AN MIT ENTERPRISE
TECHNOLOGY REVIEW
Emerging Technologies and Their Impact

Home
Topic Browse
Focus On
Current Issue
Archives
Opinions/Forums
Free Newsletters
TR100/Events
NEW! MIT Insider
Reports
Special Editions
Books
Logout
My Account
Subscribe
Renew
Customer Service

premium content
Jump
Search

Illustration by Matthew Bouchard

TR Related Articles
- The Palladium Paradox
- Digital Pirates Beware
- PIN on the Go
- Fewer Bits, Better Code

Firewall Follies

The Net Effect By Simson Garfinkel
September 2002

The complacency firewalls breed is ultimately more damaging than the computer pirates they keep out.

Do you use the Internet at work? I see lots of hands. You may not realize it, but your access to the Net is most likely mediated by some kind of firewall. Companies are spending thousands, even hundreds of thousands, of dollars on these systems—and trust them to protect their networks from snoopers and intruders. That's a problem, because firewalls often provide a mere illusion of protection. They don't make business systems significantly more secure. And by focusing attention on defending the perimeter, rather than on defending information assets within an organization, firewalls foster lax internal security practices that magnify the damage that insiders can inflict.

What firewalls do accomplish, however, is this: they make the Internet more cumbersome to use. I recently visited a friend's firm in New York and wanted to check my e-mail, so I plugged my laptop into a network jack in an unused office. Access denied: my PC wasn't set up to work with the company's firewall. So instead of reading my e-mail, I occupied myself by sniffing the traffic on the office network and probing for a way out. (Had I been inclined, I could have read everybody else's e-mail—or done real damage.)

Firewalls are simple in concept. A typical firewall consists of a special-purpose computer that has two network plugs. One plug goes to the Internet; the other connects to a company's office network. The firewall is programmed with rules that determine what traffic is allowed to pass and what is to be blocked. For example, a firewall might be set up to allow managers in human resources to browse the Internet, or to access their desktop PCs from home, while permitting people in the corporate call center only to access their e-mail. The better firewalls log everything that moves across the boundary, giving companies a powerful tool for auditing online activity.

The great appeal of firewalls is that they are supposed to ease the job of corporate security. Instead of feverishly downloading and installing security patches to protect thousands of desktop computers and servers running a menagerie of operating systems, many organizations find it easier to simply trust the firewall to keep the bad guys out. The problem with this approach: bad guys are everywhere. Sure, some are on the outside of the company's network. But there are corrupt employees on the inside, too. And even well-meaning workers can have laptops that contract viruses during business trips—viruses that then infect the office network. This is why so many companies supposedly fortified with firewalls succumbed to attacks from computer viruses and worms like Nimda and Code Red.

The existence of firewalls has also allowed companies to neglect their internal security measures and to accept lower-quality software from their vendors. Instead of hardening their systems, many vendors now advise their customers to install their equipment "behind the firewall." This has long been standard practice for software suppliers delivering systems based on Microsoft Windows. Now it is becoming common for network-based management systems that are showing up in things like photocopiers, HVAC equipment and even elevators.

Organizations that rely on their firewalls build networks with hard, crunchy outsides but soft, creamy insides. Even worse, an elaborate, expensive firewall diverts dollars and attention from other measures that truly can improve security: good backups, pervasive encryption and employee background checks, for example. My friend's company should have turned off the Ethernet jack in that unused office—or I should have triggered an alarm when I tried to use it.

Firewalls also become less secure over time, a phenomenon observed by computer consultant Dan Farmer. Here's what typically happens: Somebody inside an organization needs to send some sort of information through the firewall—perhaps because the company is involved in a joint project with another firm. To allow this transfer, a supposedly temporary hole is opened in the firewall. But that hole invariably remains in place long after it is no longer needed. After a few years, the typical firewall comes to resemble Swiss cheese.

Confusingly, there is one kind of firewall that actually can dramatically improve security. These so-called host-based firewalls are a second layer of security that mediates all communications between your desktop computer and the rest of the network. A good host-based firewall will warn you, for example, that the program you just downloaded is trying to open a connection to a pirate Web server in Russia; you can then choose to either allow the connection to go through or terminate it. Both Microsoft and Apple have primitive host-based firewalls built into the current generations of their consumer operating systems.

I'm certainly not advocating that businesses do away with their firewalls; many Microsoft operating systems are so vulnerable that there is no other practical way to protect them. But we need to build a new security paradigm. The core principle should be an assumption that every network is already compromised; systems should be designed accordingly. In practical terms, this means encrypting all information that passes over the network and equipping every computer with its own host-based firewall. This kind of belts-and-suspenders redundancy is not particularly elegant, but then again, neither is an armored car.

>> Join a discussion about this story.

Simson Garfinkel writes on information technology and its impact. He is the author of *Database Nation* (O'Reilly, 2000).

Print Version Email to Friend Write Us Add your thoughts PDF Version Order Reprints

About Us | Contact Us | Privacy | Terms of Use | Advertise | Subscribe |

Is this where computing's next
breakthrough will come from?