Federal Incident Reporting Requirements & Handling Guidelines

Tom Millar
Chief of Communications

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

NIST Special Publication 800-61

- NIST's Computer Security Incident Handling Guide
  - Revision 2 just became final on August 8th, 2012
  - Significant changes to the content and structure from previous versions
  - No longer contains the US-CERT Federal Incident Reporting Appendix (the "six categories")

Rev 2 Change Log (Appendix H)

- Deletions:
  - Removed duplicative material on forensics; pointed to SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
  - ***Deleted material specific to the old incident categories***
  - Deleted the duplicate list of recommendations
  - Deleted print resources list
  - ***Deleted federal agency incident reporting categories***

Rev 2 Change Log (Appendix H)

- Changes:
  - Revamped the list of attack vectors:
    - External/Removable Media
    - Attrition
    - Web
    - Email
    - Impersonation
    - Improper Usage
    - Loss or Theft of Equipment

Rev 2 Change Log (Appendix H)

- Changes, Continued:
  - Revamped the factors for incident handling prioritization:
    - Functional Impact
    - Information Impact
    - Recoverability

Attack Vectors

- External/Removable Media, Web, Email
- Loss or Theft of Equipment
- Attrition: DDoS or any brute force attack
- Impersonation: spoofing, MITM, rogue WAP, injects
- Improper Usage
- Other

Prioritization: Functional Impact

- ***None***: no effect on the organization's ability to provide all services to all users
- ***Low***: organization can still provide all critical services, but has lost efficiency
- ***Medium***: organization has lost the ability to provide a critical service to some users
- ***High***: organization has lost the ability to provide some critical service to any users

Prioritization: Information Impact

- ***None***: No information compromised
- ***Privacy***: Sensitive PII accessed or exfiltrated
- ***Proprietary***: Unclassified proprietary information accessed or exfiltrated
- ***Integrity Loss***: Sensitive information changed or deleted

Prioritization: Recoverability

- ***Regular***: TTR is predictable, with existing resources
- ***Supplemented***: TTR is predictable, with additional resources
- ***Extended***: TTR is unpredictable; additional resources and outside help are needed
- ***Not Recoverable***: Recovery is not possible

Coordination & Info Sharing

- Section 4 of revision 2 is devoted to this topic, based on community feedback from the public comment period
- Sharing relationships:
  - Team-to-Team: Indicators and lessons learned
  - Team-to-Coordinating Team: + impact and risk assessments
  - Coordinating Team-to-Coordinating Team: + steady state check-ins and collaborative response plans

US-CERT Reporting Guidance

- US-CERT's Federal Reporting Guidelines remain the same for now
- New guidelines are being drafted to reflect the attack vectors and prioritization changes in the revised SP
- Goals:
  - Improve the timeliness of actionable reporting and encourage sharing of technical indicator information
  - Improve the overall awareness and understanding of real impacts to our systems

US-CERT Reporting Guidance

- Your participation is critical to ensure that new guidelines are useful and effective
- This is an opportunity to improve the way the entire US Federal Government does business
- And potentially other sectors as well!
- thomas.millar@us-cert.gov

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Homeland Security