CSIRT – Introduction to Security Incident Handling

P. Jacques Houngbo
AIS 2013Technical Workshops
Lusaka, Zambia , June 2013

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"- Bruce Schneier
http://think.securityfirst.web.id/?page_id=12

AfricaCERT
United in promoting cyber security in Africa

References

- http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Introduction

- Objectives of the module :
  - Familiarize with computer security incident
  - Arise awareness on preparation
  - *Give first hands on training on incident detection*
  - Present the complete lifecycle of incident handling
  - Focus on :
    - External relationships to management, constituency and communities
    - Team internal measures to enhance level of quality in which the services are provided.

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Terminology

- Event – any observable occurrence within a system or network.
- Adverse event – an event which has a negative consequence.
- Security Incident - a violation or imminent threat of violation of IT security policies or standard security practices.

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Incident handling

- Handling incident – several phases
  - preparation: limit the number (and impacts) of incidents that will occur
  - detection, registration, triage, assignment: security breaches, incident classification, signs of incidents
  - containment, eradication, recovery: limit the spread, gather evidences, eliminate components, restore system to normal operation
  - post incident activities: lessons learned, data collected

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Incident handling – Preparation

- Preparation covers the three following groups of activities:
  - Establishing incident response capability
  - Making incident detection and analysis easy
  - Preventing incidents

Incident handling – Preparation
Establishing incident response capability (1/3)

- Communications and Facilities
  - Contact information (team members)
  - On-call information
  - Incident reporting mechanisms
  - Pagers or cell phones
  - Encryption software / digital signature
  - War room
  - Secure storage facility

Incident handling – Preparation Establishing incident response capability (2/3)

- Analysis Hardware and Software
  - Computer forensic workstations and/or backup devices
  - Spare workstations, servers, and networking equipment
  - Blank media, Removable media
  - Laptops, Easily portable printer
  - Packet sniffers and protocol analyzers
  - Computer forensic software
  - Evidence gathering accessories

Incident handling – Preparation Establishing incident response capability (3/3)

- Analysis Resources
  - Port lists
  - Documentation
  - Network diagrams and lists of critical assets
  - Baselines
  - Cryptographic hashes
- Mitigation Software
  - Media
  - Security patches
  - Backup images

Incident handling – Preparation Establishing incident response capability - *Practice*

- 4 groups : one group per task
- Tasks:
  - Design a War room
  - Design a Secure storage facility
  - Enumerate tools for network diagrams and lists of critical assets

Incident handling – Preparation
Making incident detection and analysis easy (1/2)

- Profile networks and systems
  - Study networks, systems, and applications to gain understanding of their normal behavior
- *Practice*: Profile networks and systems
  - Install OCS-Inventory agent, server and reports
  - Update your data on the server
  - Browse summaries on the server

Incident handling – Preparation
Making incident detection and analysis easy (2/2)

- Use centralized logging and create a log retention policy
- Keep all host clocks synchronized
- Maintain and use a knowledge base of information
- Use internet search engines for research
- Consider experience as being irreplaceable
- Create a diagnosis matrix for less experienced staff

Incident handling – Preparation Preventing incidents

- Periodic risk assessments of systems and applications
  - identify potential problems before they occur
  - implement a genuine plan that clearly states how risks will be mitigated, transferred, avoided or accepted
- Recommended practices for securing networks:
  - Patch management
  - Host security
  - Network security
  - Malicious code prevention
  - User awareness and training

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Incident handling
From detection to assignment

- Incident report :
  - Signs of an incident: events that trigger the process
  - Sources of precursors and indications: software alerts, log files, publicly available information, etc
- Incident registration : in the incident handling system
- Incident triage : verification, classification, prioritization, assignment
- Incident notification

AfricaCERT
United in promoting cyber security in Africa

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Incident handling
Containment, Eradication, and Recovery (1/3)

- Criteria for determining appropriate containment strategy
  - Potential damage to and theft of resources
  - Need for evidence preservation
  - Service availability
  - Time and resources needed to implement the strategy
  - Effectiveness of the strategy
  - Duration of the solution

Incident handling
Containment, Eradication, and Recovery (2/3)

- Evidence gathering and handling
  - To resolve the incident
  - For legal proceedings
- Detailed log should be kept for all evidence, including:
  - Identifying information (e.g., the location, serial number, model number, hostname, MAC address, IP address)
  - Name, title, contacts of each individual who collected or handled the evidence during the investigation
  - Time and date (including time zone) of each occurrence of evidence handling
  - Locations where the evidence was stored

Incident handling
Containment, Eradication, and Recovery (3/3)

- Eradication
  - Deletion of components of the incident(malicious code, diverting a flood of DDoS attack to a sinkhole)
  - Disabling or removing breached user accounts
- Recovery
  - Actions are typically operating system (OS) or application-specific
  - Restoration of systems to normal operation
  - Hardening systems to prevent similar incidents

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Incident handling
Post-incident activities (1/2)

- Lessons learned
  - Exactly what happened, and at what times
  - How well did staff and management perform? Were the documented procedures followed? Were they adequate?
  - What information was needed sooner?
  - Were any steps or actions taken that might have inhibited the recovery?
  - What would the staff and management do differently the next time a similar incident occurs?
  - What corrective actions can prevent similar incidents in the future?
  - What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Incident handling
Post-incident activities (2/2)

- Using Collected Incident Data
  - Number of incidents handled
  - Time per incident
  - Objective assessment of each incident
  - Subjective assessment of each incident
- Incident response audit to evaluate
  - Incident response policies, plans, and procedures
  - Team model and structure
  - Incident handler training and education
  - Tools and resources
  - Incident documentation and reports, measures of success
- Evidence retention

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Enhancing quality of services (1/4)

- Good relations to the decision makers
  - Proper funding, proper support
  - Better perspective to develop the team further
  - Using incidents as triggers for change, as opportunities to reflect on “business as usual”
- Constant awareness building referred to the added value derived from the services provided:
  - Statistics about incidents
  - Catastrophic scenario for the case if there were no CSIRT

Enhancing quality of services (2/4)

- Security-Related Information Dissemination
  - reporting guidelines and contact information for the CSIRT
  - archives of alerts, warnings, and other announcements
  - documentation about current best practices
  - general computer security guidance
  - policies, procedures, and checklists
  - patch development and distribution information
  - vendor links
  - current statistics and trends in incident reporting
  - other information that can improve overall security practices

Enhancing quality of services (3/4) Communication channels

Channels / media	Contents
Print material	Brochures, Flyers, Gadgets, Pencils, Stickers etc. should always include the essential incident reporting contacts
Public Website	Mission and goals as per constituency definition, Services, Contact details, Publicly available projects and papers
Closed member area on the Website	For Secured information only displayed to constituents
Mailing lists	Way to address various target groups through different mailing lists
SMS /text messaging	In case of emergencies such as major infrastructure outages, good alternative for informing constituents that there is something going: urgently check email and/or contact the CSIRT
Video conferencing /VOIP	Videoconferencing can add a more personal touch than voice alone
Chat	Fast and efficient way for searching for help online

Successful relationship is best initiated in person

Enhancing quality of services (4/4) Practice: Sending alerts to constituents

- You received this security news:
  - Title:Bitcoin-Mining Trojan Lurking On Skype
  - Date Published: 9th April 2013
  - URL:http://www.net-security.org/malware_news.php?id=2459

- *Practice*: Based on that report, draft an alert message

  to your constituents to
  - inform them about the case
  - provide them with advices on how they can enhance protection of their end users
  - etc.

Contents

- Introduction: module objectives
- Incident handling
  - Preparation
  - Detection, registration, triage, assignment
  - Containment, eradication, recovery
  - Post incident activities
- Enhancing quality of services
- Conclusion

Conclusion (1/2)

- Some recommendations
  - Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure
  - Profile networks and systems
  - Understand normal behaviors of networks, systems, and applications
  - Use centralized logging and create a log retention policy
  - Acquire tools and resources for incident handling
  - Establish strategies and procedures for containing incidents
  - Establish mechanisms for outside parties to report incidents
  - Prioritize incidents by business impact, based on criticality of affected resources and technical effect of incident
  - Hold lessons learned meetings after major incidents

Conclusion (2/2)

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology”- Bruce Schneier

http://think.securityfirst.web.id/?page_id=12

P. Jacques Houngbo
jacques.houngbo@africacert.org