NCUA INFORMATION TECHNOLOGY SECURITY ALERT

NATIONAL CREDIT UNION ADMINISTRATION
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: July 2, 2004

TO: All Federal and State Credit Unions
All Corporate Credit Unions
All State Supervisory Regulators

SUBJECT: Recent Cyber Attacks

PURPOSE

This alert is intended to raise awareness of a number of cyber attacks targeted at financial institutions in recent days. The attacks have the potential to infect financial institution and consumer PCs, and obtain name and password information, allowing unauthorized access to financial accounts. The attacks exploit vulnerabilities in servers and in web browsers. Additional information can be obtained from sources such as the US-CERT web site http://www.us-cert.gov/.

BACKGROUND

A vulnerability in Microsoft's Internet Information Server (IIS) may be used to compromise servers of federally insured credit unions and other enterprises. An infected server may download code to the computers of users for various purposes that may include the capture of account login (ID / Password) information. Although information concerning remediation actions is currently incomplete, federally insured credit unions should be aware of the vulnerability and increase the monitoring of their servers for unusual activity. If such activity is observed, federally insured credit unions should initiate an appropriate response including investigation, notification of law enforcement, NCUA (or applicable State Supervisory Authority), and member notification if necessary. Additionally, federally insured credit unions that use technology service providers should contact those providers to ensure that they are aware of the vulnerability and are taking appropriate risk mitigation actions.

There have been attacks against Microsoft's Internet Explorer, as well. These are designed to obtain confidential consumer data. In general, these attacks occur when a user visits an infected web site that silently downloads and installs software that records, encrypts, and transmits confidential data to the attacker. Once installed, the software specifically "looks" for account access and, if detected, begins recording the users keystrokes to capture the user's ID and password. The changing of passwords or other access codes on an infected computer is not a solution as these may also be captured. Installation of the virus is possible on a fully patched computer. Credit union remediation strategies should address both credit union and member users.

RESPONSE TO THIS THREAT

Federally insured credit unions should consider a complete range of risk mitigation techniques for their computers. Those techniques could include the scanning and cleansing of incoming web content, diligent use and updating of anti-virus definitions, regular scanning using new definitions, and auditing computers for unauthorized, unexpected, and harmful code, and a limitation on web browsing.

Federally insured credit unions members' computers may have already been successfully attacked. Federally insured credit unions should be particularly aware of unusual activity in their members' accounts, or reports of unusual information requests associated with their website reported by their members. Should unusual activity appear to be related to the member's Internet usage, federally insured credit unions should recommend that the member obtain appropriate assistance to identify and remediate any potential problems.

The vulnerabilities described in this notification continue to be researched by software, anti-virus, and other IT vendors. Explicit remediation action for all of these vulnerabilities have not yet been formally released by those vendors. NCUA recommends that credit unions and their technology service providers continue to monitor vendor and security websites (e.g. Microsoft, US_CERT) so that remediation steps, including the application of appropriate patches, can be initiated as soon as they become available.

Credit unions that have online banking should monitor FS-ISAC's website, www.fsisac.com, for additional information. Credit unions that are not currently members of FS-ISAC should consider joining. FS-ISAC provides credit unions with a means of identifying challenges presented by increasingly sophisticated cyber and physical threats.

In the event your institution is a victim of exploitation of the vulnerabilities described above, you should report the incident to law enforcement and file a Suspicious Activity Report, as appropriate, based on the impact on your credit union.

_____/s/_____
J. Leonard Skiles
Executive Director
National Credit Union Administration