

<secure transaction>

<password protection>

<encoded information>



<digital fingerprint>

<virus scan>

<encryption>

Keep nefarious characters from finding holes in your information security system and scoring member data.

DARLA DERNOVSEK

Play Defense

Assuming your credit union's information security system is impregnable because it's physically "under lock and key" not only is short-sighted, it's dangerous. Nimble-fingered malintentioned individuals easily can pick or snip the lock and find the holes in your system. When they do, the costs will pile up.

Credit unions with a sound approach to information security spend a lot of time and effort playing defense: monitoring systems, creating multiple layers of security, educating members, and exploring biometrics and other emerging tactics for countering fraud.

The result is a well-rounded approach to using technology to enhance operations and interact with members.

Search for holes

"The biggest threat facing credit unions is complacency," says Jeff Multz, vice president of sales for SecureWorks, Atlanta, which provides 24/7 protection against hacker attacks for 570 credit unions nationwide. "The threat is growing exponentially."

Many credit unions assume that establishing a perimeter-style defense based on firewalls is sufficient. But experts say credit unions also must take

into account fraudsters' ingenuity.

Phishing attacks create e-mails that mimic genuine company communications to persuade members it's safe to provide personal information, which then is used for identity theft. Spyware and botnets attempt to infiltrate computer systems to plant programs that will relay information or "borrow" computer capabilities for nefarious purposes. Worms and viruses wreak havoc by crashing systems and infecting other computers. Meanwhile, hackers around the globe continuously are creating new ways to bypass security barriers.

"There's no location and there's no time on the Internet," Multz says. "That means online criminals

FOCUS

- ▶ **Threats facing CUs** are becoming more automated, quicker, and much more lethal.
- ▶ **A sound approach** to information security entails monitoring systems, creating multiple layers of security, educating members, and exploring emerging antifraud tactics.
- ▶ **The best security** can't replace common sense. Educating members and employees often is the best preparation for dealing with new threats.

can get to you, no matter where they are in the world, faster than the girl next door.”

The Santy worm that attacked credit unions during the 2004 holiday season is an example of hackers’ inventiveness, Multz says. Santy was designed to attack at a time when most information security professionals were out of the office for holiday celebrations. Santy was the first example of automated Google hacking, using the search engine to find Web servers running a vulnerable bulletin board program, and then spreading to more than 40,000 sites before loopholes were closed.



Jeff Multz

Kevin Prince, product manager for Cavion Plus, Mounds View, Minn., says the threats facing credit unions “are becoming more automated, quicker, and much more lethal.” Cavion Plus provides Web site, e-transaction, connectivity, and security services to financial institutions.

“For example, it used to be that spam and pop-ups were just annoyances. Now they can have embedded programs and steal sensitive information or create conduits for a hacker to enter a network,

usually undetected, through a firewall,” Prince says.

“Phishing scams are happening to credit unions now,” he continues. “There are Web sites with links or search engines that can direct you toward malicious code that can infect your system. We’re also moving toward zero-day worms, where the same day a vulnerability is announced, a worm is released to compromise systems before we have time to patch.”

Layer your defense

As threats continue to proliferate, focusing on one problem at a time rarely is feasible. Several experts note that adding a single program to solve a single problem, over and over again, leads to a top-heavy system that creates new holes for hackers. Instead, experts recommend a carefully layered approach to security to guard against multiple threats (see “Security basics”).



Kevin Prince

Instead, experts recommend a carefully layered approach to security to guard against multiple threats (see “Security basics”).

Hiring outside firms to design, test, and monitor security measures can be less expensive than hiring internal experts, although both approaches require an adequate budget and senior management buy-in. An ideal approach combines internal experts with external advisers and services.

“One thing I hear consistently that concerns me is that

credit unions think security is cheap,” says Rick Fleming, chief technology officer for security firm Digital Defense, San Antonio. “They think they should be able to have all their security needs met for \$300 a year.”

But off-the-shelf software for fending off viruses and creating firewalls is unlikely to provide the level of sophistication required to prevent intrusion from determined hackers, who see financial institutions as prime targets.

Likewise, credit unions must check security firms’ credentials and experience to ensure they have a high level of expertise.

Credit unions that shortchange the budget for information security may be unaware that damage to their reputation and the need to recreate data carry a high price tag, typically outweighing actual financial losses from successful attacks, Fleming says.

► SECURITY BASICS

A sound security system may contain five overlapping layers:

► **Level one: policies and procedures.** Written documents define who has physical and online access to specific portions of the system, how access is protected, and how the credit union reacts when security is breached.

► **Level two: perimeter protection.** The credit union needs barriers at the gateways where internal and external users gain access. A firewall combines hardware and software to serve as a sentry stationed at the gateway. An appliance that sits outside the firewall to filter traffic delivers “network intrusion prevention” by setting off alarms and triggering countermeasures when attacks occur. Antivirus scans can be provided at the gateway or at every desktop computer.

► **Level three: monitoring.** Basic steps may include assigning a staff member to examine firewall logs to spot potential attacks. At the higher level known as “intrusion detection,” an outside firm maintains a 24/7 watch for potential attacks on key servers. “Intrusion prevention” and “intrusion detection” sometimes are used interchangeably, and the systems may overlap.

► **Level four: testing/audits.** A full-scale security audit by an outside firm should probe the system at least every three years, although an annual audit is better. Between audits, quarterly tests should look for common weaknesses, such as holes created by Internet connections.

► **Level five: continuous improvement.** Patching holes in software, repairing deficiencies in existing security systems, and learning about new challenges defend against emerging threats.



Rick Fleming

While a layered approach is valuable, too many credit unions start with “the outer layer of the onion,” according to Karim Toubba, vice president of product management and marketing for Redwood City, Calif.-based Ingrin Networks, which helps credit unions secure information stored

in applications and databases. That information is the innermost layer of the onion, with the greatest need for protection.

“Instead of just protecting systems, credit unions need to adopt a mechanism that protects the information within those systems,” Toubba says.

Encryption can make data unusable to outsiders or unauthorized insiders, removing the greatest risk of data theft or malicious access. To make data truly secure, they should be encrypted on a separate appliance before being stored in the credit union’s computer system. Store encryption keys on this appliance, away from the data on the computer system. That will keep the encryption keys hidden from attackers and allow encryption to occur without slowing other functions on the computer system.



Karim Toubba

Add biometrics

Another promising method for strengthening information security is the use of biometrics, which verifies the user’s identity by relying on physical characteristics such as a fingerprint or the iris of the eye. Biometric scans map physical characteristics and then convert them to mathematical equivalents stored and recalled when needed to verify identity.

Among credit unions experimenting with biometrics are Purdue Employees Federal Credit Union, West Lafayette, Ind., with \$400 million in assets, and Technology Credit Union, San Jose, Calif., with \$1.1 billion in assets. Members of both credit unions tend to be highly educated about technology.

Since 1997, Purdue Employees Federal members have been able to use their thumbprints to access accounts at kiosks in five branches, eliminating the need for passwords or plastic cards. It also uses biometrics to protect laptop computers used by traveling employees, who must provide both a password and a fingerprint to gain access.

This year the credit union plans to require a finger-



Technology CU, San Jose, Calif., uses this biometric scan device at six branches to verify the identities of members who perform transactions via tellers.

print scan for everyone who works on its computer system so it can track who’s doing what at any given time, explains Bill Arnold, assistant vice president, technology.

Purdue Employees Federal included biometric capabilities in its most recent request for proposals for online banking vendors and probably will make biometrics an optional security improvement for online banking users in the future, possibly as early as 2006. Participating members would attach a fingerprint scan device to their computers and then perform the scan each time they accessed online banking. The credit union has 28,000 members who use online banking at least once every 90 days, with 17,000 getting e-statements and 8,500 enrolling in bill payment services.

Biometric devices would be optional, Arnold says, because some members still are reluctant to use biometrics and some value convenience more than security. He notes that some members concerned about privacy may be unaware that the series of numbers generated by biometric scanners can verify a fingerprint but are insufficient to independently re-create it.

Convenience also is an issue because traveling members may need to access their accounts from computers without biometric scanners, such as those offered by hotels or coffee shops. Mandating the use of biometrics also might create an obligation to provide support for members’ computers, Arnold says. Finally, some users may be unaware that biometric technology now can verify whether the finger submitted for the scan is attached to a living person, removing the fear of criminal access.

The lack of an accepted biometric standard is another issue, according to Barbara Cure, research and

RESOURCES

- ▶ Cavion Plus, Mounds View, Minn.: 888-534-5313 or cavionplus.com.
- ▶ CUNA Technology Council: 800-356-9655, ext. 4393, or cunatechnologycouncil.org.
- ▶ CUNA's strategic alliance providers: alliances.cuna.org
- ▶ Digital Defense, San Antonio: 888-273-1412 or digitaldefense.net.
- ▶ Ingrian Networks, Redwood City, Calif.: 866-464-7426 or ingrian.com.
- ▶ SecureWorks, Atlanta: 877-905-6661 or secureworks.com.

development manager for Technology Credit Union, which has equipped six branches with biometric scans to verify the identities of members who perform transactions via tellers. The

credit union plans to use biometric screening to secure automated teller machines and online banking in the future.

Technology Credit Union introduced biometric screening in June 2003, with 5,800 members (8% of the total membership) enrolling as of January 2005—without any advertising. Cure says biometrics users tend to have higher balances and more accounts. Users come from all age groups, with the largest single group, 2,018 members (40% of all users), age 30 to 45.

If biometric security was mandatory, Cure says the credit union's internal system could adapt to accept scans from a variety of devices. However, it would be easier if all hardware manufacturers accepted and followed one standard format.

As computer manufacturers begin to add biometric scanners to new models and governments begin using biometrics to verify the identities of passport holders, Cure says pressure for a single standard will increase. "As soon as the standards question is settled and members can use one solution across multiple channels, biometrics will become very important."

Teach secure practices

While biometrics and other advances can solve specific problems, they can't replace common sense. Educating members and employees alike often is the best preparation for dealing with new threats that can mutate as they spread, says Lester Warby, vice president/chief information officer at \$413 million asset Seattle Metropolitan Credit Union and a member of the CUNA Technology Council's executive committee.

"To complicate matters even more, many of the

'crackers' are reverting to the old-fashioned hacking technique of social engineering to gain advantage and challenge our systems," Warby says. "Social engineering" refers to tactics used by phishers and con artists who create a plausible scenario online or offline to persuade people to share confidential information. "It doesn't matter how good your security systems are if you have tellers who give out their user IDs and passwords."

A truly layered approach to security must combine all types of online and offline challenges. That's the approach the Credit Union National Association (CUNA) takes as it develops third-party relationships supporting credit unions' security services, according to Wes Millar, CUNA's senior vice president of strategic alliances.



Wes Millar

"It's paramount that we look for cost-effective solutions that encompass the full range of credit unions' security risks: physical security, network security, fraud prevention, and more," Millar says.

When security breaches occur, experts advise credit unions to patch the hole and then quickly and honestly share information with members to preserve trust and gain their cooperation. The credit union must restore "business as usual" for internal and external users as soon as possible.

"One of the biggest security challenges also is the one most overlooked: maintaining business functionality while at the same time protecting the credit union's assets," Warby says. Users want quick-and-easy access, while security-conscious executives may desire total security. But total security may be attained only by placing the computer in a locked room and forbidding access to everyone.

"The trick is finding a happy and safe medium between the two," Warby maintains. For Warby and other experts, the best way to find that medium is to combine all the tools available. "It truly has to be an intrinsic, global approach to business operations that includes hardware and software, external and internal risks, staff training, and member education." ©

For more security coverage, visit CREDITUNIONmagazine.com



Lester Warby