ump _____

Т

D

S

Re Te

ju

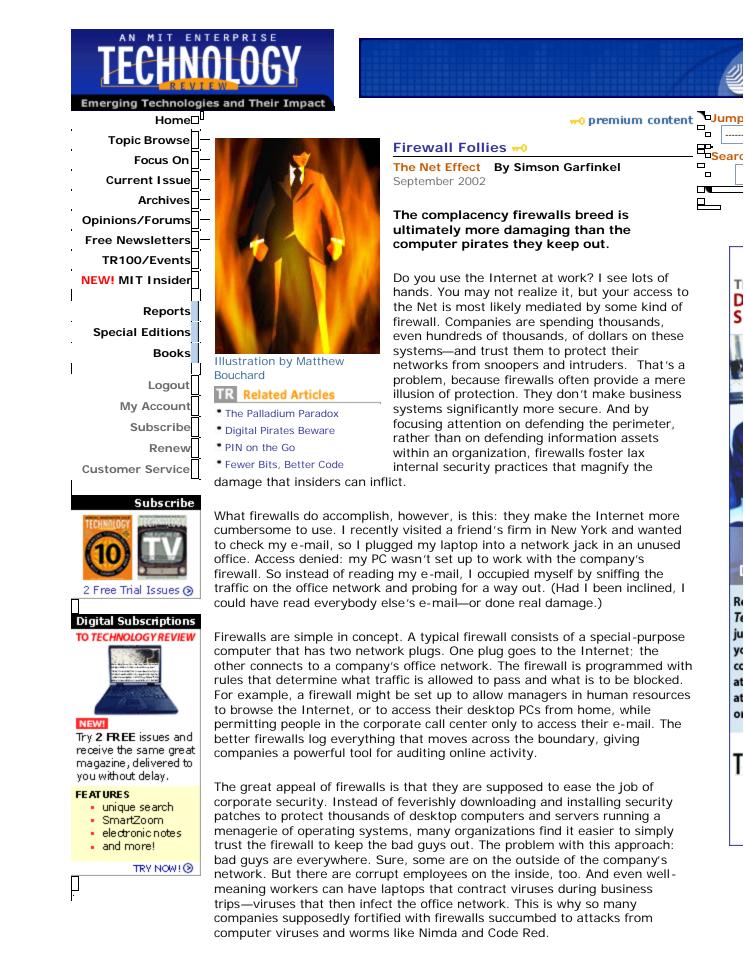
y¢

cc

at

at

OI





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-andsuspenders 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).



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

