SECURITY HOLES

Technology advances and more efficient partner networks have inadvertently generated major security holes. Here's a look into how to protect the network.

Daniel Katz-Braunscheig is what has come to be known as a "White Hat," a skilled hacker who companies pay to try and break into their systems and report back. And his favorite way to get into an enterprise network these days is the networked fax or printer.

"I don't think it's understood at all that these boxes have an embedded version of an operating system. It's a little workstation, a little server," Katz-Braunscheig says, adding that these rarely safeguarded peripherals are a wonderful way to break into a network.

But the biggest security threats have almost always been those that are not seen. They are either not known to most IT security managers or are known but ignored. In almost every instance, threats are the unintended result of improving business operations. Extranets and supply chains, for instance, help businesses, but open doors to strangers. PDAs, laptops and high-end cell phones boost employee productivity, but they also compromise companies by allowing data to be removed from the security of the corporate environment.

Often, it's the innocuous new feature or capability that inadvertently opens up the biggest security hole. With increases in both capabilities and intelligence, peripherals can now remember data and give full network access to anyone. But they remain relatively unprotected. And while it's well known that the convenience of a wireless network makes data available to data fiends who want to scan the airwaves, all devices are still connected to the network. Who would suspect the mild-mannered copy machine, scanner, fax or printer as a threat?

Toiling at home is a convenience to the worker and a benefit to the company. But is the lax security of a home network compromising data? Could it allow a Trojan horse to get inside an employee's laptop, waiting patiently for the next connection to the corporate LAN when its nefarious mission can begin?

For that matter, how safe is a hotel's high-speed connection or one at an airport, train station or client's office? Are you sharing more than you intend to when you try to download e-mail at a Starbucks? And how secure is the data on your PDA and your cell phone?

"What we have here is the vanishing perimeter," says Jason Wright, a security industry analyst for Frost & Sullivan. "Companies today have so many types of people coming in from so many different entry ways. Controlling what is done inside the network is becoming an exponentially more difficult task."

The Trusted Community

The increasing popularity of the extranet is a major point of vulnerability. Traditionally, IT managers assign a top priority to keeping intruders off the network and spend much less time and money making sure that their authorized users don't exceed their network privileges. In other words, they make sure the front door is locked with a top-notch deadbolt and hope that family members and overnight guests don't rob them.

It's an illogical position, given the well-known fact that the vast majority of information thefts and sabotage are masterminded and/or executed by insiders. But it's always easier to scare management with threats of terrorists, ill-intentioned hackers and corporate spies than it is to tell them they can't trust their own people.

The popularity of extranets is making the "just secure the front door" approach (typically firewalls and VPNs) even less logical. Not only does the list of people who have some authorized access to a company's network include that company's employees and contractors, but it also includes the employees and contractors of distributors, suppliers and major customers. And depending on the company's e-commerce approach, that list may even include not-so-major customers.

Lots of Trust

For a large company, the number of people who have at least some authorized access can easily exceed one million. That's a pretty big trusted community.

And that large a community can cause problems. Today's technology is allowing much greater and deeper access. To the extent that access improves efficiencies and time-to-market, it's a very good situation. But those improvements are leveraging the ability of your partners to be able to do more. And that's widening the security hole.

This blurring of the distinctions between groups of people considered safe and unsafe is a major crack in the proverbial armor of a typical corporate security strategy. Corporate security managers today "still live by the pyramid security model, which holds that most of the security can be handled by putting a thick border between the inside and the outside of their company," says Sachar Paul, chief security officer for SAP.

But with managers and employees alike enjoying mobile/pervasive computing, such distinctions are becoming pointless. Whether it's accessing e-mail while on an overseas trip, using a RIM BlackBerry cell phone/PDA hybrid, enhancing a company's supply chain or using radio frequency identification (RFID) or even a camera-equipped cell phone, "there is no longer a clear separation as to whether people should be considered inside or outside. The model of perimeter security is not appropriate anymore," he says.

How Secure
Do You Need To Be?

Standard Level

Who should use it?
- Human Resources
- General Office

Benefits
- Confirm user access
- Protect user output

Application
- Secure the user (user authentication, account codes)
- Secure the output (confidential/PIN printing)

Heightened Level

(Includes Standard Level)

Who should use it?
- IT Departments
- Accounting
- Financial
- Insurance
- Healthcare

Benefits
- Eliminate the latent document image
- Safeguard user access

Application
- Secure the image data (data security kit)
- Secure the network access (IP/MAC filtering)

Optimum Level

(Includes Heightened Level)

Who should use it?
- Federal Agencies
- Military
- Research & Development
- Legal

Benefits
- Audit user activity
- Protection of documents even after distribution

Application
- Secure the audit trail
- Secure the document rights

Source: Sharp Electronics

Paul argues that security must move to a permissions/privileges approach, where both inside and outside people are considered threats, and they are granted the least-level permission possible to do their jobs. This is the need-to-know approach.

Internal Controls

Beyond being potential security threats, employees also are a company's first line of defense. If they are reckless with their passwords or do not take reasonable steps to preserve both their data and their access to the network, it can undermine the most elaborate security defenses.

"You have got to look at internal controls," says Trevor Healy, vice president, Payment Services for VeriSign. "You can build as much external protection (firewall and VPN) as you wish, encrypt data, etc., but if your employees do not take basic measures, it won't help."

Healy says Sarbanes-Oxley reviews allow companies to audit systems and clean up network access, such as former employees and those employees who have excessive, unnecessary access.

"In many cases, companies are not keeping internal controls implemented," he says. "We must educate the user inside the company." Healy gave as an example companies that offer internal Wi-Fi access too easily and frequently.

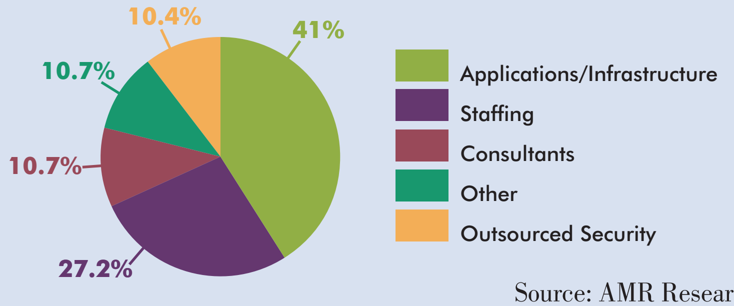
Matt Dircks, vice president of security products for NetIQ, says companies drop their guard when users are inside the network, which he says is a terrible mistake. "I call it the egg roll security approach: It's hard on the outside and soft on the inside," he says, pointing to lenient systems about permission/privilege levels and the failure to deactivate outdated accounts.

Of all the security risks, probably the most powerful and least recognized threats come from seemingly mild-mannered devices that have been around networks for years: printers, fax machines, scanners and copiers.

The problem is these devices quietly have become much more sophisticated in recent years. Copy machines can now remember hundreds of documents for an extended period, which puts the information-confidentiality threat much higher than remembering to remove the original. The copier will remember your original long after you've left and will share it with anyone it thinks is authorized. Depending on settings and equipment, these machines are not always that picky about choosing those they consider authorized.

What Are The Biggest IT Security Hurdles?

Here is how IT managers rank the top IT security challenges.



Source: AMR Research

Security resources

AMR Research
http://www.amrresearch.com

SAP AG
http://www.sap.com

VeriSign Inc.
http://www.verisign.com

Indeed, those networked peripherals pose a much greater threat than divulging to strangers what you've been scanning. Given that they are not typically seen as a threat, these devices rarely are protected. And yet they now have full network access and the brains—CPU and RAM—to use it.

"Every printer today has a CPU and it is as vulnerable as any other computer on the network. But people aren't even considering the print controller a problem," says Edward McLaughlin, president of Sharp Document Solutions.

VeriSign's Healy says he is concerned about peripherals with network access providing easy access to intruders, but stressed that a properly configured and managed network can indeed protect itself. "If network security settings are set up correctly, that unauthorized printer access attempt should set off an alarm. The question is whether someone is actively watching."

Changing Security Implications

Lance Travis, a vice president of security research at analyst firm AMR Research, says his favorite overlooked security risk happens after a major supply-chain system enhancement. Supply-chain networks that connect a company's manufacturing control system to a data network "make good business sense," he says, "but you're sharply increasing the probability that someone will be able to get into your plant-floor network."

The tendency to make accessible to outsiders systems that were never intended to be accessible to outsiders is the problem. Travis has some favorite—and frightening—examples: In 2003, the Slammer worm infected a telecommunications provider's network, which prevented communications to and from a utility's substation Supervisory Control and Data Acquisition (SCADA) control system. This in turn rendered the substation inoperable for about six hours.

The Nuclear Regulatory Commission confirmed that in January 2003 the MicrosoftSQL Server (Slammer) worm infected a private computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again.

Travis also cites a hacker in Australia who used a radio transmitter to hack into the controls of a sewage treatment system and release about 264,000 gallons of raw sewage into nearby rivers and parks.

"The implication of the security attack changes radically," he says. "If someone gets in and steals financial data, that's bad. If someone gets in and starts opening and shutting valves, it could be catastrophic." ■

For more information on
Special Advertising Section
opportunities, please contact
Stacy Sass McAnulty at 212-512-6296 or
stacy_sass-mcanulty@businessweek.com
Please visit
www.businessweek.com/adsections

Triangle Publishing
Services Co. Inc.
The Best Strategic Content for Web, Print, Multimedia and Beyond
www.triangle-publishing.com ■ 617-244-0698

Special Advertising Section Writer: Evan Schuman