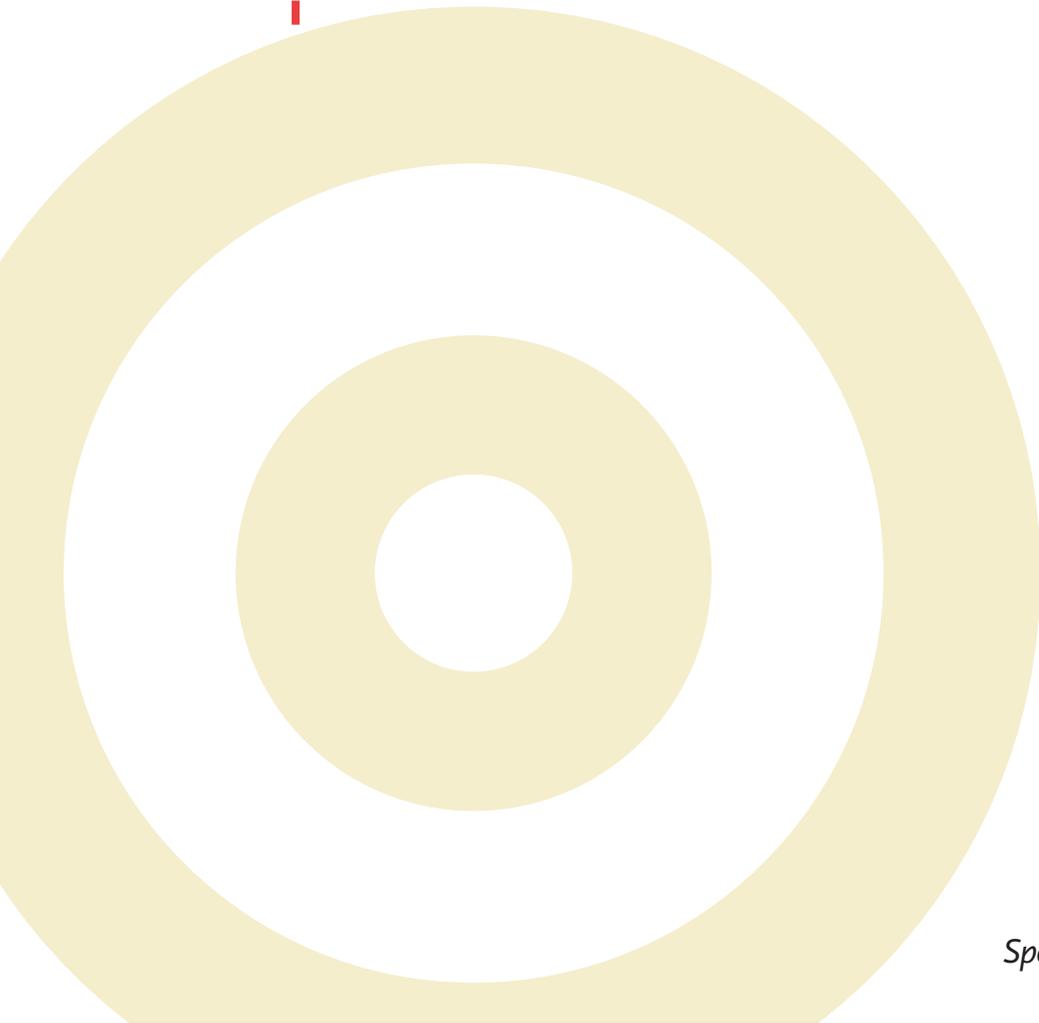


10 Remote Access Tips in 10 Minutes

By Lisa Phifer



Sponsored By:



10 Remote Access Tips in 10 Minutes

By Lisa Phifer

© 2006 TechTarget

BIO

Lisa Phifer is a site expert and contributor to SearchNetworking.com. Lisa owns Core Competence Inc., a consulting firm specializing in networking, security, and management technology. She has been involved in the design, implementation, and evaluation of these products for nearly 25 years. Over the past 10 years, she has been heavily involved with secure remote access and Virtual Private Networking, as both a user and network administrator.

This *IT Briefing* is based on a Hewlett Packard/TechTarget Webcast, “10 Remote Access Tips in 10 Minutes.” To view this Webcast online, please click the link:

Contents

• About TechTarget IT Briefings	1
• 1. Lock Down Laptops.....	1
• 2. Harden Hosts.....	1
• 3. Protect Endpoint Integrity.....	1
• 4. Eliminate Vulnerabilities	2
• 5. Enforce Endpoint Security	2
• 6. Leave Nothing Behind.....	2
• 7. Avoid Wireless Promiscuity.....	2
• 8. Safeguard Communication	3
• 9. Strengthen Authentication.....	3
• 10. Narrow Access.....	3
• Conclusion.....	4
• About TechTarget.....	4
• What makes us unique?.....	4

Copyright © 2006 Lisa Phifer All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

About TechTarget *IT Briefings*

TechTarget IT Briefings provide the pertinent information that senior level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor Connection and Expert Webcasts, TechTarget-produced IT Briefings turn Webcasts into easy-to-follow technical briefs, similar to a white paper.

Design Copyright © 2004 - 2005 TechTarget. All Rights Reserved.

For inquiries and additional information, contact:
Dennis Shiao
Director of Product Management, Webcasts
dshiao@techtargt.com

10 Remote Access Tips in 10 Minutes

Introduction

Today, about two out of three workers are now mobile, demanding anywhere access to corporate networks, services and data. Remote access solutions are increasingly being required to address connecting over any kind of link, from broadband to Wi-Fi; using any kind of device, from laptop to PDA to public PC; and working from any location - whether at home, in a hotel, at a hot spot or someone else's corporate LAN.

Keeping workers productive without compromising security has become a complex and expensive task. This document provides 10 quick tips that will help a person lock down those remote endpoints and safeguard the corporate data that they send.

1. Lock Down Laptops

It might not be particularly high tech, but many companies fall victim to mobile device loss and theft. Worse, even though most missing laptops, PDA's, and smartphones carry sensitive data, only about one in four are protected with measures that would actually pass regulatory requirements, like HIPPA or SOX.

Locking down mobile devices is an easy way to prevent disclosure of confidential data, logins and passwords should lost devices fall into the wrong hands. At minimum, every device should be locked with a native operating system PIN or password. For ease of use, consider alternatives like fingerprint readers, which are now built into some laptops and PDAs.

Data stored on mobile devices should be protected by using built-in file system encryption, boot level device encryption, or selective file encryption. This prevents data disclosure when passwords are guessed or when devices are sold without being wiped clean.

2. Harden Hosts

Devices that connect to your network over a VPN tunnel extend your network's security perimeter. Personal firewalls and host intrusion detection systems can establish "mini" perimeters around each of those remote endpoints, deflecting network-borne attack. It is surprising how many companies fail to deploy these basic host security measures. Two out of three companies use personal firewalls somewhere, but less than one-fourth routinely deploy them on every single host. Fewer still have deployed or trialed host intrusion detection. When it comes to remote access, both should be mandatory, allowing only necessary inbound and outbound traffic.

Limited one-way firewalls are built into operating systems like Windows XP, but enterprises should really use centrally administered desktop firewalls that combine two-way filtering with the ability to detect when trusted programs have been overwritten. Unlike their residential-grade counterparts, these enterprise products let information technology departments gather security logs, establish uniform policies and enforce updates.

3. Protect Endpoint Integrity

If that PDA or laptop at the far end of the tunnel has been compromised by a virus, worm or Trojan, then your VPN has just opened a backdoor into your network. This was true back in the days of dial-up too, but high-speed broadband and wireless connections have drastically increased the probability of host compromise.

Firewalls and host IDS help to protect the integrity of VPN tunnel remote endpoints, but they are not enough. Most malicious code is carried by e-mail and Web traffic that passes right through the firewall. Therefore, every device used for remote access – and that includes PDAs and smartphones – should be scanned for viruses and spyware. Devices that check e-mail should also use spam filters.

Malicious code that reaches the host can often be stopped by using features in your Web browser or e-mail client. For example, spyware can often be blocked by configuring Internet Explorer to reject Java Applets and Active X Controls. Another helpful technique is to blacklist e-mail or Web traffic from known malicious sites.

4. Eliminate Vulnerabilities

Once security measures are deployed, they must be kept up to date. Vendors like to talk about zero-day attack mitigation, but the vast majority of attacks exploit vulnerabilities for which patches are already known. The real problem is that those updates do not get deployed fast enough.

Most operating systems, many applications and every worthwhile security product can be configured to automatically apply updates. At a minimum, employees should be educated about using auto updates on personal PCs and PDAs that are used for remote access. When a company has IT control over a device that is used for remote access, then that company should assume IT responsibility for patch management, pushing any missing updates when the endpoint next connects to your VPN.

Most attacks target widely deployed applications. For that reason, companies might want to consider reducing risk by replacing some frequently exploited programs with alternatives. For example, you might encourage the use of Firefox instead of Internet Explorer.

5. Enforce Endpoint Security

Another common mistake is to assume that security measures have been correctly installed, configured, and are still running when a remote user connects to your network. End users and malware frequently disable and remove programs that get in their way. Virus outbreaks like Zotob have repeatedly illustrated this problem.

Cisco, Microsoft, and the Trusted Computing Group have all created architectures that enable analysis, reporting and enforcement of endpoint security. NAC and TNC let policy enforcement points – VPN gateways, routers, switches, and wireless access

points – check an endpoint's security state before that device is granted access to network resources. Devices that are missing patches, infected with viruses or otherwise untrustworthy can be denied network access, or redirected to a quarantine area.

Products that implement TNC are now emerging from companies such as InfoExpress, Funk and Senforce. Companies should check with their desktop security and VPN vendors to identify partnerships related to endpoint trust assessment and security enforcement.

6. Leave Nothing Behind

The trust assessment described in tip 5 applies just as much - if not more - to endpoints that lie beyond anyone's control. Specifically, those public use PCs found in business centers, Internet cafes, and airport kiosks. Many mobile workers use those PCs, with or without their company's permission, to check e-mail, download files, and access Web portals. It is not at all uncommon to find data left behind on these PCs, including logins, passwords, cached Web objects, and temporary files. Public PCs can also harbor malware that records user keystrokes.

Companies should consider taking steps to provide limited-but-secure access from public PCs. For example, some SSL VPNs can scan those PCs before prompting users for passwords. Many SSL VPNs clean up after themselves when the user's session ends. Some SSL VPNs can restrict public PC access to sensitive applications, or convert documents into images so that text cannot be left behind. Another option is to create a secure sandbox on a public PC. Some SSL VPNs can do this, but another approach is to carry your own secure operating environment with you on a bootable USB drive.

7. Avoid Wireless Promiscuity

Most laptops shipped last year included embedded Wi-Fi. Many PDAs also have Infrared, Bluetooth and 3G wireless. Unfortunately, those interfaces can all be abused either to attack the mobile device itself or to intercept transmitted data.

For example, many Wi-Fi users have at some time linked to the wrong access point, because operating

systems like Windows XP behave promiscuously, reconnecting to any device with the same name as a network that was used at some point in the past. This is a problem because phony access points can be used to run man-in-middle attacks, like breaking into SSL encrypted sessions.

To reduce that risk, devices used for remote access should connect only to known, trusted devices, be they Wi-Fi access points or Bluetooth peers. That can be accomplished through careful configuration of wireless security parameters, like requiring Bluetooth PIN authentication or Wi-Fi 802.1X certificate verification. A host-resident wireless IDS can also alert users to unwanted connections – and perhaps even break the connection before damage is done.

8. Safeguard Communication

Preventing eavesdropping and modification are well-understood security objectives for remote access. However, the consequences of failing to do so have been increasing. Interception of proprietary corporate data is hard to put a price tag on. But violating privacy regulations like HIPAA or GLBA can result in fines, or even criminal penalties. Disclosure laws like CA SB 1386 have made it impossible for companies to look the other way when the incidents do occur. Even end-users now appreciate the consequences of unencrypted communication through Identity Theft.

Individuals, small businesses, and enterprises all should use encryption to protect all data sent over any shared medium, be that broadband, wireless or the public Internet. Those without VPNs can protect their data using secure application connections like SSL-protected Webmail. Many companies are moving from traditional IPsec VPNs to SSL VPNs to reduce administration cost and support remote access from more locations.

No matter what protocol is chosen, it is important to pair that encrypted connection with a trustworthy endpoint, and to take steps to deter man-in-the-middle attacks. For example, when certificate-based server authentication is deployed, users should never accept new, potentially bogus server certificates. When password authentication is used, password

hashes should never be sent over unprotected links – secure tunnels should always be used to protect password authentication, and weak passwords should be strengthened.

9. Strengthen Authentication

In fact, avoiding passwords all together is the safest bet. Plain text passwords are easily compromised, not just through eavesdropping, but through social engineering and carelessness. Users choose easily guessed passwords. They tape them to PCs, they share them with friends, and they give them away to strangers. In one study, seven out of 10 users were willing to trade their passwords to a complete stranger in a subway station just for a chocolate bar!

Many companies enforce password length, complexity and update rules. These measures help to deter dictionary attacks and brute force cracking. But users are more likely to write long passwords down, and even complex passwords can be stolen. Addressing these risks requires using two or more authentication factors. For example, combine a password with a SecurID token or smart card, or combine a PIN with a biometric authentication method like voice recognition or handwritten signature. This prevents password sharing and defeats keystroke loggers. When choosing factors, keep mobile limitations in mind. For example, biometric and smart-card scanners usually are not portable to public PCs, but USB tokens and one-time passwords are.

10. Narrow Access

Companies should take a careful look at their VPN gateway and access rules. Many IPsec VPNs give authenticated remote users unfiltered access to the entire corporate network. But many users do not really require full-network access to complete their jobs. Applying more granular filters can put fewer company resources at risk.

In general, filters should only allow that which is expressly permitted and deny everything else. This means defining policies to grant access on a need-to-know basis. In IPsec VPN, that can be done with

selectors that filter on IP import. In SSL VPN, this can be done with policies that expose selected URLs, data objects and actions. In either case, applying restrictions to home or public PC endpoints can be a good idea.

Also, companies should consider non-VPN remote access alternatives. Employees that just need to check e-mail may not really need a VPN tunnel to accomplish that goal. In some cases, secure applications can meet worker needs just as well – perhaps even better – while exposing less of the corporate network.

Conclusion

A company new to secure remote access should treat these 10 tips as a planning checklist. A company that already has a remote access VPN should review these tips to identify measures that could be added to strengthen existing defenses.

Securing any network is an iterative process of vulnerability assessment and refinement. But do not apply new technologies and approaches just because they are popular. For example, does your work force really require remote access from public-use PCs? Could your company reduce cost by allowing remote access from home PCs? Many counter measures that apply to these scenarios are less relevant for work forces that only use tightly controlled company-owned laptops.

Take a good look your business needs for remote access and the additional risks and vulnerabilities that your company's remote access solutions create. Then incrementally deploy additional measures that address your biggest risks, commensurate with potential benefits.



About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes target media that address your need for information and resources. Our network of industry-specific Web sites give enterprise IT professionals access to experts and peers, original content and link to relevant information from across the Internet. Our conferences give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Practical technical advice and expert insights are distributed via more than 100 specialized e-mail newsletters and our Webcasts allow IT pros to ask questions of technical experts in real time.

What makes us unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of conferences, the expert interaction of Webcasts and Web radio, the laser-targeting of e-mail newsletters and the richness and depth of our print media to create compelling and actionable information for enterprise IT. For more information, visit www.techtarget.com.