SOLARWINDS WHITEPAPER

The Road to Secure Remote Connectivity and Safer Telecommuting

© 2015, SolarWinds Worldwide, LLC. All rights reserved.

Follow SolarWinds:

solarwinds

As telecommuting is becoming increasingly common in all types of organizations and businesses, it is important to make sure these practices are made secure so that the technology of remote IT can be achieved without any fears of security compromise and compliance violation.

Remote access or remote connectivity is the term used to describe how telecommuting employees access data from an organization's private network. Remote access has become so commonplace that employees connect to virtual machines, remote desktops; and IT teams use remote access to provide remote IT administration and support. While the advantages of remote connectivity are manifold in terms of simplicity and accessibility, security is one of the thorniest issues that employees and administrators need to be aware of while dealing with remote administration tools. This paper will highlight security technologies included in remote administration software and how administrators can use them to establish secure links to accessing computers both inside and outside the network firewall.

COMMON APPLICATIONS OF REMOTE DESKTOP ACCESS

- Employees in organizations use remote desktop access to connect to remote machines, virtual machines, etc. within the network, and also to initiate screen-sharing sessions with peers
- IT administrators and support technicians extensively use remote access to provide desktop support to end-users and troubleshoot system issues

In the Hands of the Hacker

Once cyber-criminals (those who exploit weakness in secure systems) gain access to one system in a network, they can then easily infect all other systems within that network. This allows them to steal business-sensitive information like usernames, passwords, credit card details, bank account details, personal information, etc. Spying is another reason attackers infect systems. Spying includes the following:

- Watching what is displayed on the system
- Capturing images with the webcam
- Getting the location of the system
- Reading or copying files and data from the system
- Introducing malware or code injection into secure systems

Employees use remote access software to gain remote access to private networks and IT administrators use them to troubleshoot employees' remote devices. When the remote access tool being used is not properly secured, it provides an easy path for an attacker to gain access into the organization's private network. Remote access tools usually use a particular port (for example, 3389 is the default port used by Windows® Remote Desktop Protocol service) for receiving and transmitting data. Though the port used by each remote access solution will vary, attackers using a port scan can easily find out which is being used.

FACING THE FACTS

According to Verizon Data Breach Investigation Report 2012[1] , *Remote access services (e.g., VNC, RDP) continue their rise in prevalence,* ***accounting for 88% of all breaches leveraging hacking techniques—more than any other vector****. Remote services accessible from the entire Internet, combined with default, weak, or stolen credentials continue to plague smaller retail and hospitality organizations. Often these victims share the same support and/or software vendor. Scripted attacks seeking victims with known remote access ports (TCP 3389, RDP or VNC), followed with issuance of known default vendor credentials, allow for targets of opportunity to be discovered and compromised in an automated and efficient manner.*

How to Secure Remote Access & Remote Connectivity

The technology of remote connectivity is used by remote administration tools for the centralized administration and troubleshooting remote computers. In order to decrease the chance hackers will gain access to their corporate networks, organizations must be sure to select remote access tools with good authentication and encryption methods.

Authentication

Most remote administration applications use PKI (Public Key Infrastructure) technology for secured authentication. A PKI enables users of an unsecure public network (i.e. the Internet) to securely and privately exchange data through the use of a public and private cryptographic key pair that is obtained and shared through a trusted authority. In the public key cryptography method, a secret key is created and shared between the sender and responder for encrypting and decrypting the messages. PKI solutions claim advantages such as confidentiality, authenticity, integrity, and non-repudiation. But these advantages cannot be delivered if the credentials of a session are stolen.

- **Smart Card Authentication**: Smart Card authentication is the ideal authentication mechanism because it makes hacking of information highly sophisticated, time-consuming, and expensive. In cases where smart card authentication is not used, attackers will gain access to the user's system by placing the user credentials (PKI vendor credentials files, key files, etc. which can be obtained easily with software like Back Orifice or SubSeven) in a 'PKI credentials' folder on their system. But when Smart Card authentication is used, PKI credentials are stored in the card and not in the 'PKI credentials' folder. This prevents the attacker from logging in with the credentials placed in their 'PKI credentials' folder.

- **Multi-Factor Authentication:** This method allows a user to authenticates with multiple authenticating factors:
  - Data factors – Information that the user knows such as example passwords, PINs, etc.
  - Property factors – Hardware that the user owns such as smart cards, RSA secure tokens, etc.
  - Physical factors – Physical types of identification such as biometrics, fingerprints, retinal scans, etc.

Encryption

Encryption means converting data into a form which cannot be easily decrypted by unauthorized people, commonly known as Ciphertext. Ciphertext can be decrypted only with the help of a decryption key. Encryption is very important, especially while transferring the data through the Internet because anyone can easily eavesdrop on communication by interpreting unencrypted data. There are different methods used for encryption, most common and well-known ones being RSA and AES.

- **RSA:** The most famous and commonly used encryption system is RSA. RSA uses both a public and private key to encrypt the message. The opposite key of that which is used to encrypt the message is needed to decrypt the message—making it extremely difficult for hackers to decrypt. RSA uses two large prime numbers for its encryption. The basic security of RSA depends on the fact that it is difficult to find prime factors of a composite number. There are two ways that a message can be encrypted/ decrypted: encrypt with the public key and decrypt with the private key and vice versa.

- **AES:** A publicly available and frequently used method of encryption, this approach uses an algorithm based on many substitutions, permutations, and linear transformations. All the operations are done on data blocks of 16 bytes and the operations are repeated several times in a process known as ‘rounds’. A unique roundkey is generated during each round and then incorporated in the calculation. The block structure of AES makes it difficult for attackers to decrypt the cipher. There are different versions in AES – AES-128, AES-192, and AES-256. The only difference between each version of AES is the length of the key – 128 bit, 192 bit, or 256 bit correspondingly.

Internet Proxy

When on-the-fly and after-hours support are becoming more common in organizations, IT teams incorporate secure technologies to support end-users when they are outside the firewall, and without VPN connectivity. (For example, supporting travelling end-users like the sales team.) In addition to authentication and encryption, there has to be a secure channel such as an Internet proxy to help connect remote machines over the Internet.

An Internet proxy is deployed within the firewall which acts as the secure medium to transmit data between the IT admin using the remote administration tool inside the network and the end-user whose remote machine is outside the firewall. The proxy server terminates all unwanted traffic coming in from the Internet and additionally ensures the integrity of the IT admin’s workstation or server is not exposed directly to the Internet.

So, if you are considering selecting a remote access software for supporting end-users outside the firewall, make sure there is a secure Internet proxy component included in the deployment to safely connect to systems outside the network firewall.

8 Security Tips to Protect Against Remote Connectivity Breaches

Here are some tips for IT teams to secure remote connectivity and prevent malicious entities and intruders from gaining access into private networks:

1. Secure the network with anti-malware solutions in order to detect and isolate a Trojan before it can install any kind of script onto systems.
2. Adapt the usage of a strong user logon password for remote connections. Also, make sure the password is changed in regular intervals.
3. Ensure that all software and operating systems are patched and up to date. The latest patches will always have fixes to known vulnerabilities.
4. Educate end-users and warn them to be careful while opening emails from unknown senders, especially mails with attachments.
5. Maintain a log of activities done through remote administration. Audit logs on a regular basis and take immediate action if you find any trail of abnormal activities.
6. Keep a constant check on the organization's firewall. If possible, allow only known IP addresses to connect to the network.
7. Configure alerts on the firewall to inform you when there is any port scan happening from outside the firewall.
8. Ensure the remote administration tool you use has end-to-end integrity and control. Proper authentication and encryption methods such as AES or RSA give end-to-end integrity and control to the remote administration tool.

Security is a critical factor which should be properly analyzed before implementing a remote administration tool. Check for the various authentication types available, especially Smart Card authentication which can go a long way in protecting your network. Encryption is another important aspect. When connecting to remote machines over third-party insecure networks such as the Internet, ensure that proper authentication and encryption are available for the remote support tool which initiates the remote connection.

DameWare® Provides Secure Remote Connectivity

DameWare Remote Support is a centralized and easy-to-use remote administration software that enables IT pros to connect to their client machines for IT support and troubleshooting. DameWare Remote Support includes DameWare Mini Remote Control, a remote control tool that provides the capability to remotely connect to Windows®, Linux® and Mac OS® X computers.

DameWare provides an array of secure remote connectivity options including:

- Proprietary Challenge/Response
- Windows NT Challenge/Response
- Encrypted Windows Logon
- Smart Card Logon & Authentication

Smart Card Logon & Authentication

DameWare was the first remote administration software to offer Smart Card authentication and interactive Smart Card logon. This strengthens identity and authentication management for remote desktop connections, and provides two-factor authentication for remote administration in secure networks. Learn more »

Secure Internet Proxy for Over-the-Internet Remote Session

With the help of secure Internet proxy, DameWare ensures secure remote connectivity to end-users located outside the network firewall. When end-users are situated outside the network without VPN connectivity, DameWare Remote Support allows IT technicians the option to access these remote machines via a secure Internet proxy server. The end-user only needs to have Internet access to support this remote connectivity. Learn more »

Secure Mobile Gateway for Remote Connectivity from Mobile

The optional mobile gateway server provides secure access for IT technicians to remote control end-user systems from their mobile interfaces (iOS® and Android™). The DameWare Mobile Gateway service can be configured on a server that is placed in a DMZ, internet-facing, or accessible through a VPN connection. Remote sessions initiated from mobile devices are controlled by the mobile gateway, ensuring secure connections through a server that you control. Learn more »

Trusted by the U.S. Army

DameWare is a brand trusted by the U.S. Army, DoD, and other civilian and intelligence agencies. DameWare has received U.S. Army Certificate of Networthiness (CoN) which ensures that the software meets strict U.S. Army and Department of Defense (DoD) standards for security, compatibility and sustainability.

LEARN MORE

DOWNLOAD FREE TRIAL

Fully Functional for 14 Days

About SolarWinds®

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack®, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at http://www.solarwinds.com.