

## FOCUS

- ▶ **CUs are** three to four times more likely than banks to be compromised by hackers because CUs are smaller and have fewer resources, less technical savvy and support, and less awareness of server vulnerabilities.
- ▶ **The most dangerous** hackers may be internal: employees who know the system so well that their intrusions and thefts are virtually undetectable.
- ▶ **Because new methods** of attack constantly turn up, CUs must apply appropriate software patches immediately.



# Keep Hackers At Bay

PATRICK TOTTY

**Intrusion  
detection systems  
reveal server  
vulnerabilities.**

When credit unions tell Kevin Prince they've never been hacked, so there's no need to bother with intrusion detection systems, his answer usually stops them in their tracks: "How do you know you haven't been hacked? You have no systems for detecting intrusions, so how would you know?"

Prince is senior product manager at Mounds View, Minn.-based Cavion Plus, the new name of recently merged Internet technology providers Liberty Internet Services and CUNA Network Services. "Intrusion is a misunderstood

topic for the most part, although there's been a dramatic increase in understanding its seriousness. Credit unions are three to four times more likely to be compromised than banks because credit unions are smaller and have fewer resources, less technical savvy and support, and less awareness of the problem."

Credit unions' biggest misperception about intrusion detection systems is that firewalls alone provide sufficient protection. "But once you open a hole through the wall—with electronic banking or e-mail—a firewall can't protect you," says Prince. "A majority of the scripts hackers use go through Web and e-mail ports."

(continued)

© 2005 Credit Union National Association. Reprinted with permission.

## ► KEEP SYSTEMS SAFE WITH SOFTWARE UPDATES

As vendors such as Microsoft discover security flaws in their operating systems and software, they make available “patches” to fix these problems. But patches work only if your credit union knows about and loads them in a timely manner on its systems—from internal networks to Web-based automated teller machines (ATMs).

Not doing so can have serious consequences. Just ask Bank of America Corp., Charlotte, N.C. During last year’s Super Bowl weekend, the SQL Slammer worm infected the bank’s systems, disabling most of its 13,000 ATMs and affecting its online banking system and call centers.

Patches that could have prevented the outage were available from Microsoft six months earlier, but staff didn’t install them, says Rich Griesser, senior manager of systems and security in the Tucson, Ariz., office of Clifton Gunderson Technology Solutions. However, some say Microsoft released so many SQL Server updates that it was impossible to apply them all, reports *Computer Technology Review*.

Few credit unions have a patch management program or are up-to-date with patches, especially on systems from vendors, Griesser says. Credit unions do well at patching external firewalls, routers, and switches but fall short on securing and updating internal workstations, servers, and communication devices.

Credit unions with nonproprietary network operating systems (such as Microsoft, Novell, or Linux) are the most vulnerable to security flaws and the attacks they invite, Griesser says. Viruses and worms don’t necessarily come through e-mail anymore, he says. Infecting your systems can be as easy as an employee visiting the wrong Web site or downloading a product containing hidden, malicious code. Without up-to-date patches, your credit union can be extremely vulnerable.

Regulators are making it clear that patch management is credit unions’ responsibility. National Credit Union Administration (NCUA) Letter to Credit Unions No. 03-CU-14 indicates credit unions must install vendors’ software patches and must have a patch management program as part of their computer security program.

Without patch management, you risk system unavailability, security weaknesses, and/or corruption of critical system components or data, the letter says. Here’s what to do, according to Griesser and NCUA:

- Establish a patch management policy.
- Take a systems inventory quarterly or even more often. With an inventory, you can rebuild machines that attacks render unusable.
- Read up on current threats and patches at [www.cert.org](http://www.cert.org) and [www.ntbugtraq.org](http://www.ntbugtraq.org); vendor Web sites; patch alert listservs; vulnerability scanning and reporting services; and Internet news groups.
- Evaluate the technical, business, and security impact of each patch. NCUA wants credit unions to test patches before installing them. But Griesser says most credit unions lack the time and resources to do so. Install the patch, and have a back-out strategy if it doesn’t work, he advises. Prior to installing the patch, work with your vendors to understand how it will affect a system.

“Credit unions have to form extensive relationships with their vendors to combat these attacks,” Griesser says. Tell vendors, “We need to load these patches, and we understand you have an application that may not work with it. We need you to work hard to ensure your application is up to speed with these patches so we can load them on our systems.”

—Mary Mink

## Two types of hackers

Hackers, the most common source of assaults on servers, can be divided into two categories, according to Rick Fleming, vice president of strategic technology at Digital Defense Inc. The San Antonio-based computer security firm provides vulnerability assessments and penetration testing, as well as security policy reviews and training.

“The stereotypical 16-year-old kid on a Mountain Dew high certainly exists, but he’s not nearly as dangerous as a pro, the organized criminal out to steal information for financial gain,” Fleming says.

Most hackers use automation to scour the Web for vulnerable sites, then home in on ones they think they can penetrate and where they can leave a mark. The main object is bragging rights: “Hey, I hacked into so-and-so’s site!”

But the pros are interested in profit, not vandalism. They usually already know something about their targets and seek to quietly enter them through back doors to look for financial data, source codes, or proprietary secrets they can sell.

Even more insidious are attacks by hackers who hijack servers and use them to surreptitiously store contraband (such as “warez”—illicit software copies) or harness their processing power in tandem with other captured servers to send spam or mount overwhelming “denial-of-service” attacks on large Web sites.

But perhaps the most dangerous hackers are internal: employees who know the system so well that their intrusions and thefts are virtually undetectable.

In any case, says Mike Hrabik, chief technology officer at Solutionary, Omaha, Neb., a new generation of hackers, armed with automation and easy-to-use tools, confronts intrusion detection systems today. “People who couldn’t hack before, now can. They’re also coordinated, well-educated, and willing to share techniques,” says Hrabik, whose company offers assistance with security assessments, policies, deployments, and technology selection, as well as monitoring services that continually probe credit union systems for weaknesses.

Worms are another looming concern. Worms are self-extracting and replicating code strings

that exploit vulnerabilities in Microsoft's software. "We're seeing a radical shortening of the time it takes for people to detect weaknesses in Microsoft code and develop attacks," says Fleming. "The Code Red worm in 2001 took two years for someone to develop. Later, SQL Slammer took six months. The latest one, Blaster, took 22 days."

### **Intrusion prevention**

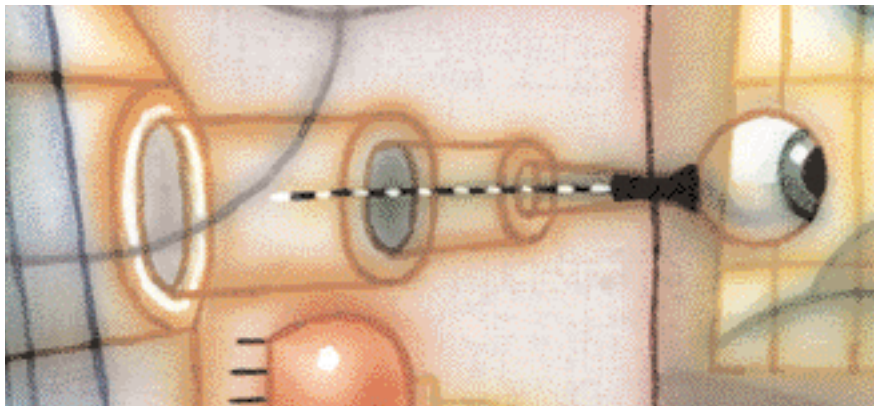
Intrusion detection systems have another element: intrusion prevention systems. There's a crucial difference between the two. For example, Digital Defense's "Network Interrogator" electronically probes a system, seeking potential vulnerabilities that haven't yet been exploited. But it doesn't attempt to penetrate the system. A penetration test, however, attempts to compromise a system by exploiting its vulnerabilities to gain the deepest access it can. The idea is that you can learn far more from an actual intrusion than from a potential one.

A further distinction between the two is that intrusion detection is passive: It can detect intrusions from all sources but can't block them. Intrusion prevention doesn't detect so much as block, acting as a barrier against certain known hostile or suspicious outside sources. But it has its limitations. While it can be installed on a network to look at all incoming Web traffic, it can't stop intrusions from inbound and partner modems, virtual private networks, and branches. Plus, if you block one source such as America Online, you block everyone who uses that carrier—a move that can alienate members.

On the other hand, says Prince, defenders do have some advantages. Because most credit unions are employer- or community-based, "it's mostly only locals who want to communicate with them. This makes it easy for us to set up blocks on packets from, say, Pakistan or South America, which the odds would say are intruders. Our firewall will incorporate a 'blacklist' of unacceptable sources, something most large corporate networks can't do."

For hackers trolling for would-be victims, the credit union world is divided into three realms:

- ▶ Big institutions that have dedicated security people and the means to hire third-party "eyes" to supplement them;



**“The stereotypical 16-year-old kid on a Mountain Dew high certainly exists, but he’s not nearly as dangerous as a pro, the organized criminal out to steal information for financial gain.”**

—RICK FLEMING

- ▶ Small credit unions that will come under hacker scrutiny because of automated programs but are too small potatoes for either boasting or theft; and

- ▶ A middle group of institutions that have more money, Web-based services, and servers than small credit unions.

“But their problem is that while they’re big enough to budget a full-time information technology [IT] person who’s busy struggling with printers and connections, they’re not big enough to budget a full-time security person,” says Fleming.

Despite their need for help with intrusion detection, credit unions can be leery of vendors. “Some worry that we’ll test to destruction or disruption, such as rebooting servers,” says Fleming. “Others won’t tell us anything about their systems beyond their Internet protocol addresses, fearing we’ll somehow compromise their security.”

Vendors answer that the real choice is between letting bad guys hack their way into sensitive areas or allowing a trusted third party enough ac-

cess to do what it needs to do. “Generally, small or medium-sized credit unions aren’t worried about third-party consultants,” says Hrabik. “But the larger ones can be skittish. They’re not always sure about plugging us in, so we do have to jump through some hoops.”

Fleming says intrusion detection vendors are understanding about giving credit unions time to trust them. “We know to step gingerly. We know tests can be disruptive, even though they’re the best way to spot vulnerabilities. And we’re aware that sometimes what we tell an IT department is that its baby is ugly. That’s hard-to-take news for people who have slaved to build a good system.”

He says vendors also remind clients there are legal consequences if they misrepresent themselves. “Improper accessing of data is an individual felony in most places, not to mention corporate criminal liabilities.”

### **How often must you monitor?**

Intrusion monitoring frequency varies among credit unions. Fleming says 75% of his company’s customers subscribe to an annual penetration test, relying in the meantime on monthly vulnerability assessments whose results they can access from a secured site. Prince says that because new meth-

ods of attack constantly turn up, credit unions must apply appropriate patches immediately (“Keep Systems Safe With Software Updates,” p. 44). Also, they need a mechanism in place that constantly looks for attacks and automatically updates their protection nightly.

Hrabik agrees that intrusion detection maintenance and updates must take on a hurried air. “We used to do yearly assessments, then went to quarterly. Now with the

latest worms, which ‘learn’ from their predecessors, it takes less than 30 days to go from a potential threat to a clear and present danger.”

He adds that patching and defending now are more complex because of many systems’ inter-

connectivity. “There are lots of potential infections from inside and out, such as a traveling colleague bringing back a contaminated laptop and connecting it to the system.”

Prince advises credit unions to understand that, with few exceptions, intrusion detection is an outsourced technology. “In-house just doesn’t work that well. An IT guy wearing eight hats with no formal training just can’t do it. It makes sense logistically and financially to outsource.”

He says the historic perception of intrusion detection as being very expensive has been justified. “There still are vendors who will charge \$15,000 or \$20,000 up front and \$2,000 per month per sensor—expenses that require a credit union to have considerable assets.” But he says it’s possible nowadays for a state-of-the-art system to cost \$1,100 up front and \$485 a month thereafter.

Hackers’ increasing sophistication and speed of innovation are stirring vendors to be more open with one another about identification methods. At the same time, customers are more savvy. “People know there’s no one solution,” says Hrabik. “They know you need a combination of things: antivirus software, detection systems, firewalls, and a willingness to commit to frequent downloads of updates and patches.”

For those credit unions still on the fence about intrusion detection systems, Prince advises budgeting for it, “even if you’re not sure you want to commit to it. Then consult with vendors until all your questions and concerns have been addressed. Once they are, and you decide to go ahead, you’ll thank yourself for having set aside money for it ahead of time.”

“In the end, this isn’t about spending millions on technology,” says Fleming. “It’s about having an overall plan with clear policies, layers of protection, and basic knowledge about how best to secure your data.” ☉

## RESOURCES

- ▶ Cavion Plus, Mounds View, Minn.; 888-534-5313 or [www.cavionplus.com](http://www.cavionplus.com).
- ▶ Digital Defense Inc., San Antonio; 888-273-1412 or [www.digitaldefense.net](http://www.digitaldefense.net).
- ▶ Solutionary, Omaha, Neb.; 866-333-2133 or [www.solutionary.com](http://www.solutionary.com).
- ▶ Clifton Gunderson Technology Solutions, Peoria, Ill.; 888-272-3476 or [www.cliftoncpa.com](http://www.cliftoncpa.com).