December 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURING EXTERNAL COMPUTERS AND OTHER DEVICES USED BY TELEWORKERS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Many workers highly value the arrangements that they have with their employers to work from home or from other locations away from their organizations' facilities. This popular practice of teleworking, or telecommuting, benefits both the organizations and their staff members, who are able to read and send email, access Web sites, review and edit documents, and perform many other tasks from remote sites. These teleworkers use devices such as desktop and laptop computers, personal digital assistants (PDAs), and cell phones to access their organization's nonpublic computing resources and to conduct business from them when they are at home or traveling.

For many years, teleworkers were limited in their activities because their dial-up modems, which were the primary communications mechanism for remote access, operated at slow speeds. Today high-speed Internet connectivity and broadband communications provide fast data transfer rates, greatly expanding the productive use of remote access capabilities by teleworkers. But with increasing intruder attacks and other threats in today's computing environment, teleworkers and their organizations are challenged to plan carefully to protect the security of telework devices, networks, and information resources.

User's Guide to Securing External Devices for Telework and Remote Access

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) has issued a new guide that provides practical advice to help workers secure their external devices that they need for teleworking. NIST Special Publication (SP) 800-114, *User's Guide to Securing External Devices for Telework and Remote Access: Recommendations of the National Institute of Standards and Technology*, written by Karen Scarfone and Murugiah Souppaya, focuses on the security of the teleworker's computing devices and recommends steps to protect the devices, the computer operating systems (OSs) and applications, and the home networks that the computers use.

The guide provides an overview of telework technologies and the security issues related to the use of telework devices. The basic issues of securing information and home networks, and of using external networks, are discussed. Recommendations to users cover protecting their devices, computer operating systems and applications, and for protecting the information stored on telework computers and removable media. Advice is provided for protecting the

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 November 2006:

- *Guide to Securing Computers Using Windows XP Home Edition, November 2006*
- *Maintaining Effective Information Technology (IT) Security Through Test, Training, and Exercise Programs, December 2006*
- *Security Controls for Information Systems: Revised Guidelines Issued by NIST, January 2007*
- *Intrusion Detection and Prevention Systems, February 2007*
- *Improving the Security of Electronic Mail: Updated Guidelines Issued by NIST, March 2007*
- *Securing Wireless Networks, April 2007*
- *Securing Radio Frequency Identification (RFID) Systems, May 2007*
- *Forensic Techniques for Cell Phones, June 2007*
- *Border Gateway Protocol Security, July 2007*
- *Secure Web Services, August 2007*
- *The Common Vulnerability Scoring System, October 2007*
- *Using Storage Encryption Technologies to Protect End User Devices, November 2007*

wireless home networks that are used for remote access communications.

A section of NIST SP 800-114 focuses on protecting cell phones, PDAs, and smart phones, such as hybrid cell phone/PDA devices (for example, BlackBerry and Windows Mobile devices). Another section guides teleworkers in the safe use of devices that are secured by a third party, such as a computer provided for public use at a conference or hotel.

The publication's useful appendices present supplemental information and supporting material, including security-related considerations for telework, such as using cellular phones and Voice over Internet Protocol (VoIP) phone services; using wireless personal area network (WPAN) technologies such as Bluetooth; using wireless broadband data cards; and ensuring the secure destruction of removable media and printed materials that might contain sensitive information. Also included in the appendices are a glossary, a list of acronyms and abbreviations, and a list of in-print resources and online tools and resources that users may wish to consult for additional information about securing their telework devices.

NIST SP 800-114 is available at NIST's Web site at http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf.

Who We Are
The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

Security of Telework Devices: A Challenge for Workers and Their Organizations

Both personal computers and consumer devices are used for telework, and different ownership arrangements apply to the devices. Personal computers (PCs) are desktop and laptop computers that run standard PC OSs (e.g., Windows, Linux/UNIX, Mac OS). These devices gain access to broadband networks through cable modems, digital subscriber lines, satellite, and wireless connections. Consumer devices are small, usually mobile, computers that do not run standard PC OSs. Examples are networking-capable PDAs, cell phones, and video game systems. Consumer devices are most often used for remote access applications that use Web browsers, primarily Secure Sockets Layer (SSL) Virtual Private Networks (VPNs) and individual Web application access.

Telework devices may be owned, configured, and managed by the worker's organization and can be used for any of the organization's access methods. Some teleworker devices are owned by the worker, who is responsible for securing them and maintaining their security. Another arrangement is the devices that are owned, configured, and secured by third parties, such as kiosk computers at hotels, and PCs or consumer devices owned by friends and family of the worker. Remote access options for third party-secured devices are usually limited because users are often unable to install software onto them, such as VPN software, terminal server software, and Web browser plug-ins.

Because of their security policies and technology limitations, organizations often limit the types of devices that can be used for remote access. An organization might require the worker to use only the organization's PCs. Some organizations have tiered access levels, such as allowing the organization's PCs to access many resources, teleworker-owned PCs to access a more limited set of resources, and consumer devices and third-party PCs to access only one or two resources, such as Web-based email. This 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. Before they use their own or third-party computers for remote access to their organization's resources, teleworkers should check to confirm that the organization's latest policies allow such access.

There are risks associated with remote access to information resources in general, and broadband communications, if not properly protected, can be especially vulnerable to intruder attacks. When a telework device uses remote access, it is essentially a logical extension of the organization's own network. Therefore, if the telework device is not secured properly, it poses additional risk not only to the information that the teleworker accesses but also to the organization's other systems and networks. For example, a telework device infected with a worm could spread the worm through remote access to the organization's internal computers. Therefore, telework devices should be secured properly and have their security maintained regularly.

Many organizations automatically check the security health of each telework device that attempts to use remote access to the organization's information resources to ensure that the device complies with the organization's policies. Examples of the checks that an organization might conduct are verifying that the OS is fully patched, that antivirus software is installed and up-to-date, and that a personal firewall is enabled. The organization can also check if the device has been secured by the organization and whether the device is a desktop or laptop computer, a PDA, a video game system, or other device. Based on the results of these checks, the organization can determine whether the device should be permitted to use remote access.

With good planning and careful implementation of sensible guidelines, organizations can support the popular practice of telecommuting, while protecting their networks and information resources.

Threats to External Devices

People who want to cause mischief, disrupt organizational operations, and commit fraud are a major threat to the security of external devices used by teleworkers. Telework devices are susceptible to the insertion of malware, also known as malicious code. Malware is a computer program that is covertly placed onto a computing device with the intent of compromising the confidentiality, integrity, or availability of the device's data, applications, or OS. Common types of malware threats include viruses, worms, malicious mobile code, Trojan horses, rootkits, and spyware. Malware threats can infect devices through email, Web sites, file downloads and file sharing, peer-to-peer software, and instant messaging. Another common threat for telework devices is the loss or theft of the device. Someone with physical access to a device has many options for attempting to view the information stored on it.

Teleworkers can increase the security of their devices by adopting security protections, or security controls. These measures taken against the threats compensate for the device's security weaknesses, or vulnerabilities. Some vulnerabilities can be eliminated through security protections. For example, the user can enable a feature in an application to automatically download and install new versions of the application to correct previous errors. Some vulnerabilities cannot be eliminated, but security protections can prevent attacks. For example, antivirus software can stop an infected email from being opened by a user, or hard drive encryption can make files unreadable by others. However, not all vulnerabilities can be eliminated. The complexity of computing and remote access makes total protection of information resources almost impossible. But organizations can realize a more realistic goal of applying security protections to give attackers as few opportunities as feasible to gain access to a device or to damage the device's software or information.

NIST Recommendations

Teleworkers should take an important first step before implementing any of the recommendations or suggestions in the guide. They should back up all of their data and verify the validity of the backups. Users with limited experience in configuring personal computers, consumer devices, or home networks should seek expert assistance in applying the guide's recommendations to avoid any potential losses of data, device, or application functionality.

NIST recommends that teleworkers take the following steps to improve and maintain the security of their external telework devices:

*** Become thoroughly familiar with their organization's policies and requirements, and know how to protect the organization's information that they may access.**

Sensitive information that is stored on or sent to or from external telework devices must be protected. It is important to prevent malicious parties from accessing or altering information. An unauthorized release of sensitive information could damage the public's trust in the organization, jeopardize the mission of the organization, or harm the individuals whose personal information is compromised. Many methods can be employed to protect the personal information that is accessed during teleworking, including protecting the physical security of telework devices, encrypting files stored on devices, and ensuring that information stored on devices is backed up.

*** Ensure that all the telework devices used on wired and wireless home networks are properly secured, and that home networks are protected also.**

Appropriate security measures should be applied to the PCs and consumer devices that use the same wired and wireless home networks to which the telework device normally connects. If these other devices become infected with malware or are otherwise compromised, they could attack the telework device or eavesdrop on its communications. Teleworkers should also be cautious about allowing others to place devices on the teleworkers' home networks, in case one of these devices is compromised.

Teleworkers should also apply security measures to the home networks to which their telework devices normally connect. One example of such a security measure is to use a broadband router or firewall appliance to prevent computers outside the home network from initiating communications with telework devices on the home network. Another example is to ensure that sensitive information transmitted over a wireless home network is adequately protected through strong encryption.

*** Secure the operating systems and primary applications of desktop or laptop PCs that the teleworker owns and uses for telework.**

Securing a telework PC includes the following actions:

-- Use a combination of security software, such as antivirus and antispyware software, personal firewalls, spam and Web content filtering, and popup blocking, to stop most attacks, particularly malware.

-- Restrict who can use the PC by having a separate standard user account for each person; assign a password to each user account; use the standard user accounts for daily use; and protect user sessions from unauthorized physical access.

-- Ensure that updates are regularly applied to the operating system and primary applications, such as Web browsers, email clients, instant messaging clients, and security software.

-- Disable unneeded networking features on the PC and configure wireless networking securely.

-- Configure primary applications to filter content and stop other activity that is likely to be malicious.

-- Install and use only known and trusted software.

-- Configure remote access software based on the organization's requirements and recommendations.

-- Maintain the security of the PC on an ongoing basis, such as changing passwords regularly and checking the status of security software periodically.

*** Secure the consumer devices that the teleworker owns and uses for telework, based on the security recommendations of the devices' manufacturers.**

A wide variety of consumer devices exists, and security features available for these devices also vary widely. While some devices offer only a few basic features, others offer sophisticated features similar to those offered by PCs. Devices with less sophisticated features are not necessarily less secure than those with many more security features. Many devices offer more security features because the capabilities that they provide, such as access to wireless networking and capabilities for instant messaging, make them more susceptible to attack than devices without these capabilities.

General recommendations for securing telework devices are:

-- Limit access to the device, such as setting a personal identification number (PIN) or password and automatically locking a device after an idle period.

-- Disable networking capabilities, such as Bluetooth, except when they are needed.

-- Use additional security software, such as antivirus software and personal firewalls, if appropriate.

-- Ensure that security updates, if available, are acquired and installed at least monthly, preferably weekly.

-- Configure applications to support security, such as blocking activity that is likely to be malicious.

*** Consider the security state of a third-party device before using it for telework.**

Teleworkers often want to perform remote access to their organization's network from third-party devices. They may want to check their email from a kiosk computer at a conference, for example. However, they may not know if such devices have been secured properly or if they have been compromised. Consequently, a teleworker could use a third-party device infected with malware that steals information from users (e.g., passwords or email messages). Many organizations either forbid third-party devices to be used for remote access or permit only limited use, such as for Web-based email. Teleworkers should consider who is responsible for securing a third-party device and who can access the device before deciding whether or not to use it. Whenever possible, teleworkers should not use publicly accessible third-party devices for telework, and teleworkers should avoid using any third-party devices for performing sensitive functions or accessing sensitive information.

More Information

NIST SP 800-114 was originally issued for public comment as an update to NIST SP 800-46, *Security for Telecommuting and Broadband Communications*. However, as the scope of NIST SP 800-114 evolved, NIST decided to issue it as a supplement to SP 800-46, rather than as a replacement.

NIST SP 800-114, NIST SP 800-46 and other NIST publications assist organizations in planning and implementing a comprehensive approach to information security. For information about NIST standards and guidelines that are referenced in the security guide for teleworker devices, as well as other security-related publications, see NIST's Web page at http://csrc.nist.gov/publications/index.html.

For information about standards and guidance for protecting information, communications, and operations through the application of cryptographic security techniques, see http://csrc.nist.gov/groups/ST/toolkit/index.html.

Many manufacturers document their security recommendations in their product documentation or on their Web sites. Some manufacturers also make security checklists available for securing their operating systems, applications, and devices. Many of these checklists are posted on the NIST Security Checklists for IT Products site, located at http://csrc.nist.gov/checklists/.