National Insider Threat Special Interest Group (NITSIG)

Combating The Insider Threat To Information Systems

A Proactive And Defensive Security Posture

March 3, 2018

Information / Information Systems / Network Threats

Vulnerability
Lack of Data Management Plan / Security Classification Marking And Guidance
Threat
Data Is Not Marked Accordingly, Or The Correct Security Classifications Are Not Applied To Hardware And Documents.
Mitigation
Define How Data Is Handled / Cataloged From The Point Of Ingestion. Apply Security Classification Markings. Define Retention Requirements.

Vulnerability
Lack Of Password Management For Critical Network Servers, Network Devices, Routers, Firewalls, Etc.
Threat
Rouge Network Administrator Takes Network Hostage. Ensure More Then One Network Administrator Holds The Keys To The Castle.
Mitigation
Ensure Passwords Stored In Safe

Vulnerability
Individuals Using Network Resources Are In Violation Of Network/Computer Systems Rules Of Behavior. Possible Leak Of Sensitive or Classified Information, Virus Infections, Etc.
Threat
Improper Usage Of Network Resources (Computer Systems, Software Applications, Networks, Bandwidth, And Supporting Network Devices, Etc.)By Individuals.
Mitigation
Monitoring Of Floppy, USB/DVD-CD/PDA Access/Connections, Instant Messaging, Social Networking, Print Jobs, Web Surfing Habits, E-Mail Content Filtering, E-Mail Attachments, Use Of Encryption, Zip Files, Stenography Applications. Review Of Software And Database Application Logs, Operating Systems Event Logs, Network Router Logs.

Vulnerability
Network Jacks That Are “Hot” Or “Live”
Threat
Individuals Can Use Live Network Jacks To Possibly Access Network, Capture Data, Sniff Traffic.
Mitigation
Disable Network Jacks Not In Use.

Vulnerability
Use Of Group Accounts For Network Login.
Threat
Unable To Associate Actions With Individuals.
Mitigation
No Shared Group Accounts. All Network Accounts Must Be Associated With Individuals.

Vulnerability
Large Print Jobs That May Be Out Of Scope Of Individuals Duties
Threat
Without Auditing , Unable To Detect Large Print Jobs That May Be Outside Scope Of Duties.
Mitigation
Audit Print Jobs. User Of Banner Pages On Print Jobs.

Vulnerability
Document Scanner Hooked Up To Un-Classified Network In Classified Areas, With No Restrictions On Access To Scanner. (Includes: Portable Pen Scanners)
Threat
Possible Leak Of Sensitive or Classified Information To The Internet.
Mitigation
Limited Access To Document Scanner. (Example: Network Administrators Only)

Vulnerability
No Mapping Of Network Infrastructure (Computer, Servers, Routers, Firewalls, Other Network Devices.
Threat
Unable To Quickly Determine Threats To Network Infrastructure.
Mitigation
Map Network Infrastructure With Software Tool.

Vulnerability
No Mapping Of Network Traffic Traversing Network Infrastructure.
Threat
Unable To Determine Un-Authorized Or Suspicious Activity On Network.
Mitigation
Network Sniffer Trace, Intrusion Detection System.

Vulnerability
Lack Of Control For Software Applications, Workstations, Servers, Laptops And Networking Infrastructure Assets.
Threat
Loss Of Hardware And Software.
Mitigation
Proper Asset Management Procedures

Vulnerability
Non-Secure Configurations Of Software Applications. Database, Workstations, Servers, Laptops, Network Routers.
Threat
Possible Breach Of Computers And Networks. Un-Authorized Access To Data.
Mitigation
Use Secure Configurations From NIST, DISA, Commercial Vendors, Operating System And Software Application Patch Management, Consensus Audit Guidelines. Use Of Encryption On Desktops, Laptops. Implement Strict Password Policies.

Vulnerability
Lack Of Configuration Management Of Computer System And Networks
Threat
Un-Authorized Installation Of Hardware And Software
Mitigation
Configuration Control Board, Configuration Change Requests/CCR’s

Vulnerability
Failure To “Clean” Documents Before Releasing To Lower Level Classified Systems Or The Internet
Threat
Release Of Classified Or Sensitive Data
Mitigation
MetaData Cleaning/Document Flattening Software To Remove Hidden MetaData From Adobe PDF, MS-Word, Excel, PowerPoint Files.

Vulnerability
Key Catcher
Threat
Plug & Play Hardware Keylogger Installs In Seconds
• Record on one PC & retrieve data on another.
• No software to install.
• Works with all PC operating systems.
Mitigation
Check Switch Boxes And USB/PS/2 Ports For Key Catcher Devices

Vulnerability
Recording of Classified or Sensitive Conversations To Wav File.
Change Extension To .Doc File. Send From Work To Other Source On Internet.
Threat
Release Of Classified Or Sensitive Information
Mitigation
Removal Of Windows Sounder Recorder Application, Disable Microphone Port.

Vulnerability
Authorization Creep. Accumulation Of Privileges.
Threat
Un-Authorized Access To Data. Need To Know Principle.
Mitigation
Review Of Access Rights For; Physical Security, Computer/Network Access, Software Applications, Database Access. Separation Of Duties, Least Privilege.

Vulnerability
Un-Authorized Access To Facility, Computer/Network Access, Software Applications, Database Access.
Threat
Un-Authorized Access To Facility. Un-Authorized Access To Data.
Mitigation
Proper Termination Procedures. Removal Of Facility Access, Computer And Network Access. Disable Network Account After 60/90 days of inactivity.

Vulnerability
Lack Of Backup And Recovery Procedures. Lack Of Structured Incident Response Team.
Threat
Inability To Quickly Recover From Incidents.
Mitigation
Proper Incident Response And Handling Procedures/CSIRT, Including Computer Forensics Investigations. Backup And Recovery Procedures.

Contact Information

Founder / Chairman Of The National Insider Threat Special Interest Group
CEO Insider Threat Defense, Inc.
Insider Threat Program Development / Management Training Course Instructor
Insider Threat Vulnerability Assessor & Mitigation Specialist
888-363-7241 / 561-809-6800
jimhenderson@nationalinsiderthreatsig.org
www.nationalinsiderthreatsig.org
www.insiderthreatdefense.us
james.henderson@insiderthreatdefense.us