THIS LETTER APPLIES TO ALL FINANCIAL INSTITUTIONS THAT MAINTAIN COMPUTER NETWORKS CONNECTED TO THE INTERNET.

SECURITY MONITORING OF COMPUTER NETWORKS

FIL-67-2000
October 3, 2000

TO: CHIEF EXECUTIVE OFFICER
SUBJECT: *Security Monitoring of Computer Networks*

Any financial institution that maintains computer networks connected to the Internet should be aware that such connections create vulnerabilities that may pose risks to the institution's information assets. Such risks could arise whether computer networks are maintained in-house, outsourced to a third-party service provider, or both.

In this Financial Institution Letter (FIL), the FDIC has suggested some practices for maintaining secure network operating systems and certain application programs run by such operating systems. The FIL addresses the need to watch for external - as well as internal - threats to computer networks from crackers/hackers and suggests steps for reducing computer network vulnerabilities.

External Threats

When a financial institution network is linked to the Internet, either through an in-house connection or an outsourcing arrangement, crackers/hackers can exploit any weakness or "hole" in the institution's computer operating systems and applications to gain access to the network, and, ultimately, to financial institution data. Several Internet sites provide free notification of systems and application vulnerabilities to site subscribers. (A short, but not all-encompassing, list of such Web sites is attached. These sites focus on the most common network operating systems used by most financial institutions.) However, examiners have noted that many financial institutions are not using these Web sites. Crackers/hackers routinely monitor the Web sites to learn of new weaknesses that have been found. Financial institutions that do not subscribe to such services and do not keep operating system patches current are very vulnerable to attacks. The FDIC recommends that financial institutions use these services to augment system security.

Management should ensure that bank staff or the bank's service provider perform regular reviews of the security parameter settings on devices such as routers, firewalls and network servers to ensure they remain at current settings, particularly following the installation of updates to network operating systems or application programs. Recovery procedures should ensure that all revisions and patches are updated on the system to prevent exploitable files or other weaknesses from being reintroduced if a system crash occurs. There should be procedures for recording receipt, approval and necessary action on security program bulletins, patches and upgrades.

Another important method to monitor network activity is the automated audit/logging feature built into firewall, router and host systems, providing audit trails of daily activity that are essential to any forensic investigation. These logs are an important management tool; however, many institutions use more advanced tools because they require fewer computer resources, provide concise, timely information, and take less time to review. These more sophisticated automated tools alert operational personnel and management on a real-time basis to attempts to compromise systems. These automated tools make it easier for operational personnel to recognize and respond to attempts to compromise computer systems. Whichever method management uses, it is imperative that appropriate personnel activate security logs and review them frequently.

A cracker/hacker may attempt to access confidential financial institution information on the Internet with the intent to change or destroy it. Management should prepare a formal, written recovery plan and form an incident response team. If there is an attack on a computer system, the incident response team should be prepared to take appropriate action. The FDIC's FIL-68-99, *Risk Assessment Tools and Practices For Information System Security*, provides guidance on defense and incident response strategies. Once a compromise is identified, procedures should be in place to bring computer systems back in a secure environment. A trusted copy of the institution's Web site, operating system(s) and bank and customer data should be available to restore the site and/or system to its original condition. The plan should be tested periodically to ensure that the recovery process will work as expected.

Internal Threats

Notwithstanding news stories about crackers/hackers, the majority of intrusions originate inside financial institutions. For that reason and others, it is important to maintain sound internal controls. These should include regular management reviews of employee access levels to ensure they are appropriate for each employee's job responsibilities. Management should periodically verify the existence of adequate segregation of duties or, if necessary, appropriate compensating controls. The FDIC recommends background checks of bank personnel and contractor personnel having access to the bank's systems or data.

Outsourcing

Whether Internet or core banking functions exist in-house or are outsourced, management is responsible for ensuring that financial institution and customer data are protected. If a financial institution relies on a third-party service provider, management must have a general understanding of the provider's information security program to effectively evaluate whether the security system can protect institution and customer data. Management should review an up-to- date independent evaluation of the third-party service provider's security program, which should address external and internal threats to computer security. The evaluation also should address what actions were taken to correct weaknesses following vulnerability assessments or penetration analyses.

For more information, please contact Thomas J. Tuzinski, Review Examiner in the Division of Supervision, at 202-898-6748.

Michael J. Zamorski
Acting Director

Attachment: Web Site Security Resources As Of October 2000

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (800-276-6003 or 202-416-6940).

WEB SITE SECURITY RESOURCES AS OF OCTOBER 2000

These sites are listed to alert you to the availability of the services that these and similar sites offer. The listing of these representative sites does not constitute the FDIC's endorsement or recommendation of the sites or reflect on any sites not listed. The FDIC has not evaluated the sites listed. If you elect to use any such Web site, you should do so only after careful, independent evaluation of the services it offers. The FDIC expressly disclaims any liability arising out of the use of such services.

- www.cerias.purdue.edu- Center for Education and Research in Information Assurance and Security, sponsored by Purdue University; free online seminars and access to research papers.

- www.cert.org- Computer Emergency Response Team at Carnegie Mellon University; analyzes product vulnerabilities and provides available patches or "fixes."

- www.icsa.net- International Computer Security Association; conducts research, testing and certification programs for computer systems, provides information on current industry events, security vulnerabilities, and technical papers.

- www.nipc.gov- National Infrastructure Protection Center; provides advisories, alerts and warnings concerning system vulnerabilities. This site links to InfraGard, another useful site.

- www.ntbugtraq.org- collection of security advisories, vulnerabilities and solutions; Bugtraq mailing list.

- www.sans.org- System Administration, Networking and Security Institute; general computer security site, provides security alerts to subscribers.