CSIRT Services

Perpétus Jacques Houngbo
Dar Es Salaam, May – June 2011

“Misuse of technology is a social problem, not a technological one.” – Steve Jobs
http://think.securityfirst.web.id/?page_id=12

References

- http://www.cert.org/csirts/services.html

Contents

- Introduction
- Service Categories
- Service Descriptions
  - Reactive Services
  - Proactive Services
  - Security Quality Management Services
- Conclusion

Contents

- Introduction
- Service Categories
- Service Descriptions
  - Reactive Services
  - Proactive Services
  - Security Quality Management Services
- Conclusion

Introduction

- CSIRT services defined during creation process
- CSIRT services, but also covered by “security team”
- Great care while choosing services, impact on:
  - resources
  - skills sets
  - partnerships
- Quality / Quantity
- Think big, start small and ...scale fast

Contents

- Introduction
- Service Categories
- Service Descriptions
  - Reactive Services
  - Proactive Services
  - Security Quality Management Services
- Conclusion

Service categories

- Reactive services
  - services are triggered by an event or request
  - services aim at cure of compromised system
- Proactive services
  - prepare, protect, and secure
  - reduce the number of incidents
- Security quality management services
  - improve the overall security
  - reduce the number of incidents

Some CSIRT in Africa

- Kenya, CSIRT-KENYA, Kenyan National Computer Security Incident Response Team / www.csirt.or.ke
- Mauritius, CERT-MU, Mauritian National Computer Security Incident Response Centre http://www.cert-mu.org.mu/
- South Africa, ECS-CSIRT, South African Computer Security Incident Response Team http://www.e-comsec.com/ECSCSIRT/tabid/109/Default.aspx
- Tunisia, tunCERT, Tunisian Computer Emergency Response Team http://www.ansi.tn/en/about_cert-tcc.htm

Contents

- Introduction
- Service Categories
- Service Descriptions
  - Reactive Services
  - Proactive Services
  - Security Quality Management Services
- Conclusion

Reactive services

- Alerts and Warnings
- Incident Handling
- Vulnerability Handling
- Artifact Handling

Reactive services: alerts and warnings

- Dissemination of information
  - intruder attack
  - security vulnerability
  - intrusion alert
  - computer virus
  - hoax
- Guidance for protecting their systems or recovering any systems that were affected

Reactive services: alerts and warnings

- Practice:
  - How to disseminate information
    - Internet, intranets, web sites, brochures, seminars, training classes
  - How to provide guidance for protecting systems and recovering
    - Learning, practicing, mastering => expertise
    - Adopting best practices
    - Marketing your knowledge and expertise

Reactive services: incident handling

Activities include: protection of systems, rebuilding, repairing.

- Incident analysis:
  - forensic evidence collection
  - tracking or tracing
- Incident response on-site: team to travel, or already in place
- Incident response support: remote assistance
- Incident response coordination: include different parties (law, IT, etc.), no direct on-site response

Reactive services: vulnerability handling

Activities include: protection of systems, rebuilding, repairing.

- Vulnerability analysis: technical analysis and examination of vulnerabilities
- Vulnerability response: developing or researching patches, fixes, and workarounds
- Vulnerability response coordination: dissemination of information, assessment of implementation of solutions

Reactive services: vulnerability analysis

Tools:

- eEye Retina Network Security Scanner
- GFI LANguard Network Security Scanner
- ISS Internet Scanner
- SAINT Vulnerability Scanner
- Shadow Security Scanner
- Open Source Nessus
- Microsoft Baseline Security Analyzer (MBSA)
- Cerberus Internet Scanner
- etc.

Reactive services: vulnerability analysis

Practice:

- Retina Community, eEye Retina Network Security Scanner

Reactive services: artifact handling

Artifact : any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures.

- Artifact analysis: identification, classification
- Artifact response: use of signatures
- Artifact response coordination: dissemination of information
- Tool: Microsoft Attack Surface Analyzer

Contents

- Introduction
- Service Categories
- Service Descriptions
  - Reactive Services
  - Proactive Services
  - Security Quality Management Services
- Conclusion

Proactive services

- Announcements
- Technology Watch
- Security Audits or Assessments: infrastructure review, best practice review, scanning, penetration testing
- Configuration and Maintenance of Security Tools, Applications, and Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Contents

- Introduction
- Service Categories
- Service Descriptions
  - Reactive Services
  - Proactive Services
  - Security Quality Management Services
- Conclusion

Security Quality Management Services

Improvement of the overall security

- Risk Analysis
- Business Continuity and Disaster Recovery Planning
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation or Certification

Security Quality Management Services

Improvement of the overall security: Risk Analysis

- Failure Mode and Effects Analysis (FMEA) in practice

Conclusion

- Information security goes beyond beyond the CIA triad (Confidentiality, Integrity, Availability). Extension to accountability, authenticity and non-repudiation.
- Many cross links of services
- Services offered must be tailored to the specific needs and prospective evolution of the constituency
- Services offered must be tailored to resources available: financial, organizational, human
- Dissemination of information is very important
- Prevention is better than cure
- Quality / Quantity
- Think big, start small and ...scale fast

“Misuse of technology is a social problem, not a technological one.” – Steve Jobs

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

Perpétus Jacques Houngbo
jacques.houngbo@auriane-etudes.com