS can be used). This information should be displayed on an information displayer (projector or LCD/plasma displays).
- How to respond to network failures?
  - Emergency procedures should be developed in case of a network failure.
- How to secure all CERT infrastructures?
  - Firewall(s) – how many, IDS, IPS?
  - An antivirus filter should be integrated with the mail server; AV protection with the latest virus definitions is highly recommended for workstations. (Please note that AV protection should not block incident reports because they may contain malware samples sent intentionally.)
  - The physical security of critical network elements should be assured.
  - Physical security should also cover confidential papers, faxes, documents, etc. Use a safe-box.
  - Server hardening delivers another layer of protection – one can use kernel patches (ie, PaX, Exec Shield, SE Linux, LIDS, grsecurity), hardening scripts (Bastille Linux), kernel-level packet filtering (netfilter), and host-based intrusion detection systems (OSSEC, tripwire).

Sometimes incident analysis requires going outside the network centre or lab. What tools are helpful in working remotely?

- Laptop
- Mobile phone
- Portable HDD or flash drive with large storage space
- PDA with internet connection and e-mail client, web browser, etc, connected via VPN?

What basic software should you have for incident handling in the context of the first questions?

- For handling an incident via e-mail you should have an e-mail client installed. (A possible free one is Mozilla Thunderbird.)
- For handling an incident via RTIR you should have Internet browsers installed. (Possible free ones are Mozilla Firefox and Opera.)

What basic software do you need to perform incident analysis in the context of?

- network forensics:
  - Tools for obtaining information about addresses, domain names, etc (CLI: whois, dig, host; there are also web-based online versions of these tools.
  - Tools for analysing pcap files (CLI: tcpdump, GUI: Wireshark)
  - Tools for analysing netflow data (CLI: nfdump, GUI: nfsen)
  - Lab isolated with firewall: subnet and hosts
- computer forensics:
  - Tools for data preservation (hardware: DriveBlocker, etc, ???)
  - Tools for data analysis (EnCase, etc, ???)
  - Isolated lab: hosts and subnet
- malware/binary analysis
  - Isolated and monitored lab: host or subnet (with different types of operating systems; an IDS/IPS will be useful to identify malware: Snorts)
  - Virtual environment (software: VirtualBox, Vmware
  - Reverse engineering tools

The checklists below could help you judge how well the students' ideas and solutions comply with the main assumptions.

Assumptions	yes/no
Backup Internet connection from other ISP	
Firewall(s) (how many), IDS, IPS, etc.	
Web server (HA cluster)	
Mail server	
Incident handling server (HA cluster) – for example for RTIR	
Central database (HA cluster)	
Backup server	
Services available from the Internet are separated from internal network by situating them in demilitarized zone (DMZ)	
Internal services such as backup, database and incident handling servers, as well as team workstations, are located behind firewall	
Lab subnet isolated with firewall	
Servers should be equipped with hot-swap RAID arrays and connected to UPS system	

Assumptions	**yes/no**
Fax machine	
Telephone	
Shredder	
Printer	
Established position of duty officer	
Filing cabinets	
Safe-box	
Info displayer – projector or LCD/plasma displays	
Extra tools	
Discussion/consultation table	
Screen/board	
Tools for outside work:	
- Mobile phone	
- PDA	
- Laptop	
- Portable HDD	

- **Task 2 Discuss the proposed infrastructure for a further 3-5 services**

Once the first task has been completed, a set of services should be chosen, partly by the trainer, and partly by the students. The set chosen should include services from all main categories such as *reactive services, proactive services* and *security quality management services.* About 3-5 services should be chosen.

In a manner similar to the previous exercise, the students should create a concept of providing those particular services using a hardware and software infrastructure. They should design a network environment, including computers, network devices and connections between them. It is important that the students face the task of the separation of the services in relation to their criticality. It is advisable that the trainer prepares, for each service, a basic set of

solutions (as in the example exercise) in order to facilitate discussion. A checklist would be useful to evaluate proposals. How could the topology presented in the first task be extended to accommodate the new services?

4.3 Summary of the exercise

Summarize the exercise. By going through so many services, you have established with your students quite large infrastructures. Compare these infrastructures with the one you initially thought of. Did the discussion contribute anything? If you have carried out this exercise before, how was the outcome different this time?

Encourage students to exchange their opinions, ask questions, and give their feedback about the exercise.

4.4 EVALUATION METRICS

Evaluating the results of this exercise. The main criteria should be how active the students were during the discussions. Did they introduce new ideas? Use the checklists you prepared beforehand to track what students missed.

4.5 REFERENCES

1. CERT services, http://www.cert.org/csirts/services.html.