ALERT 2001–4

OCC ALERT

Comptroller of the Currency
Administrator of National Banks

Subject: Network Security Vulnerabilities

TO: Chief Executive Officers and Chief Information Technology Officers of National Banks, Federal Branches, Service Providers and Software Vendors; Department and Division Heads, and Examining Personnel

PURPOSE

This alert is intended to raise awareness regarding potential threats in electronic banking systems and to remind banks and service providers to identify and correct network security vulnerabilities.

BACKGROUND

In recent weeks, hackers have exploited a number of significant vulnerabilities in e-commerce systems. Recent National Infrastructure Protection Center (NIPC) advisories report an increase in unauthorized activities targeting e-commerce Web sites and identify some common and frequently utilized vulnerabilities in commercially available hardware and software.[1] These vulnerabilities may allow unauthorized access to bank and service provider systems. Unauthorized intrusions threaten the confidentiality, integrity, and availability of bank information systems and customer information. If successful in breaching a system and gaining access to customer records, unauthorized parties may fraudulently withdraw funds from bank accounts, obtain funds through identity theft, or extort funds by threatening public disclosure.

RESPONSE TO NETWORK SECURITY VULNERABILITIES

In response to the increased risks, the Office of the Comptroller of the Currency (OCC) advises banks and service providers to review the NIPC advisories. In addition, banks should review their controls to safeguard customer information and bank information systems. As part of this effort, banks and service providers should take the following steps to respond to network vulnerabilities:

- Identify systems vulnerabilities in a timely manner and evaluate the inherent risks, taking into account the network system configuration and system architecture.

[1] NIPC Advisory 01-003, "E-Commerce Vulnerabilities Update," dated March 8, 2001; and NIPC Advisory 00-60, "E-Commerce Vulnerabilities," dated December 1, 2000. Refer to www.nipc.gov for additional information.

- Eliminate unwarranted risks by applying vendor-provided software fixes, commonly called "patches."

- Ensure that exploitable files and services are assessed and removed or disabled, based upon known vulnerabilities and business needs.

- Ensure that changes to security configurations are documented, approved, and tested.

- Update vulnerability scanning and intrusion detection tools to identify known vulnerabilities and related unauthorized activities.

- Conduct subsequent penetration testing and vulnerability assessments, as warranted.

- Review contracts with service providers to ensure that security maintenance and reporting responsibilities are clearly described. As part of this review, banks should ensure that service providers notify them of systems security breaches that may affect their bank.

- Establish monitoring, reporting, and investigation controls that identify unusual funds transfer activities as a potential indicator of system security breaches.

ADDITIONAL INFORMATION

A bank's board of directors is responsible for ensuring that an effective information security program is in place and operating properly. In the event that bank information systems are subject to unlawful activities, including suspected intrusions, the events should be reported in Suspicious Activity Reports, consistent with 12 CFR 21.11. Additional information on OCC and FFIEC information security guidance can be obtained on the OCC's Web site at www.occ.treas.gov and includes:

- OCC Bulletin 2001–8: Guidelines Establishing Standards for Safeguarding Customer Information (February 15, 2001)
- OCC Advisory Letter 2000–12: FFIEC Guidance on Risk Management of Outsourced Technology Services (November 28, 2000)
- OCC Bulletin 2000–19: Suspicious Activity Report: New SAR Form (June 19, 2000)
- OCC Bulletin 2000–14: Infrastructure Threats -- Intrusion Risks (May 15, 2000)
- OCC Bulletin 98–38: Technology Risk Management: PC Banking (August 24, 1998)

Questions regarding this alert should be directed to Clifford A. Wilke, Director, Bank Technology Division, at (202) 874–5920 or by e-mail: clifford.wilke@occ.treas.gov.

_____

Clifford A. Wilke
Director, Bank Technology Division