Policy, Strategy and Operations

IWOSI: The Information Warfare, Cyber Warfare and Open Sources Intelligence – Yasar University Izmir, Turkey 2012

Part II-2: 2012.04.18, 13:30-17:00

Dr. Nikolaj Goranin, CISM, CISA
Vilnius Gediminas Technical University

What is incident?

- Any type of event, that can harm organization.
- By definition, incidents are unexpected and often confusing.
- Decision, how to solve the incident should not be done in time of crisis.

Uninterruptable Functioning – Definitions

- Incident management and response – emergency operations, that take place as a result of an incident.
- IRM is a part of Business Continuity Planning (BCP), but focuses on security related breaches.
- Disaster Recovery Plan (DRP) focuses on natural disasters and catastrophies.

IRP

- Preparing a BIA of the effect of the loss of critical business processes
- Identifying and prioritizing the systems and other resources required to support critical business processes in the event of a disruption
- Assessing incident detection and monitoring capabilities
- Defining and obtaining agreement on severity criteria and declaration criteria
- Establishing clear roles and responsibiilties

BCP

- Choosing appropriate strategies for recovering at least sufficient facilities to support the critical business processes until full operations can be restored
- Developing a detailed plan for the critical business functions to continue to operate at an acceptable level

DRP

- Developing the detailed plan for recovering IT facilities
- Training stuff how to follow plans
- Testing the plans
- Maintaining the plans as the business changes and systems develop
- Storing the plans so that they can be accessed despite computer and network failures
- Auditing the plans

Goals of IRM

- Detect incidents quickly
- Diagnose incidents accurately
- Manage them properly
- Contain and minimize damage
- Restore affected services
- Determine root causes
- Implement improvements to prevent recurrence

Incident Response, Recovery and Continuity

- Incident response:
  - Evacuation, safety, media handling.
- Recovery:
  - Deployment of teams, activation of recovery plans, incident communication, restore of interim business activity.
- Continuity:
  - Increased stability, asset recovery, rebuilding business, return to “normal” operation.

Incident Response Planning

- Incident detection capabilities
- Clearly defined severity criteria
- Assessment and triage capabilities
- Declaration criteria
- Scope of incident management
- Response capabilities

Incident Management Outcomes

- Assets are adequately protected
- IRP is in place
- Incidents are identified and contained, recovery fits in AIW
- Good control of communication flows
- Lessons learned are documented
- Assurance is provided to stakeholders

Requirements to Effective IRM

- Consolidate and correlate inputs from multiple systems
- Identify incidents or potential incidents
- Prioritize incidents based on business impact
- Track incidents until they are closed
- Provide status tracking and notifications
- Integrate with major IT management systems
- Implement good practices guidelines

Incident Management Metrics

- Total number of reported incidents
- Total number of detected incidents
- Average time to respond to an incident relative to AIW
- Average time to resolve an incident
- Total number of incidents resolved
- Proactive and preventive measures taken
- Number of employees covered by training
- Total savings from potential damage of the solved incident

CERT

- Computer Emergency Response Team is a name given to expert groups that handle computer security incidents.
- Most groups append the abbreviation CERT or CSIRT to their designation where the latter stands for Computer Security Incident Response Team.
- For some teams the spelling of CERT refers to Computer Emergency Readiness Team while handling the same tasks.

Recovery Sites

- Hot sites
- Warm sites
- Cold sites
- Mobile sites

- Reciprocal agreements

Continuity of Network Services

- Redundancy
- Alternative routing
- Diverse routing
- Long-haul network diversity
- Last-mile circuit protection
- Voice recovery

IRP Testing

- Requirements:
  - Periodic testing
  - Testing of critical infrastructure and applications

- Test types:
  - Checklist review
  - Structured walkthrough
  - Simulation test
  - Parallel test
  - Full interruption test

Legal Aspects of Forensic Evidence

- Chain of custody
- Activity log
- Signed duplicates of original evidence media
- No “strike-back”

Discussion