ITL BULLETIN

ITL BULLETIN MARCH 2020

Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions

Karen Scarfone[1], Jeffrey Greene, and Murugiah Souppaya
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Many people *telework* (also known as *telecommuting*), which is the ability for an organization's employees, contractors, business partners, vendors, and other users to perform work from locations other than the organization's facilities. Teleworkers use various client devices, such as desktop and laptop computers, smartphones, and tablets, to read and send email, access websites, review and edit documents, and perform many other tasks. These client devices may be controlled by the organization, by third parties (the organization's contractors, business partners, or vendors), or by the users themselves (e.g., BYOD). 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 National Institute of Standards and Technology (NIST) has guidelines on telework and remote access to help organizations mitigate security risks associated with the enterprise technologies used for teleworking, such as remote access servers, telework client devices, and remote access communications. NIST Special Publication (SP) 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* was issued in 2016, and its recommendations are still relevant today. This Information Technology Laboratory (ITL) Bulletin summarizes key concepts and recommendations from SP 800-46 Revision 2. They include deploying some or all of the following security measures:

- Developing and enforcing a telework security policy, such as having tiered levels of remote access
- Requiring multi-factor authentication for enterprise access

[1] Karen Scarfone is a NIST Associate from Scarfone Cybersecurity.

- Using validated encryption technologies to protect communications and data stored on the client devices
- Ensuring that remote access servers are secured effectively and kept fully patched
- Securing all types of telework client devices—including desktop and laptop computers, smartphones, and tablets—against common threats

Remote Access Methods

Organizations have many options for providing remote access to their computing resources. The remote access methods most commonly used by teleworkers are divided into four categories based on their high-level architectures: tunneling, portals, direct application access, and remote desktop access.

Tunneling involves establishing a secure communications tunnel between a telework client device and a remote access server, typically a virtual private network (VPN) gateway. The tunnel uses cryptography to protect the confidentiality 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. The types of VPNs most commonly used for teleworking are Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL) tunnels.

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. Most portal architectures today are SSL VPNs, and in fact, most SSL VPNs are portals, not tunnels.

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 webmail. The teleworker runs a web browser and connects using Hypertext Transfer Protocol Secure (HTTPS) to a web server that provides email access, and then the server authenticates the teleworker. For cases such as webmail that use a ubiquitous application client (e.g., a web browser), direct application access provides a highly flexible remote access solution that can be used from nearly any client device.

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 input control (e.g., keyboard, mouse) over the remote computer and sees that computer's screen on the local telework client device's screen. Generally, remote desktop access solutions, such as those using the Microsoft Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC), should only be used for exceptional cases after a careful analysis of the security risks. The other types of remote access solutions described in this bulletin offer superior security capabilities.

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

A **lack of physical security** controls is an issue because telework client devices are used in a variety of locations outside of the organization's control, such as employees' homes, coffee shops, and other businesses. 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.

Unsecured networks are 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 broadband networks, such as cable, and wireless mechanisms, such as Institute of Electrical and Electronics Engineers (IEEE) 802.11 and cellular networks. These communications systems are susceptible to eavesdropping as well as man-in-the-middle attacks to intercept and modify communications.

Providing external access to internal-only resources such as sensitive servers will expose them to new threats 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. NIST recommends that organizations apply the following safeguards to improve the security of their telework and remote access technologies:

Plan telework-related 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 malicious parties will gain control of telework client devices and attempt to recover sensitive data from them or leverage the devices to gain access to the enterprise network. Options for mitigating this type of threat include encrypting the device's storage, encrypting all sensitive data stored on client devices, and not storing sensitive data on client devices. For mitigating device reuse threats, the primary option is using strong authentication—preferably multi-factor—for enterprise access.

Organizations should also assume that communications on external networks, which are outside of the organization's control, are susceptible to eavesdropping, interception, and modification. These types of threats can be mitigated, although 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 the use of anti-malware technologies, network access control solutions that verify the client's security posture before granting access, and 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, remote access, and BYOD 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 computers to access many resources, BYOD computers to access a limited set of resources, and BYOD mobile devices to access only one or two lower risk resources, such as webmail. 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.

Ensure that remote access servers are secured effectively and configured to enforce telework security policies.
The security of remote access servers is particularly important because they provide a way for external hosts to gain access to internal resources, as well as providing a secured, isolated telework environment for organization-issued, third party-controlled, and BYOD client devices. In addition to permitting unauthorized access to enterprise resources and telework client devices, a compromised server could be used to eavesdrop on communications, manipulate them, and 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 organization-controlled telework client devices against common threats, and maintain their security regularly.
There are many threats to telework client devices, including malware, device loss or theft, and social engineering. Generally, telework client devices should include all of the local security controls used in the organization's secure configuration baseline for its non-telework client devices, such as applying operating system and application updates promptly, disabling unneeded services, and using anti-malware 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.

Organizations should ensure that all types of telework client devices are secured, including desktop and laptop computers, smartphones, and tablets. 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 devices on how they should secure them.

Conclusion

Making an organization's resources remotely accessible enables telework but also increases security risk. Organizations should carefully consider the balance between the benefits of providing remote access to additional resources and the potential impact of a compromise of those resources. To mitigate risk, organizations should ensure that any internal resources they choose to make available through remote access for telework purposes are hardened against external threats and that access to the resources is limited to the minimum necessary.

Additional Resources:

- NIST Special Publication (SP) 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*
- NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*
- NIST SP 800-77 Revision 1 (Draft), *Guide to IPsec VPNs*
- NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
- NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*
- NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*
- NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*
- NIST SP 1800-4, *Mobile Device Security: Cloud and Hybrid Builds*
- NIST SP 1800-21 (Draft), *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)*
- National Checklist Program Repository

ITL Bulletin Publisher: Katherine Green
Information Technology Laboratory
National Institute of Standards and Technology
katherine.green@nist.gov