Dorothy Lunn, an Information Security Officer with the Federal Government, contributed the following comment:

"At the strong suggestion of a security class instructor, I downloaded and installed a personal firewall on my home PC. It didn't take long to see why my PC needed a firewall. Aside from numerous pings there have been attempts to access my PC and to download packets to it. I realize now that home PCs are a huge resource for hackers and cyber terrorists. As a result of my experience, I believe that IT professionals have a responsibility to protect their home PCs with a personal firewall in addition to antivirus software. I asked several attendees at a conference recently whether they had a firewall on their home PC. Not a single person answered affirmatively. I downloaded the personal firewall from ZoneAlarm at <http://www.zonelabs.com/> since it is free for personal and non-profit use."

* * *

Why should corporate network managers care about personal firewalls? Because the corporate network is, amoeba-like, spreading extensions out of the office that make corporate data vulnerable to hacker attacks. Portable and home computers can be linked easily using synchronizing software such as the Microsoft Windows "Briefcase" feature and the well-known Laplink products <http://www.laplink.com/>. Many workers bring files home and work on company projects outside normal working hours; many of us even telecommute, doing significant amounts of work outside the corporate milieu. We are exposing corporate data via Internet connections without the protection of the corporate firewalls.

The second problem we're facing is persistent Internet connections. Cable modems, satellite systems — employees are exposing unprotected corporate data to the 'Net for much longer times than when dialup modems were the norm. Even with dialup lines, one can see frequent port scans and unauthorized attempts to connect to various ports from (largely) automated scanners; however, persistent connections make the problem much worse. Personally,

Third, there are automated programs in use by criminal hackers that are designed to find unprotected systems and infiltrate them for nefarious purposes such as distributed denial-of-service attacks.

When employees expose their corporate laptops or their home computers with corporate data to the Internet, they put those data at risk. When compromised portable computers are brought back into the workplace and connected to internal networks, their burden of malicious software effectively gets through the corporate firewall and puts all corporate systems at risk.

The combination of these factors makes home and portable computers a significant element for corporate security. I fully concur with Ms Lunn in urging all network managers to ensure that every workstation computer that carries corporate data should be protected by a personal
firewall.

* * *

In the next article in this series, I will look at Steve Gibson’s testing tools for personal firewalls.

* * *

Mich Kabay can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from the Information Security University project, see <http://infosecu.com>.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.