Preparation 1

- Define actors, for each entity, who will be involved into the crisis cell. These actors should be documented in a contact list kept permanently up to date.
- Make sure that analysis tools are up, functional (Antivirus, IDS, logs analysers), not compromised, and up to date.
- Make sure to have architecture map of your networks.
- Make sure that an up to date inventory of the assets is available.
- Perform a continuous security watch and inform the people in charge of security about the threat trends.

Identification 2

Detect the infection

Information coming from several sources should be gathered and analyzed:

- Antivirus logs,
- Intrusion Detection Systems,
- Suspicious connection attempts on servers,
- High amount of accounts locked,
- Suspicious network traffic,
- Suspicious connection attempts in firewalls,
- High increase of support calls,
- High load or system freeze,
- High volumes of e-mail sent

If one or several of these symptoms have been spotted, the actors defined in the “preparation” step will get in touch and if necessary, create a crisis cell.

Identify the infection

Analyze the symptoms to identify the worm, its propagation vectors and countermeasures.

Leads can be found from :

- CERT’s bulletins;
- External support contacts (antivirus companies, etc.) ;
- Security websites (Secunia, SecurityFocus etc.)

Notify Chief Information Security Officer.
Contact your CERT if required.

Assess the perimeter of the infection

Define the boundaries of the infection (i.e.: global infection, bounded to a subsidiary, etc.).
If possible, identify the business impact of the infection.

Containment 3

The following actions should be performed and monitored by the crisis management cell:

1. Disconnect the infected area from the Internet.
2. Isolate the infected area. Disconnect it from any network.
3. If business-critical traffic cannot be disconnected, allow it after ensuring that it cannot be an infection vector or find validated circumventions techniques.
4. Neutralize the propagation vectors. A propagation vector can be anything from network traffic to software flaw. Relevant countermeasures have to be applied (patch, traffic blocking, disable devices, etc.)
   For example, the following techniques can be used:
   - Patch deployment tools (WSUS),
   - Windows GPO,
   - Firewall rules,
   - Operational procedures.
5. Repeat steps 2 to 4 on each sub-area of the infected area until the worm stops spreading. If possible, monitor the infection using analysis tools (antivirus console, server logs, support calls).

The spreading of the worm must be monitored.

Mobile devices

Make sure that no laptop, PDA or mobile storage can be used as a propagation vector by the worm. If possible, block all their connections.

Ask end-users to follow directives precisely.

At the end of this step, the infection should be contained.

Remediation 4

Identify

Identify tools and remediation methods.
The following resources should be considered:

- Vendor fixes (Microsoft, Oracle, etc.)
- Antivirus signature database
- External support contacts
- Security websites

Define a disinfection process. The process has to be validated by an external structure, like your CERT for example.

Test

Test the disinfection process and make sure that it properly works without damaging any service.

Deploy

Deploy the disinfection tools. Several options can be used:

- Windows WSUS
- GPO
- Antivirus signature deployment
- Manual disinfection

Warning: some worms can block some of the remediation deployment methods. If so, a workaround has to be found.

Remediation progress should be monitored by the crisis cell.

Recovery 5

Verify all previous steps have been done correctly and get a management approval before following next steps.

1. Reopen the network traffic that was used as a propagation method by the worm.
2. Reconnect sub-areas together
3. Reconnect the mobile laptops to the area
4. Reconnect the area to your local network
5. Reconnect the area to the Internet

All of these steps shall be made in a step-by-step manner and a technical monitoring shall be enforced by the crisis team.

Aftermath 6

Report

A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost

Capitalize

Actions to improve the worm infection management processes should be defined to capitalize on this experience.

[redacted]

Abstract

This Incident Response Methodology is a cheat sheet dedicated to incident handlers investigating a precise security issue.
Who should use IRM sheets?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes and do not panic. Contact your CERT immediately if needed.

Incident handling steps

6 steps are defined to handle security Incidents

Preparation: get ready to handle the incident
Identification: detect the incident
Containment: limit the impact of the incident
Remediation: remove the threat
Recovery: recover to a normal stage
Aftermath: draw up and improve the process

IRM provides detailed information for each step.