Securing Teleworker Networks

Lisa Phifer

More remote work plus more Internet attacks make for a very dangerous combination

Twenty-seven percent of the U.S. workforce telecommutes at least one day per week. Millions of others are day-extenders, working from home at night and on weekends. This teleworker access to company intranets and business applications increases productivity—and security risk.

Teleworkers push the enterprise security perimeter well beyond the corporate firewall. Always-on residential broadband and wireless services expose home networks to near-continuous probing. Once discovered, unprotected home networks make for easy attack targets. Work-at-home PCs that are compromised can expose confidential data and create back doors. Without appropriate safeguards, mass mailing worms like SoBig and remote access trojans like SubSeven can ride remote access connections right into the company intranet.

For all but the most security-sensitive facilities, cutting off teleworker access is simply unthinkable. Instead, most IT departments try to beef up teleworker security with VPN and antivirus software. But as teleworker nodes morph into teleworker networks, should your security strategy change? Could you be doing more—or spending less—to eliminate these weak links in your corporate network's protective armor?

To answer these questions, let's consider the threats associated with teleworker home networks, the security measures available to address them and the business consequences of failing to do so.

The Rise Of Teleworking

Those who work from home reap many benefits, including the ability to live in remote locales, avoid lengthy commutes and conveniently interleave work and personal commitments. According to an annual survey by the International Telework Association and Council, two-thirds of teleworkers experience greater job satisfaction, and 80 percent feel that teleworking increases their job commitment.

There are tangible benefits for employers as well. According to "Economics of Teleworking" by Noel Hodson, the average worker spends the equivalent of 30 working days per year commuting, traveling or engaging in office chit-chat. Converting even half of this down time into productive time is a clear win for employers. For example, teleworking saves AT&T an estimated $65 million in productivity gains, $10 million in staff retention and $25 million in reduced real estate costs each year. IBM believes that teleworking boosts employee productivity about 20 percent, and eliminating office space for 10,000 teleworkers saves the company $75 million a year.

For the past decade, many government agencies have promoted telecommuting as a method of improving air quality by reducing auto exhaust. For example, in response to the Clean Air Act, Congress established a telecommuting center in Washington, DC. By law, all federal employees in the DC area must be given the option to telecommute by 2006. Legislation like this all over the world has added fuel (so to speak) to the growing teleworker movement.

Even so, teleworking might have remained a promising but largely unrealized vision were it not for the emergence of affordable high-speed Internet access. Early teleworkers were hampered by lengthy file downloads, expensive metered ISDN services and tied-up phone lines that rendered the worker unreachable during the business day. More recently, residential broadband services like DSL, cable modem and satellite Internet have fundamentally altered the teleworker experience.

According to the Pew Internet and America Life Project, as of March 2003, nearly one in three homes had high-speed Internet access—that's approximately 30 million residential broadband subscribers. Although speeds vary, broadband downloads are typically 5 to 20 times faster than dialup. As a result, those working from home today usually have ready access to email, file sharing, videoconferencing and other applications required to conduct business effectively from afar.

Lisa Phifer is vice president of Core Competence, Inc., a network security consulting firm based in Chester Springs, PA.

The Impact On Network Security

There are clear quality-of-life and financial benefits for teleworkers and their employers, but there also are drawbacks. Topping that list: Loss of corporate control over IT resources and associated impact on enterprise network security.

In the mid-'90s, teleworkers used company-issued laptops to direct-dial into remote access servers operated by employers. Companies controlled both endpoints and trusted the private telephone call connecting them. In the late '90s, virtual private networking emerged to leverage the public Internet for remote access. Companies began to install VPN software on company laptops, protecting traffic over untrusted public links. In short, organizations expanded their networks' security perimeter to incorporate teleworker remote laptops. This strategy is sound when the VPN client, gateway and tunnel can be trusted.

However, new technologies and economic pressures are changing those assumptions. To cut costs, companies are dropping laptop leases and encouraging teleworkers to use personal home PCs instead. IT departments have tired of installing software on computers that employees take home and then promptly corrupt or break. Administering company-issued laptops was expensive but do-able; exerting IT control over personal PCs is proving less tractable. The result: That remote node at the far end of the VPN tunnel is becoming harder and harder to trust.

Moreover, that node is increasingly likely to be a remote network, or at least a member of a remote network. Today's high-speed broadband links are often terminated by residential gateways—entry-level access routers that employ network address translation (NAT) for Internet connection sharing. Teleworkers share the ample capacity of their broadband link with spouses, siblings and roommates. Once interconnected, these home networks typically use Windows workgroups to share resources like printers and (sometimes unintentionally) files.

The cocoon of trust surrounding teleworker PCs was already unraveling when 802.11 wireless LANs hit the scene last year. Whether they embrace 802.11 or not, most organizations that support teleworking do have wireless LANs to worry about—specifically, the sub-$100 wireless routers used in home networks. Printer sharing with close family members is low-risk compared to improperly-secured wireless LANs that share resources with everyone located within several hundred feet. 802.11 can be used safely, but "war drives" across the globe have repeatedly found that at least 2 in 3 wireless LANs operate without airlink security (see *BCR*, September 2002, pp. 26–32).

Understanding The Risks

Without corporate oversight and IT assistance, few users recognize these security risks, much less take appropriate steps to lock down their home networks. Companies can make considerable headway simply by educating teleworkers about these security risks:

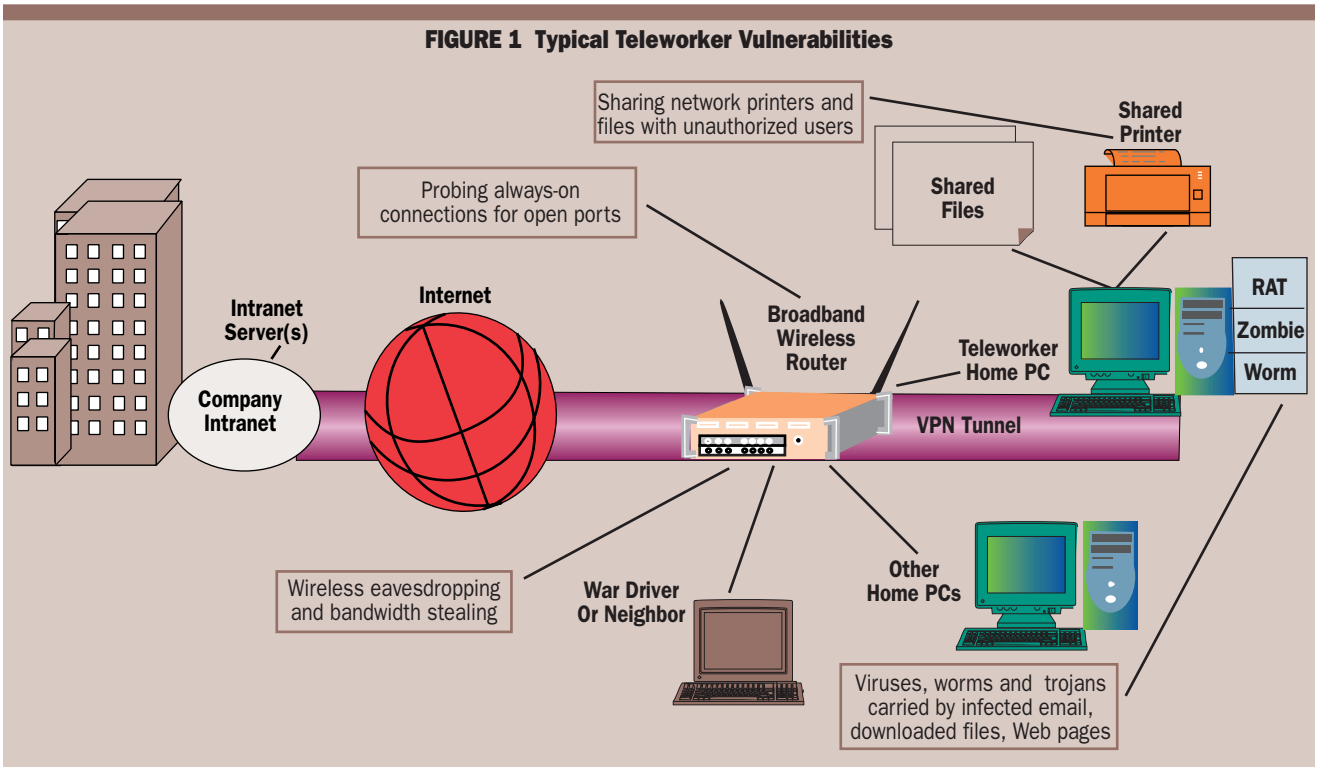
- **Always-On Broadband:** High-speed connections are convenient for both users and attackers. Increasing time spent on-line not only widens the window of opportunity, but makes it easier to repeatedly probe the same target.

  Only inexperienced ankle biters launch obvious sequential port scans. Those with more serious intentions scan particularly vulnerable ports in random order over long periods of time, making detection less likely. Ports often probed include 25 (smtp), 80 (http), 135 (DCOM RPC, exploited recently by Blaster), 137 (netbios), 445 (ssl) and 1434 (SQL, exploited recently by Slammer). Any open port can potentially be used to inject inbound traffic, infecting or exploiting host(s) using the broadband connection. Teleworkers should be encouraged to close all unused ports and make broadband gateways as invisible as possible.
- **Wireless LANs:** Most 802.11 products ship with built-in airlink security measures that are disabled by default. This makes installing a wireless router easy—in fact, too easy. Unless someone configures authentication and encryption keys into the router and all wireless devices, anyone can eavesdrop on data sent over the wireless connection. To make matters worse, anyone can send data to or through the wireless router, stealing bandwidth, launching spam or using the link to attack others. Teleworkers should be taught to enable basic airlink security measures, although (as we shall explain) more is required to firmly close this security loophole.
- **Network Resource Sharing:** Cable networks and wireless LANs are point-to-multipoint in nature. This means that teleworkers may be sharing printers and files not only with their families, but with their neighbors and opportunistic "war drivers" parked outside.

  Sharing is embedded in every Windows PC, enabled with just one click. Although passwords can be required, many users skip this, leaving shares open to anyone who finds them. Finding them is not hard—that's where port 137 comes into play. Attackers probe this port to gain information about the PC itself, its operating systems, shared resources, user names and domain names. Such information can be used to download confidential files, overwrite system files or infect the target with malicious code. Teleworkers should be counseled to block NetBIOS traffic on broadband and wireless links, and to avoid sharing resources on PCs that house company data.
- **Virus Infection:** Most of us are well aware of computer viruses, but awareness does not seem to be stemming the tide of viruses choking mail servers and Internet links. For example, TrendMicro estimates that SoBig.F infected nearly 770,000 computers worldwide in the week

With broadband, "always on" means always exposed

FIGURE 1 Typical Teleworker Vulnerabilities



following its August 18 posting to UseNet as a pornographic picture.

Analysis suggests that anti-virus measures were relatively effective at stopping SoBig.F from spreading inside corporate networks—most of the infected PCs propagating SoBig.F were home PCs. PCs outside company networks are less likely to run current anti-virus software and more likely to continue operating without detection once infected. Because SoBig.F harvests email addresses from victims to use as forged source addresses, many companies subsequently received hundreds of "delivery failure" messages carrying copies of the virus, adding insult to injury. Incidents like these show there is still room for improvement in teleworker virus protection.

■ **Trojan Horses:** Worms cause server downtime due to traffic spikes and clean-up, but trojan horses can have more far-reaching impact. A trojan horse is malicious code presented as something benign—for example, included in shareware or embedded in JPEG or MP3 files. Remote access trojans like SubSeven and BackOrifice let attackers control PCs remotely. When a compromised PC launches a VPN tunnel, attackers can use the tunnel to access to servers inside the company intranet.

Zombies are trojans that wait quietly until a predefined moment to follow instructions—for example, perpetrating large-scale distributed denial of service (DDoS) floods like the February 2000 attack that cost CNN, eBay, and Yahoo! over $1 billon dollars. Teleworker nodes must be protected against trojan horses to avoid both intranet compromise and corporate liability.

Figure 1 illustrates a typical teleworker home network, highlighting the common intrusion vectors discussed above. Note that these vulnerabilities exist even though the teleworker is using a VPN tunnel to connect to the company intranet.

Defending Teleworker Networks

User education is an essential ingredient, but don't stop there. Review security threats and at-risk resources, then revisit your teleworker security policies to determine whether any updates are appropriate. It may be necessary to augment existing policies to incorporate countermeasures for new threats, like best practices for wireless router configuration. It also may be time to incorporate recent advances in distributed security management, like tight coupling between VPN clients and other desktop security software. Here are some of the countermeasures that may prove helpful.

■ **Wireless-aware SOHO Firewalls and Routers:** Wireless access points (APs) relay frames between 802.11 wireless and Ethernet wired LAN segments. Wireless routers usually combine AP, packet-filtering, NAT and WAN access router functionality in one box. Most teleworkers choose wireless routers, over APs, because they offer Internet connection sharing and rudimentary protection against Internet probes.

Many teleworkers should consider using SOHO firewalls that can be combined with wireless using external or integrated APs. Some basic comparisons between entry-level routers and SOHO firewalls:

■ Entry-level routers provide stateless packet filtering; small/home-office routers offer stateful

packet and sometimes also application content inspection.

- Entry-level routers depend on outbound NAT and private addressing to deflect inbound traffic; SOHO firewalls enforce granular policies that expressly block unauthorized traffic moving in both directions.
- Entry-level routers usually lack remote logging or management features; SOHO firewalls are designed to be remotely administered over secure channels, preventing misconfiguration by end users.
- Entry-level routers may let VPN tunnels pass through untouched; SOHO firewalls can combine VPN and firewall policies to mandate security in accordance with business needs—for example, requiring VPN on wireless traffic forwarded to your company network.

There are many SOHO firewalls on the market today. Some companies purchase both SOHO and central site VPN/firewalls from a single vendor to simplify administration. Vendors like Netgear and D-Link sell entry-level wireless routers *and* upscale versions with stateful packet inspection and VPN support. Firewall vendors like WatchGuard and SonicWALL now sell SOHO security appliances with embedded wireless access points. Advanced security and remote administration capabilities make these products a bit more expensive than entry-level routers, but the investment can be well worth it.

- **Airlink Security:** Whether standalone, combined with a router, or embedded in a SOHO firewall, every 802.11 AP includes basic airlink security features: a Service Set Identifier (SSID) that names the wireless LAN, a shared key used for group-level authentication and Wired Equivalent Privacy (WEP) for link encryption.

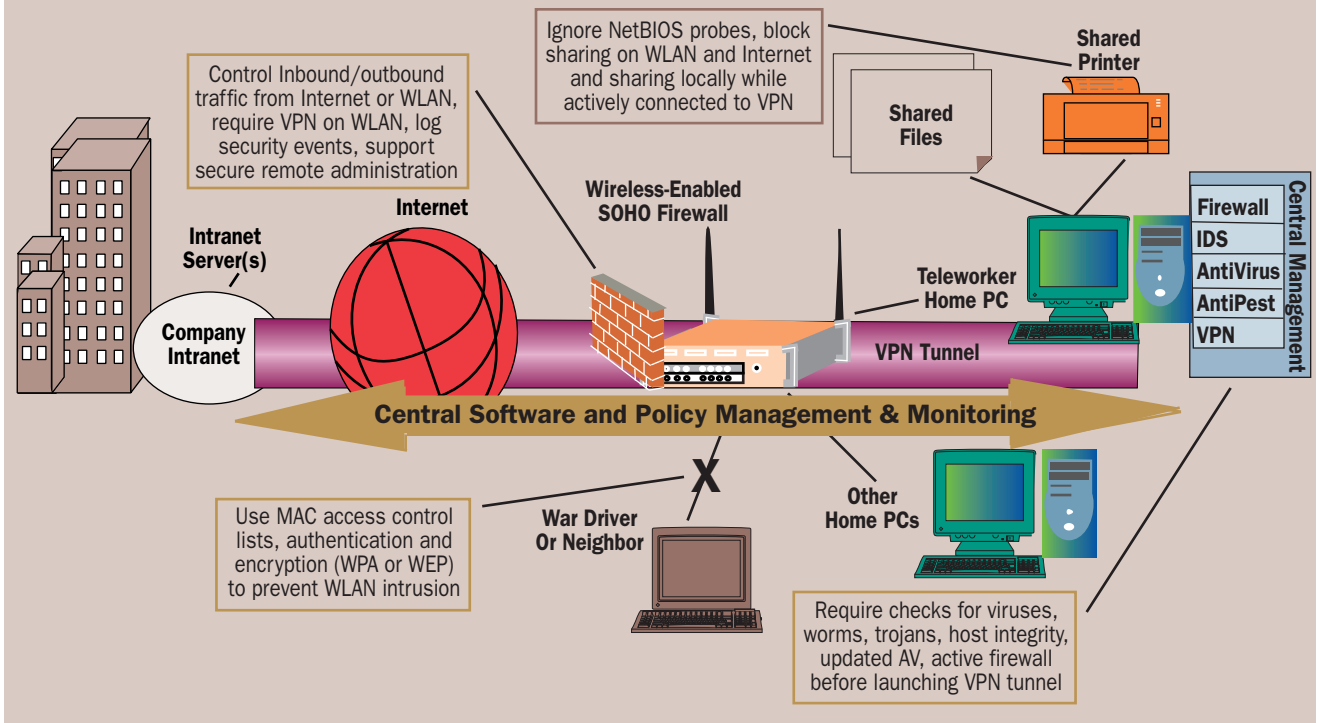
At minimum, APs should be configured with unique SSIDs that disclose nothing about the teleworker's name or location, and with random shared keys for authentication and encryption. When possible, configure access control lists to block LAN access by unrecognized stations. These steps are relatively simple and will deflect casual war driving and bandwidth theft.

Unfortunately, the MAC addresses used to identify stations can be forged, and WEP keys can be broken with shareware tools like Kismet and WEPcrack. To address these vulnerabilities, many vendors are now releasing Wi-Fi Protected Access (WPA) upgrades. WPA uses key mixing, sequencing and a message integrity check to virtually eliminate key cracking and data frame forgery.

In enterprise LANs, WPA can be combined with 802.1X port access control for more robust user-level authentication. However, 802.1X is often impractical for teleworker LANs because it requires AP access to a RADIUS server. Instead, WPA can also be configured with a secret passphrase that is more secure than the old shared key method, but does require everyone to know the same passphrase. Teleworkers should be encouraged to upgrade to WPA when available and pick long, random passphrases. (For more on WPA, see *BCR*, May 2003, pp. 42–46.)

Airlink security has improved, and is essential

FIGURE 2 Teleworker Configuration With Added Security



Many wonder why teleworkers should bother with airlink security when using VPN tunneling. The answer is simple: airlink security prevents unauthorized use or abuse of the wireless LAN itself and attached network resources. Enabling WPA prevents war drivers from using company-paid broadband links to send spam or attack others. WPA also safeguards personal traffic on the teleworker's LAN—in particular, any local LAN traffic that might "leak" outside the VPN tunnel, like sending jobs to a shared printer.

■ **Desktop Security Software:** Many companies already recommend or supply desktop security software for use on teleworker PCs. Over the past few years, many such products have been extended to provide stronger central control and monitoring. For example:

• Anti-virus scanners from companies like McAfee, Symantec and TrendMicro are now available in enterprise editions that permit central control over updates and scan actions. These can be complemented by products like PestPatrol, from the company of the same name, that detect remote access trojans, zombies, spyware and other non-viral malware. Some wireless routers and SOHO firewalls can also provide network-based anti-virus, delivering a one-two punch to knock out viruses at the desktop and gateway.

Centralized management is desirable—but difficult

• Enterprise-grade desktop firewall suites like InfoExpress CyberArmor, Sygate Secure Enterprise and ZoneLabs Integrity now provide remote installation, firewall policy configuration and event monitoring on teleworker PCs. Some incorporate intrusion prevention features that attempt to stop both network-borne and system-level attacks.

These products have come a long way since standalone personal firewalls emerged, making desktop firewalling less visible to users and more tightly controlled by employers. One common problem with personal firewalls is that users simply turn them off when problems are encountered. Centrally-controlled desktop firewalls can prevent this from happening and help IT staff diagnose and remedy such problems.

■ **VPN Clients:** As previously mentioned, companies that support teleworkers typically employ VPN clients to authenticate users at the VPN gateway and safeguard traffic in transit over the public Internet.

Many companies use VPN client software sold by their gateway vendor—for example, vendor-specific clients supplied by CheckPoint, Cisco and Nortel. These clients are tightly coupled with gateways to add functionality like user-level authentication, virtual IP address assignment, NAT traversal and remote policy administration/update/audit. NAT traversal is particularly important to teleworkers who must pass tunneled traffic through a broadband/wireless router or SOHO firewall. For best results, look for both VPN pass-through in the router/firewall and NAT traversal in the VPN gateway/client.

Several VPN clients are now integrated with other desktop security products, letting IT staff dictate security policies that combine VPN, firewall, anti-virus, IDS and pest control measures. For example, Check Point's VPN-1 SecureClient can be configured to invoke PestPatrol during VPN tunnel set-up, permitting company intranet access only if no trojans, zombies or other malware are detected. Similar scenarios can be constructed to require desktop integrity scans, current AV signatures and active firewall/IDS software. Companies may not own the teleworker's PC 24/7, but policies like these can enforce security checks before treating the node as a trusted member of the VPN.

Central management and monitoring can help, but administering VPN client software is an IT pain point. Some companies are now trying to avoid adding VPN client software by adopting "clientless" solutions. Examples include using SSL-protected Web portals, SSL VPN gateways from vendors like Neoteris, V-ONE and Whale, or managed remote access services from providers like GoToMyPC and Aventail. (For more on SSL VPNs, see *BCR*, April 2003, pp. 47–54).

This raises an interesting question: if remote nodes are difficult to control and trust, can narrowing access to just one or two applications reduce both cost and risk? Avoiding software installation is necessary on public and business partners' PCs where companies have no oversight. Teleworker PCs are more of a grey area. Every company must consider deployed measures, specific alternatives, business needs and security objectives to strike a balance between cost and effectiveness.

Figure 2 depicts the same teleworker home network shown in Figure 1, after adding new security measures that:

1.) Block unwanted inbound and outbound traffic from the Internet and WLAN.

2.) Authenticate, encrypt and protect wireless LAN (WLAN) traffic.

3) Enforce desktop intrusion detection (IDS), anti-virus and pest scanning.

4) Stop unwanted traffic like accidental NetBIOS sharing.

5) Verify desktop security before letting VPN tunnels connect to the company intranet.

Let Policy Be Your Guide

Whether your company simply provides best practice guidelines, recommends products, purchases products for teleworkers or actively installs and manages them, technologies like these can help you adapt your existing defenses to address new teleworker threats.

But don't deploy teleworker network security technologies simply because they exist. Choose solutions that expressly support your company's security policy and are cost-justified. Your objective should never be to completely eliminate risk—an impossible task—but rather to reduce risk to acceptable levels.

Finally, be sure to define an Acceptable Use Policy (AUP) that clearly spells out authorized use, required security measures and known risks. Can teleworkers connect company laptops to wireless LANs? Can personal PCs employed for business use shared printers on a teleworker LAN? Make sure your AUP addresses questions like these. Educating IT staff and end users about risks and how to manage them will play an important part in any successful teleworking program□

Companies Mentioned In This Article

Aventail (www.aventail.com)
CheckPoint (www.checkpoint.com)
Cisco (www.cisco.com)
CNN (www.cnn.com)
D-Link (www.dlink.com)
eBay (www.ebay.com)
GoToMyPC (www.gotomypc.com)
IBM (www.ibm.com)
InfoExpress (www.infoexpress.com)
McAfee (www.mcafee.com)
Neoteris (www.neoteris.com)
Netgear (www.netgear.com)
Nortel (www.nortelnetworks.com)
PestPatrol (www.pestpatrol.com)
SonicWALL (www.sonicwall.com)
Sygate (www.sygate.com)
Symantec (www.Symantec.com)
TrendMicro (www.trendmicro.com)
V-ONE (www.v-one.com)
WatchGuard (www.watchguard.com)
Whale (www.whalecommunications.com)
Yahoo! (www.yahoo.com)
ZoneLabs (www.zonelabs.com)

You can't eliminate risk, but you can rein it in