Computer Security Incident Handling

Emil Simion

Agenda

- Organizing a Computer Security Incident Response Capability
- Handling an Incident
- Coordination and Information Sharing
- Scenarious

Organizing a Computer Security Incident Response Capability

- Events and Incidents
- Need for Incident Response
- Incident Response Policy, Plan, and Procedure Creation:
  - Policy Elements
  - Plan Elements
  - Procedure Elements
  - Sharing Information With Outside Parties
- Incident Response Team Structure:
  - Team Models
  - Team Model Selection
  - Incident Response Personnel
  - Dependencies within Organizations
- Incident Response Team Services
- Recommendations

Handling an Incident

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity
- Incident Handling Checklist
- Recommendations

Coordination and Information Sharing

- Coordination
- Information Sharing Techniques
- Granular Information Sharing
- Recommendations

Questions scenarios

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity
- General Questions

Scenarious

- Domain Name System (DNS) Server Denial of Service (DoS)
- Worm and Distributed Denial of Service (DDoS) Agent Infestation
- Stolen Documents
- Compromised Database Server
- Unknown Exfiltration
- Unauthorized Access to Payroll Records
- Disappearing Host
- Telecommuting Compromise
- Anonymous Threat
- Peer-to-Peer File Sharing
- Unknown Wireless Access Point

References

- NIST 800-61R1, *Computer Security Incident Response*.