June 2009

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY FOR ENTERPRISE TELEWORK AND REMOTE ACCESS SOLUTIONS

Karen Scarfone, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Many people telework (also known as telecommuting), which is the ability for an organization's employees and contractors to perform work from locations other than the organization's facilities. Teleworkers use various client devices, such as desktop and laptop computers, cell phones, and personal digital assistants (PDAs), to read and send email, access Web sites, review and edit documents, and perform many other tasks. Most teleworkers use remote access, which is the ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently updated its guidelines on telework and remote access to help organizations protect their IT systems and information from the security risks that accompany the use of telework and remote access technologies. The revised guidelines discuss the technology, the current security risks involved in its use, and the recommended security solutions.

NIST Special Publication (SP) 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security: Recommendations of the National Institute of Standards and Technology*

NIST SP 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security*, written by Karen Scarfone and Murugiah Souppaya of NIST, and Paul Hoffman of the VPN Consortium, was issued in June 2009. It is a complete rewrite of the original NIST SP 800-46, *Security for Telecommuting and Broadband Communications*, which was released in August 2002.

The new guidelines discuss the technical and physical vulnerabilities and threats against enterprise telework and remote access solutions. One section of the publication presents recommendations for securing remote access solutions, while another section focuses specifically on protecting telework client devices and their data. The last section of the guide discusses security throughout the telework and remote access life cycle.

NIST SP 800-46 Revision 1 contains an extensive list of references to online sources of information about telework and remote access security. The appendices include a glossary of the technical terms employed in the publication and an acronym list. NIST SP 800-46 Revision 1 is available from the NIST Web site: http://csrc.nist.gov/publications/PubsSPs.html.

Remote Access Methods

Organizations have many options for providing remote access to their computing resources. In NIST SP 800-46 Revision 1, the remote access methods most commonly used for teleworkers are divided into four categories based on their high-level architectures: tunneling, portals, remote desktop access, and direct application access.

Tunneling involves establishing a secure communications tunnel between a telework client device and a remote access server, often a virtual private network (VPN) gateway. The tunnel uses cryptography to protect the confidentiality

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since April 2008:

and integrity of the communications. Application software on the client device, such as email clients and Web browsers, can communicate securely through the tunnel with servers within the organization. Tunnels can also authenticate users and restrict access, such as limiting which systems a telework client device can connect to.

A **portal** is a server that offers access to one or more applications through a single centralized interface. A teleworker uses a portal client on a telework client device to access the portal. Most portals are Web-based—for them, the portal client is a regular Web browser. The application client software is installed on the portal server, and it communicates with application server software on servers within the organization. The portal protects communications between the client devices and the portal, and portals can also authenticate users and restrict access to the organization's internal resources.

A **remote desktop access** solution gives a teleworker the ability to remotely control a particular desktop computer at the organization, most often the user's own computer at the organization's office, from a telework client device. The teleworker has keyboard and mouse control over the remote computer and sees that computer's screen on the local telework client device's screen. Remote desktop access allows the user to access all of the applications, data, and other resources that are normally available from their computer in the office.

With **direct application access**, remote access is accomplished without using remote access software. A teleworker can access an individual application directly, with the application providing its own security (communications encryption, user authentication, etc.) One of the most common examples of direct application access is Web-based access to email, also known as Webmail. The teleworker runs a Web browser and connects to a Web server that provides email access. The Web server runs HTTP over SSL (HTTPS) to protect the communications, and the Webmail application on the server authenticates the teleworker before granting access to the teleworker's email.

Security Concerns

Telework and remote access technologies often need additional protection because their nature generally places them at higher exposure to external threats than technologies only accessed from inside the organization. Major security concerns for telework and remote access technologies include the following:

Lack of physical security controls is an issue because telework client devices are used in a variety of locations outside the organization's control, such as employees' homes, coffee shops, hotels, and conferences. The mobile nature of these devices makes them likely to be lost or stolen, which places the data on the devices at increased risk of compromise. Malicious parties may attempt to recover sensitive data from the devices. Even if a client device is always in the possession of its owner, there are other physical security risks, such as an attacker looking over a teleworker's shoulder at a coffee shop and viewing sensitive data on the client device's screen.

Unsecured networks are frequently used for remote access. Because nearly all remote access occurs over the Internet, organizations normally have no control over the security of the external networks used by telework clients. Communications systems used for remote access include telephone and Digital Subscriber Line (DSL) modems, broadband networks such as cable, and wireless mechanisms such as IEEE 802.11, WiMAX, and cellular networks. Attackers may eavesdrop on sensitive information, as well as intercepting and modifying communications.

Client devices infected with malware pose risks not only to the devices' data, but to other systems within the organization. Telework client devices, particularly laptops, are often used on external networks and then brought into the organization and attached directly to the organization's internal networks. If a client device is infected with malware, this malware may spread throughout the organization once the client device is connected to the internal network.

Providing remote access to internal resources such as servers may place them at additional risk. If these internal resources were not previously accessible from external networks, making them available via remote access will expose them to new threats, particularly from untrusted client devices and networks, and significantly increase the likelihood that they will be compromised. Each form of remote access that can be used to access an internal resource increases the risk of that resource being compromised.

NIST's Recommendations for Improving the Security of Telework and Remote Access Solutions

All the components of telework and remote access solutions, including client devices, remote access servers, and internal resources accessed through remote access, should be secured against expected threats, as identified through threat models.

NIST recommends that organizations apply the following safeguards to improve the security of their telework and remote access technologies:

Plan telework security policies and controls based on the assumption that external environments contain hostile threats.

An organization should assume that external facilities, networks, and devices contain hostile threats that will attempt to gain access to the organization's data and resources. Organizations should assume that telework client devices, which are used in a variety of external locations and are particularly prone to loss or theft, will be acquired by malicious parties who will attempt to recover sensitive data from

them. Options for mitigating this type of threat include encrypting the device's storage and not storing sensitive data on client devices.

Organizations should also assume that communications on external networks, which are outside the organization's control, are susceptible to eavesdropping, interception, and modification. This type of threat can be mitigated, but not eliminated, by using encryption technologies to protect the confidentiality and integrity of communications, as well as authenticating each of the endpoints to each other to verify their identities.

Another important assumption is that telework client devices will become infected with malware; possible controls for this include using antimalware technologies, using network access control solutions that verify the client's security posture before granting access, and using a separate network at the organization's facilities for telework client devices brought in for internal use.

Develop a telework security policy that defines telework and remote access requirements.

A telework security policy should define which forms of remote access the organization permits, which types of telework devices are permitted to use each form of remote access, and the type of access each type of teleworker is granted. It should also cover how the organization's remote access servers are administered and how policies in those servers are updated.

As part of creating a telework security policy, an organization should make its own risk-based decisions about what levels of remote access should be permitted from which types of telework client devices. For example, an organization may choose to have tiered levels of remote access, such as allowing organization-owned personal computers (PCs) to access many resources, teleworker-owned PCs to access a limited set of resources, and other PCs and types of devices (e.g., cell phones, personal digital assistants [PDAs]) to access only one or two lower-risk resources, such as Web-based email. Having tiered levels of remote access allows an organization to limit the risk it incurs by permitting the most-controlled devices to have the most access and the least-controlled devices to have minimal access.

There are many factors that organizations should consider when setting policy regarding levels of remote access to grant; examples include the sensitivity of the telework, the level of confidence in the telework client device's security posture, the cost associated with telework devices, the locations from which telework is performed, and compliance with mandates and other policies. For telework situations that an organization determines are particularly high-risk, an organization may choose to specify additional security requirements. For example, high-risk telework might be permitted only from organization-issued and secured telework client devices that employ multifactor authentication and storage encryption. Organizations may also choose to reduce risk by prohibiting telework and remote access involving particular types of information, such as highly sensitive personally identifiable information (PII).

Ensure that remote access servers are secured effectively and are configured to enforce telework security policies.

Remote access servers provide a way for external hosts to gain access to internal resources, so their security is particularly important. In addition to permitting unauthorized access to resources, a compromised server could be used to eavesdrop on remote access communications and manipulate them, as well as to provide a "jumping off" point for attacking other hosts within the organization. It is particularly important for organizations to ensure that remote access servers are kept fully patched, and that they can only be managed from trusted hosts by authorized administrators. Organizations should also carefully consider the network placement of remote access servers; in most cases, a server should be placed at an organization's network perimeter so that it acts as a single point of entry to the network and enforces the telework security policy before any remote access traffic is permitted into the organization's internal networks.

Secure telework client devices against common threats and maintain their security regularly.

There are many threats to telework client devices, including malware and device loss or theft. Generally, telework client devices should include all the local security controls used in the organization's secure configuration baseline for its non-telework client devices. Examples are applying operating system and application updates promptly, disabling unneeded services, and using antimalware software and a personal firewall. However, because telework devices are generally at greater risk in external environments than in enterprise environments, additional security controls are recommended, such as encrypting sensitive data stored on the devices.

Existing security controls may need to be adjusted. For example, if a personal firewall on a telework client device has a single policy for all environments, then it is likely to be too restrictive in some situations and not restrictive enough in others. Whenever possible, organizations should use personal firewalls capable of supporting multiple policies for their telework client devices and configure the firewalls properly for the enterprise environment and an external environment, at a minimum.

Organizations should ensure that all types of telework client devices are secured, including PCs, cell phones, and PDAs. For PCs, this includes physical security (for example, using cable locks to deter theft). For devices other than PCs, security capabilities and the appropriate security actions vary widely by device type and specific products, so organizations should provide guidance to device administrators and users who are responsible for securing telework consumer devices on how they should secure them.

More Information

Because telework and remote access technologies interface with so many other types of technologies, ranging from client devices to enterprise authentication services, organizations are encouraged to take advantage of the resources that are

listed in the appendices to NIST SP 800-46 Revision 1 for additional information.

Publications developed by NIST's Information Technology Laboratory help information management and information security personnel in planning and implementing a comprehensive approach to information security. The security of telework and remote access solutions depends upon attention to basic issues such as security planning, security awareness and training, risk management, application of cryptographic methods, and use of security controls. Organizations can draw upon NIST standards and guidelines on these issues and other issues related to the protection of networks and devices, including:

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

NIST SP 800-48, Rev. 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*

NIST SP 800-53, Rev. 2, *Recommended Security Controls for Federal Information Systems*

NIST SP 800-63 Version 1.0.2, *Electronic Authentication Guidelines*

NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*

NIST SP 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*

NIST SP 800-77, *Guide to IPsec VPNs*

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*

NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*

NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*

NIST SP 800-113, *Guide to SSL VPNs*

NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*

NIST SP 800-121, *Guide to Bluetooth Security*

NIST SP 800-123, *Guide to General Server Security*

NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*

For information about NIST standards and guidelines, as well as other security-related publications that help organizations protect their telework and remote access solutions, see NIST's Web page: http://csrc.nist.gov/publications/index.html

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.