Information Assurance

Barry C. West
U.S. General Services Administration
Office of Electronic Government
18th & F St NW, Washington DC 20405
Phone: +1-202-208-3584
e-mail:barry.west@gsa.gov

Presented at the THIC Meeting at the Naval Surface Warfare Center Carderock, 9500 MacArthur Blvd

West Bethesda MD 20817-5700

October 4, 2000

The Premier Advanced Recording Technology Forum

THIC Inc.

Computer Security Policy

- “In many ways policy is like computer code - it is something that should be written down, then read, interpreted and executed.”

What is policy ??

- Policy is a set of rules or procedures based on risks and vulnerabilities and is to be used by everyone to protect our resources

Policy

- Every organization has a security policy, it just may not be written
- Good policy is clear, specific, concise and realistic
- Policy is protection for systems administrators and security professionals
- If your organization won’t create a policy, write your own!

According to the SANS Institute, the ten worst security mistakes IT people make are:

- 1) Connecting systems to the Internet before hardening them (removing unnecessary services and patching necessary ones).
- 2) Connecting test systems to the Internet with default accounts/passwords
- 3) Failing to update systems when security vulnerabilities are found and patches or upgrades are available

- 4) Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI
- 5) Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated
- 6) Failing to maintain and test backups
- 7) Running unnecessary services, especially ftpd, telnetd, finger, rpc, mail and rservices

- 8) Implementing firewalls with rules that allow malicious or dangerous traffic
- 9) Failing to implement or update virus detection software
- 10) Failing to educate users on what to look for and what to do when they see a potential security problem

The Seven Worst Security Mistakes Senior Exec. Make...

- 1) Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job
- 2) Failing to understand the relationship of information security to the business problem - they typically understand physical security but not IT security

- 3) Failing to deal with the operational aspects of security - not following through on fixes
- 4) Relying primarily on a firewall
- 5) Failing to realize how much money their information and organizational reputations are worth
- 6) Authorizing reactive, short-term fixes so problems re-emerge rapidly
- 7) Pretending the problem will go away if they ignore it

Where can users go for help?

- - General Services Administration (GSA)
  http://ec.fed.gov
- - National Institute of Standards and Technology (NIST) Computer Security Special Publications - located at
  http://csrc.nist.gov/nistpubs
- - Government Accounting Office (GAO) reports
- - Office of Management and Budget (OMB) Circular A-130 “Security of Federal Automated Information Resources”

Where can user's go for help?

- Index to IETF RFCs, including 2196
  www.ietf.org/rfc.html
- Site Security Handbook Addendum for ISPs
  www.ietf.org/internet-drafts/draft-ietf-grip-ssh-add-00.txt
- SANS Model Security Policies
  www.sans.org/newlook/resources/policies/policies.htm
- University of Toronto Policies
  www.utoronto.ca/security/policies.html

CIO Council -Security, Privacy, and Critical Infrastructure Committee

- It’s mission is to ensure implementation of security policies within the Federal Government that gain public confidence and protect services, privacy, and sensitive or national security information.

Federal Best Security Practices (BSPs)

- The Security Practices Subcommittee (SPS) of the CIO Council has designed this web site as an educational resource for Federal security professionals -

  http://bsp.cio.gov

Information Security
“Best Practice”

- Every organization must have one or more individuals clearly assigned with the responsibility to track and follow-up on relevant security alerts and other vulnerability information from multiple sources.

Sources of Vulnerability Information

- National Infrastructure Protection Center - www.nipc.gov
- Federal Computer Incident Response Capability - 1-888-282-0870 www.fedcirc.gov
- Computer Emergency Response Team - www.cert.org
- Computer Incident Advisory Capability - www.ciac.org

Privacy

- Privacy of personal data is a chief concern for Government and industry as they gradually move many public transactions online.

Privacy Act's Risk Implications and Rules

- Collect only what is needed
- Limit use and disclosure
- Allow for review and correction

Risk Management Analysis

- How much will it cost to minimize the risk posed by the vulnerability?
- Are the security enhancement costs commensurate with the asset's overall importance?
- How long will it take to implement fully the proposed security enhancement?

Key Issues for the Future

- $$ - Fiscal 2001 and beyond must be realistic dollar figures to support our infrastructures across government and industry
- Security Awareness / Security Plans
- Training of Personnel
- Taking action NOW, rather than waiting for a national crisis to occur

FirstGov.gov

- First government-wide portal of government information. Provides a one stop location to all government web sites. The site will evolve to other features and functionality over the next 12 months.

- www.firstgov.gov

Contact Information

- Barry C. West
  U.S. General Services Administration
  202-208-3584
  barry.west@gsa.gov