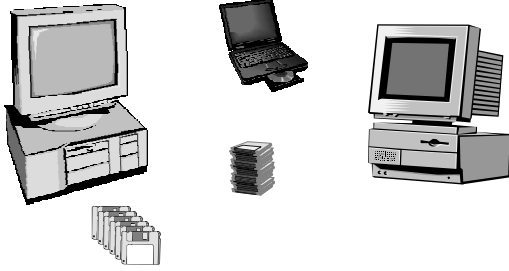


Current Information Security Issues



Current Information Security Issues

- Remote Access - Two Factor Authentication
- OMB-M-06-16 - Data Encryption
- OMB-M-06-15 – Protecting PII
- Application Security
 - Who's responsibility
- Asset and Inventory Management
 - Data and Hardware (laptops etc.)
- Disaster Recovery
 - Are you ready?
- SCADA Security



Current Information Security Issues

• REMOTE ACCESS - 2 Factor Authentication

- VPN Software such as Secure Remote or RSA SecurID installed on workstation.

- Provides an encrypted channel for secure data transfer through www.



- Web based VPN software will allow connection from any machine on the internet – no software needed.

- US DOT is currently using method with good results.

Current Information Security Issues

•OMB-M-06-16 – Protecting Sensitive Agency Data

- Data Encryption
 - Entire contents of desktop drive
 - ALL removable media
 - Thumb Drives
 - CD-R/CD-RW \DVD-R
- Track movement of sensitive data to removable devices.
 - Appliances and software can now track data movement to removable media devices at user level
- Two factor authentication for remote access.

Current Information Security Issues

OMB-M-06-15 – Protecting Personal Identity Information (PII)

- 128 bit Encryption of data on Laptops.
- 128 bit Encryption of Databases on Servers.
- 128 bit Encryption of removable media containing PII.
- Two-factor authentication for remote access.
- OMB-M-06-19 Requires agencies to report all incidents involving PII to the US Computer Emergency Readiness Team (US-CERT) within 1 hour of discovering incident.

Current Information Security Issues

• APPLICATION SECURITY

- 75 % of all attacks are done at the application level.
- Ascertain asset inventory and vulnerability status.
 - Data and application security reviews.
 - Block know attacks and attackers through network appliances and desktop agents.
 - i.e. Firewalls, IDS, and anti-virus software .

Current Information Security Issues

- Asset and Inventory Management
 - Hardware
 - Laptops, Thumb drives, removable media
 - PII and Sensitive Data
 - How can you protect something if you do not know exists?

 - Most agencies do not know where PII or sensitive data has been downloaded or distributed to.

Current Information Security Issues

- DISASTER RECOVERY
 - Secure remote access through VPN
 - Web based VPN solution now available.
 - Ensure employees are trained and proficient at using VPN hardware and software.
 - Gartner Urges IT Managers to act quickly on Pandemic Planning – *Computer World 11/29/06*
 - Pandemic Planning – Bird Flu
 - Telecommuting capabilities.

Current Information Security Issues

- SCADA SYSTEM SECURITY
 - *Supervisory Control And Data Acquisition*

SCADA systems are used to monitor or to control chemical, physical or transport processes, in municipal water supply systems, to control electric power distribution and generation, gas and oil pipelines, and other distributed processes.

 - Currently there are no reporting requirements when these systems are compromised.

Current Information Security Issues

- **SCADA SYSTEM SECURITY**

- Simple logic gate devices that move a control valve open or close.
- Most are designed to last 30+ Years.
- Still accessed through modems.
- During Y2K – programmers addressed date issues but not security when programs were updated.

- **STRENGTHEN SCADA SYSTEM SECURITY?**

- *Regular Vulnerability Assessments*

Current Information Security Issues

QUESTIONS?

Craig M. Goscha, Director
National Computer Forensic Division
USDA OIG
cmgoscha@oig.usda.gov
816-926-7644
