Remote Access

Security and Security Issues

Matthew Scholl

Supervisory Information Security Specialist

Computer Security Division

National Institute of Standards and Technology (NIST)

May 1, 2007

Remote Access Defined

- Access by users (or information systems) communicating external to an information system security perimeter.

Remote Access Security

- Assure the confidentiality of information, the integrity of data and the availability of resources to a geographically distributed workforce

Remote Access Security

- There are many ways to conduct remote access securely, but each is dependent upon
  - Mission and needs of the organization
  - Available resources
  - Security and Privacy risk tolerances

Remote Access Security

- Communication Capabilities
- Network Capabilities
- Endpoint Capabilities

Remote Access Security

Communication Capabilities

- Cable Modem/DSL/Satellite/Dial Up/Power Line/Home Wireless
- Wireless Phones/Cell Phones
- Blackberries/PDAs/Smart Phones
- Email

Remote Access Security

Network Capabilities

- Virtual Private Networks (VPN)
  - Gateway-Gateway/Host-Gateway/Host-Host
    - IPSec VPNs
    - Data Link VPN
    - Transport Layer VPN
    - Application Layer VPN
- Encryption

Remote Access Security

Endpoint Capabilities

- Use of strong passwords and multifactor authentication
- Anti Virus / Anti Spyware / Anti Spam
- Personal Firewall
- Secure Web Browsers
- Secure Endpoint Configuration
- Patching, Updating, and Monitoring
- Node Validation

Remote Access Security Issues

- Keeping up with rapid changes and increased availability of technology
- Training
  - Can users correctly use the security technologies?
- Awareness
  - Where and under what circumstances are resources being accessed?
- Solution Support
  - Can the organization deploy and maintain the solution and support the users?
- Endpoints are the weakest link

Trends in Secure Remote Access

- Expanding support of secure remote access for teleworkers, travelers, and home computer users
- Expanding usage of and support for mobile devices (smart phones, etc..) and wireless LANs
- Increasing usage of two-factor authentication
- Increasing focus on securing the “endpoints”
- Growing adoption of secure remote access to support disaster recovery

Remote Access

References

- NIST SP 800-46 – Security for Telecommuting and Broadband Connections
- NIST SP 800-77 – Guide to IPsec VPNs
- OPM Interagency Telework Site, Telework.Gov
- General Services Administration Telework Library