

Desktop Computer Security

William P. Flinn

Colorado Technical University
Information Systems Security

CS-659

Fall 2005

Hypothesis:

- Desktop computers offer many and varied access points into an organization's network.
- There are many ways in which a desktop computer can be compromised and used against the organization.

Presentation Overview

- Why Secure Desktops/Workstations?
- Risks and Benefits of Desktop Security
- Types of Threats and How to Secure:
 - Operating Systems and Software Threats
 - Physical Security Threats
 - End-Users
- Other Security Strategies
- Summary and Conclusions

Why Secure Desktops/Workstations?

- They contain information
 - Some is sensitive and/or proprietary
- They are connected to the network!
- Attacks can come in from the Internet or other infected computers on the network
- Attacks can be brought in from the outside
 - Via sneaker-net (flash drives, CDs, etc.)
 - Can attack other computers on the network
- Computers can be lost or stolen
 - Particularly laptops!

Risks and Benefits of Desktop Security

- Do risk analysis!
 - Assess what needs to be secured and how much the cost
- Apply the right amount of mitigation to the right amount of risk
 - Don't protect a \$10 horse with a \$50 fence
 - Weigh the business needs with the need to secure
 - Example: "The USB Device Vulnerability"

Type of Threat – Operating System and Software

- Operating systems and software contain vulnerabilities
- Viruses, WORMS, Trojans
- Spyware & Malware
- Unneeded services and startup apps

How to Secure – Operating System and Software

- Patches and updates
 - Don't forget the rollback strategy
- Antivirus Software
 - Standalone –v- managed clients
- Anti-Spyware
- Personal Firewalls
- Disable unneeded services and startup apps

Type of Threat – Physical Security

- Theft and Loss
 - Loss of proprietary/sensitive information
- Physical access
 - Attacker logging into computer as an authorized user
 - Accessing a computer that is already logged onto network
- Retiring Computers
 - Leaving data on hard drives

How to Secure – Physical Threats

- BIOS Passwords
- Locks
- Personnel access to office areas
 - Cards, ID Badges
- Policy
 - Make users lock their screen or log out when they leave
- Wipe hard drives when retiring or donating old machines

Type of Threat – End-Users

- Security unaware
 - They want to do business and not be slowed down by a security policy
- Poor security habits
 - Leaving screens unlocked when they leave the workstation
- Poor password habits
 - Using weak passwords or leaving passwords out in the open

How to Secure – End-Users

- Education and awareness
- Security policy
 - Acceptable use policy is cornerstone!
- Enforce password policies through AD, NDS, eDirectory
- Security templates on workstations that enforce screensavers, etc.

Other Security Strategies

- Strategic planning
- Be familiar with computer security compliance directives
 - NIST/FIPS
 - SOX
 - HIPAA
- Vulnerability scanning
- Centralized patch management systems
- Antivirus management servers

Conclusions

- Workstation security affects network security
- Don't rely on "bagel security" (hardened perimeter) as the only network defense
- Perform risk analysis
- Apply appropriate measures to the threats

Conclusion

- Questions and Answers