Evaluation Report

OIG-08-035

INFORMATION TECHNOLOGY: Network Security at the Office of the Comptroller of the Currency Needs Improvement

June 03, 2008

Office of Inspector General

Department of the Treasury

Contents

Appendices

Abbreviations

CIO	Chief Information Officer
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
SP	Special Publication
TD P	Treasury Directive Publication

John C. Dugan
Comptroller of the Currency

The purpose of our evaluation was to assess the network security of the Office of the Comptroller of the Currency (OCC). Our overall objective was to determine whether sufficient protections exist to prevent intrusions into OCC's network, systems, or computer equipment. To accomplish this objective, we used specialized software to detect and exploit vulnerabilities in OCC's systems. We also performed two social engineering tests to assess users' awareness of e-mail security threats and followed up on findings from our prior report.[1] We performed our work from June through December 2007. Appendix 1 contains a detailed description of our objective, scope, and methodology.

Results in Brief

We determined that OCC has not established adequate security controls to protect its network, systems, equipment, and data. Specifically, we found high- and medium-severity vulnerabilities, including one that allowed us to gain full access on one OCC server.[2] We had four overall findings:

1. Configuration management needs improvement [repeat finding].
2. Logical access control needs to be strengthened [repeat finding].

[1] *Information Technology: Effective Security Controls Needed to Mitigate Critical Vulnerabilities in the Office of the Comptroller of the Currency's Networked Information Systems*, OIG-06-040 (Sep. 14, 2006).
[2] International Business Machines Internet Security Systems a company that provides security products and services designed to protect organizations against Internet threats, defines high-severity vulnerabilities as allowing immediate remote or local access, or immediate execution of code or commands, with unauthorized privileges.

3. User awareness of e-mail social engineering needs improvement [new finding].
4. Wireless security needs improvement [new finding].

Furthermore, we determined that, despite progress, some planned corrective actions addressing the findings and recommendations in our prior report remain incomplete. Table 1 lists unimplemented prior-year recommendations.

Table 1: Unimplemented Prior-Year Recommendations

Prior-year recommendations	Current status
Apply the latest service packs and security updates for systems and applications.	Incomplete; see finding 1.
Disable or remove unused options and services for compact discs and optional subsystems.	Incomplete; see finding 1.
Correct password security measures in OCC's systems to meet OCC's policy requirements.	Incomplete; see finding 2.

Consequently, we reiterate these recommendations from our prior report.

Upon completion of our fieldwork, we provided four Notifications of Findings and Recommendations, which included 21 recommendations (including incomplete recommendations), to the Chief Information Officer (CIO) of OCC. The CIO concurred with our findings and recommendations and provided plans for corrective actions. Due to the sensitivity of the recommendations, we summarized them as follows for this report:

1. Apply the latest service packs and security updates for systems and applications [repeat recommendation].
2. Disable or remove unnecessary or unused services running on OCC systems [repeat recommendation].
3. Reconfigure system services with more secure options [new recommendation].
4. Implement security configurations required by Treasury Directive Publication (TD P) 85-01 and OCC policies [new recommendation].

5. Ensure that the principle of least privilege is enforced and applied to all OCC computer users as required by OCC policy [new recommendation].
6. Ensure that account management and access controls are adequate for OCC systems [new recommendation].
7. Correct password security measures in OCC's systems to meet policy requirements [repeat recommendation].
8. Improve user awareness training on e-mail security, phishing, and incident reporting [new recommendation].
9. Ensure that appropriate wireless access restrictions exist [new recommendation].
10. Ensure OCC users are trained on the security risks of connecting to unapproved or unknown wireless networks [new recommendation].

Upon completion of our fieldwork, we provided the CIO a crosswalk linking the summary recommendations listed above to the 21 recommendations provided in the Notifications of Findings and Recommendations. As noted in appendix 2, OCC management concurred with our recommendations. We agreed that the formal steps the Comptroller has taken are responsive to the intent of the recommendations.

Background

OCC was created by Congress to charter national banks, to oversee a nationwide system of banking institutions, and to assure that national banks are safe and sound, competitive and profitable, and capable of serving in the best possible manner the banking needs of their customers. OCC's network and systems are integral parts of its mission support structure. Several of OCC's systems contain personally identifiable information collected during examinations and other oversight activities. By law, OCC is prohibited from releasing information from its bank safety and soundness examinations to the public.

Because OCC's network computers are connected with each other, other bureaus' networks, and the Internet, it is important that proper configurations and controls be in place to ensure that only authorized users are granted access. Unauthorized access to OCC's network could provide an intruder with the opportunity to compromise the confidentiality, integrity, and availability of sensitive information. Once inside, unauthorized users could extract, delete, or modify sensitive data; discover user names and passwords; and launch denial-of-service attacks. Undetected, such activities could hinder OCC's mission and undermine public faith in the safety of banking information.

Findings and Recommendations

Finding 1 Configuration Management Needs Improvement

We determined that configuration management needs improvement. We found that several servers were missing critical patches. Also, unnecessary or insecure services were running on systems, and system services were configured with insecure options. We also found several high- and medium-severity vulnerabilities that did not meet the configuration management requirements set forth by the National Institute of Standards and Technology (NIST); TD P 85-01, "Treasury Information Technology Security Program" (Nov. 3, 2006); and OCC. Some of these vulnerabilities were repeat findings from our previous report. In particular, we exploited successfully the vulnerability on one of the servers and gained full, unauthorized access to this system with the local administrative privilege.

TD P 85-01 requires bureaus to ensure that security patches are tested and installed on a timeline in accordance with the criticality of the patches. NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems," recommends that the organization configure the information system to provide only essential capabilities and specifically prohibits or restricts the use of the functions, ports, protocols, and/or services as defined by the agency. "OCC

Information and Security Program: Policies, Standards, and Required Controls" states that OCC reviews the functions and services provided by information systems, or individual components of information systems, to determine which functions and services (e.g., VoIP, IM, FTP, HTTP, file sharing) are not essential for mission objectives.

Failure to apply up-to-date patches precluded OCC from adequately protecting systems on its network from virus infection and hacker attacks. Also, unnecessary or insecure services, including services configured with insecure options, could result in a larger potential attack surface, more potential entry points, information disclosure, or additional overhead to maintain unneeded functionality.

Recommendations

We recommend that the Comptroller of the Currency do the following:

1. Apply the latest service packs and security updates for systems and applications [repeat recommendation].
2. Disable or remove unnecessary or unused services running on OCC systems [repeat recommendation].
3. Reconfigure system services with more secure options [new recommendation].
4. Implement security configurations required by TD P 85-01 and OCC policies [new recommendation].

Finding 2 Logical Access Control Needs To Be Strengthened

We determined that logical access control needs to be strengthened. We found that OCC did not follow the principle of least-privileged user account to ensure that users always log on with limited privileges. Specifically, local administrative privileges were given out excessively. We also found that OCC had inadequate account management procedures, insufficient access controls for Windows shares, and weak authentication measures, resulting in security vulnerabilities.

NIST SP 800-53 requires that the information system enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. In addition, OCC policy requires that all accounts be role-based and implemented through role-based group membership. No individual role should be allowed to cross system/application or environment boundaries. Moreover, "OCC Information Security Program: Policies, Standards, and Required Controls" requires users to identify themselves and authenticate their identity using unique credentials before they can access OCC information systems and provides specific password requirements.

Appendix III to Office of Management and Budget Circular No. A-130, "Security of Federal Automated Information Resources," requires that a number of technical, operational, and management controls be used in every general support system to prevent and detect security breaches or violations. Such controls include least privilege, which is the practice of restricting a user's access (to data files, processing capability, or peripherals) or type of access (read, write, execute, and delete) to the minimum necessary to perform his or her job. In addition, an individual should be assigned to be a focal point for assuring that security within the system, including ways to prevent, detect, and recover from security problems, is adequate.

If the principle of least privilege is not enforced to ensure that users always log on with the minimum necessary access, attacks could be more likely to succeed. A user or a program with local administrative rights could make system wide changes, either intentionally or accidentally, making it far easier for malicious software to be installed on that computer.

In addition, if OCC does not enforce password security measures that meet Treasury policy requirements, the existing vulnerabilities could directly compromise OCC's network and systems by allowing attackers immediate access as privileged users, such as administrators, using widely known hacker programs.

Recommendations

We recommend that the Comptroller of the Currency do the following:

5. Ensure that the principle of least privilege is enforced and applied to all OCC computer users as required by OCC policy [new recommendation].
6. Ensure that account management and access controls for OCC systems are adequate [new recommendation].
7. Correct password security measures in OCC's systems to meet Treasury's policy requirements [repeat recommendation].

Finding 3 User Awareness of E-mail Social Engineering Needs Improvement

We determined that user awareness of social engineering via e-mail needs improvement. We conducted two e-mail social engineering awareness tests at OCC. In the first test, we sent an e-mail containing a link to malicious code that resided on our laptop to 1000 e-mail addresses. Although OCC's countermeasures prevented the code from running, 194 users accessed this link. During the second test, we sent a phishing e-mail to 2,783 e-mail addresses with a link to a spoofed Web site set up on our laptop asking users to enter their passwords.[3] Two hundred twenty-nine users accessed this link, and 153 entered their passwords. The OCC Computer Incident Response Center reported 105 user calls the day of the first test and 183 user calls the day of the second. The average daily calls for the weekday over the 3-month period during which the tests occurred was 94. Only one user actually admitted clicking on the link used during the second test.

"OCC Information Security Program: Policies, Standards, and Required Controls" states the following:

[3] Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking e-mail in an attempt to gather information from recipients. A spoofed Web site is a site designed to look like a legitimate site, sometimes using components from a legitimate site, that is intended to deceive.

- OCC users shall safeguard authenticators by maintaining possession of their individual authenticators; not loaning or sharing authenticators with others; and reporting lost or compromised authenticators immediately.

- OCC employees and contractors are responsible for: preserving the security of OCC systems; all actions and functions performed using their identification and authentication credentials; compliance with password policies; securing the confidentiality of their identification and authentication credentials; and immediately reporting suspicious system activity noted during logon to local resident technical associates.

- OCC employees and contractors are responsible for reporting security incidents or suspected incidents to local Technical Support Representatives.

The ability of attackers to convince large numbers of OCC employees and contractors to connect to unknown Web sites and provide sensitive information could undermine the security of OCC's network. This threat was compounded by the fact that only 1 out of 229 users who accessed the phishing site reported the potential security breach. In a real attack, the incident could have led to the unreported disclosure of user passwords. As a result, unauthorized people could have gained access to the OCC network or user accounts.

Recommendation

We recommend that the Comptroller of the Currency do the following:

8. Improve user awareness training on e-mail security, phishing, and incident reporting [new recommendation].

Finding 4 Wireless Security Needs Improvement

We determined that OCC's wireless security needs improvement. OCC users have the ability and authorization to connect to potentially malicious wireless systems with their OCC laptops. According to OCC management, OCC users did not receive any training regarding the risks of connecting to unauthorized wireless networks. Our testing enabled 21 OCC laptops to connect to a fake access point that we had set up.

"OCC Information Security Program: Policies, Standards, and Required Controls" states that OCC allows the use of wireless technologies only if an authorizing official approves the use; strong authentication and identification methods are used; approved encryption is used; and networks are scanned for rogue access points.

TD P 85-01 requires that bureaus takes steps to protect their wireless networks, including establishing usage restrictions and implementation guidance for wireless technologies and documenting, monitoring, and controlling wireless access to the information system. Also, bureaus are required to employ security mechanisms for wireless networks consistent with the sensitivity of the information to be transmitted.

NIST SP 800-48, "Wireless Network Security: 802.11, Bluetooth, and Handheld Devices," provides additional guidance on wireless network security, with particular emphasis on Institute of Electrical and Electronics Engineers 802.11b and Bluetooth standards.

If OCC's systems were connected to an attacker's wireless access point, an attacker could establish fake services to obtain information from the connected systems, gain access to OCC's LAN, or establish a man-in-the-middle set-up to view information transmitted via wireless from the attached systems.

Recommendations

We recommend that the Comptroller of the Currency do the following:

9. Ensure that appropriate wireless access restrictions exist. [new recommendation].
10. Ensure that OCC users are trained on the security risks of connecting to unapproved or unknown wireless networks [new recommendation].

* * * * * *

I would like to extend my appreciation to the OCC CIO and OCC staff for the cooperation and courtesies extended to my staff during the evaluation. If you have any questions, please contact me, at (202) 927-5171 or Gerald J. Steere, IT Specialist, Office of Information Technology Audits, at (202) 927-6351. Major contributors to this report are listed in appendix 3.

/s/

Tram J. Dang, Acting Director
Office of Information Technology Audits

The overall objective was to determine whether sufficient protections exist to prevent intrusions into the Office of the Comptroller of the Currency (OCC) network, systems or computer equipment. This evaluation is included in the Office of Inspector General Annual Plan for 2007.[4] In addition, the results of this evaluation may be used to support our Department of the Treasury work undertaken in accordance with the requirements of the Federal Information Security Management Act. We performed our fieldwork at OCC locations and the Treasury Office of Inspector General in Washington, D.C., from June through December 2007. We conducted our evaluation in accordance with the President's Council on Integrity and Efficiency's Quality Standards for Inspections.

We performed most logical tests from within OCC's network and from the Internet.[5] We did not prioritize or rank the security vulnerabilities detected by the tools used, nor did we evaluate the remedies for the vulnerabilities identified. In conducting our review, we used specialized software to conduct the vulnerability scanning and penetration testing. We also performed two social engineering tests to evaluate user awareness and responsibility in protecting computer equipment.

Upon completion of our tests, we provided OCC management with reports generated by our tools and evidence of findings. The reports provided details on specific vulnerabilities detected and exploited and the suggested actions needed to address them. We also provided OCC management with Notifications of Findings and Recommendations so that corrective actions could be implemented immediately

[4] See OIG, *Annual Plan Fiscal Year 2007*, p. 32.
[5] Logical tests are tests that exploit vulnerabilities in the computer's software.

MEMORANDUM

Comptroller of the Currency
Administrator of National Banks

Washington, DC 20219

To: Tram Dang, Acting Director, Information Technology Audits

From: John C. Dugan, Comptroller of the Currency [redacted]

Date: 5/29/08

Subject: Comments on Draft Evaluation Report

We have received and reviewed your draft report titled "Information Technology: Network Security at the Office of the Comptroller of the Currency Needs Improvement." Your overall objective was to determine whether sufficient protections exist to prevent intrusions into the OCC's network, systems, or computer equipment. To accomplish this objective, you used specialized software to detect and exploit vulnerabilities in the OCC's systems. You also performed two social engineering tests to assess users' awareness of e-mail security threats.

The results of your testing, led you to conclude that: (1) the OCC's configuration management needs improvement; (2) logical access control needs to be strengthened; (3) user awareness of e-mail social engineering needs improvement; and (4) wireless security needs improvement. We concur with these findings.

Your report served to underscore a number of items we had already identified and taken measures to correct. Other corrective actions are underway. The attached table provides the status of our actions to implement all of your recommendations. Detailed supporting documentation is being provided separately.

Your evaluation was also helpful in pointing out the need to improve some of our business processes. For example, we now track and report remediation efforts through the Audit Fix integrated project team to identify, track, and ensure corrective actions taken are effective in preventing future vulnerabilities. A newly formed Information Assurance (IA) team tests our remedial efforts and also performs continuous scanning of the OCC's networks, workstations, servers, databases and major applications to test for the vulnerabilities you identified. The IA team also conducts monthly reviews for compliance with our password policy.

In addition, we have formalized our configuration management process through the Enterprise Change Control Board (ECCB). Information technology security requirements are now being integrated with the ECCB's change management processes and leveraged for stronger configuration management practices. While this initiative is continuing to evolve, it has already

helped improve OCC's overall security posture by making vulnerability testing a standard part of OCC's configuration management program.

The OCC remains committed to strengthening our information technology security program. If you need additional information, please contact Bajinder Paul, Chief Information Officer, at 202-874-4480.

Thank you for the opportunity to review and comment on your draft report.

Attachment

-2-

Status of Recommendations: Network Security Needs Additional Improvement

Recommendation	Status of Corrective Action
1. Apply the latest service packs and security updates for systems and applications.	Completed February 29, 2008.
2. Disable or remove unnecessary or unused services running on OCC systems.	Completed March 19, 2008.
3. Reconfigure system services with more secure options.	Numerous corrective actions have already been completed. By May 30, 2008 we will strengthen authentication for outbound e-mail messages by limiting use of SMTP to an authorized list of platforms. At the same time, we will have completed testing of our remediation of applications compatible with earlier, less secure versions of Windows and push them into production.
4. Implement security configurations required by Treasury Directive Publication (TD P) 85-01 and OCC policies.	We have developed an archiving solution to minimize the risk of loss of audit information on three servers. This solution will be implemented by May 30, 2008.
5. Ensure that the principle of least privilege is enforced and applied to all OCC computer users as required by OCC policy.	To complete implementation of this recommendation, the OCC will apply NIST security configuration standards to all OCC workstation computers. We are currently developing a Federal Desktop Core Configuration that we plan to put into place by December 31, 2008.
6. Ensure that account management and access controls are adequate for OCC systems.	Completed March 15, 2008.
7. Correct password security measures in OCC's systems to meet policy requirements.	Completed March 3, 2008.
8. Improve user awareness training on e-mail security, phishing, and incident reporting.	Actions to improve user awareness taken by March 31, 2008; user awareness training is ongoing.
9. Ensure that appropriate wireless access restrictions exist.	We took a two-pronged approach to this recommendation. First, we undertook a training initiative for users that was completed by March 31. Second, we will push a software driver to all laptops by June 30, 2008 that will prevent unauthorized wireless access while connected to the OCC network.
10. Ensure OCC users are trained on the security risks of connecting to unapproved or unknown wireless networks.	Actions to improve user awareness taken by March 31, 2008; user awareness training is ongoing.

-3-

Appendix 3
Major Contributors

Office of Information Technology Audits

Louis C. King, Former Director
Tram J. Dang, Acting Director
Gerald J. Steere, IT Specialist (Lead)
Abdirahman M. Salah, IT Specialist
Kenneth Harness, Referencer

Appendix 4
Distribution List

Office of the Comptroller of the Currency

Chief Information Officer

Department of the Treasury

Office of Accounting and Internal Control
Office of Strategic Planning and Performance Management
Office of Chief Information Officer

Office of Management and Budget

Office of Inspector General Budget Examiner