May 19, 2010

DEBORAH J. JUDY
DIRECTOR, INFORMATION TECHNOLOGY OPERATIONS

CHARLES L. MCGANN, JR.
MANAGER, CORPORATE INFORMATION SECURITY

SUBJECT: Audit Report – Modem Security at the [redacted] (Report Number IS-AR-10-009)

This report presents the results of our self-initiated audit of modem security at the [redacted] (Project Number 10RG013IT000). Our objective was to determine whether controls over modems are adequate to protect information resources at the [redacted] This audit addresses operational risk. See Appendix A for additional information about this audit.

Modem security is essential to preserve the integrity and confidentiality of the U.S. Postal Service network. Policy[1] prohibits accessing the intranet via a modem without the explicit approval of the manager, Corporate Information Security Office Information Security Services. Unsecure or unauthorized modems may provide malicious users undetected access to Postal Service information resources.

Conclusion

Security controls over modems are adequate to protect information resources at the [redacted]. Using security software, we scanned 4,906 telephone numbers dedicated to the [redacted] and identified five modems. We were unable to penetrate these modems to gain access to information resources on the Postal Service network. However, management can improve controls over modems by performing required modem security assessments and properly accounting for modems.

[1] Handbook AS-805, *Information Security,* Section 5-5, Prohibited Uses of Information Resources, dated November 2009.

Modem Security Assessments

Management is not performing modem security assessments at the [redacted]. This occurred because management viewed the assessments as a lower priority to other assessments including payment card industry scans and certifications and accreditations. Administrators last performed an assessment of the [redacted] in September 2007. Postal Service policy requires protection of the network infrastructure through vulnerability scans, penetration testing, and assessments.[2] By performing modem security assessments, management can reduce the risk associated with unauthorized or incorrectly configured modems that could provide malicious users with unauthorized – and potentially undetected – access to Postal Service information resources.

We recommend the manager, Corporate Information Security, direct the manager, National Information System Security, to:

1. Periodically identify and assess modems at the [redacted] and communicate the results to the manager, Telecommunication Services.

Modem Accountability

Management does not maintain an asset inventory of modems. Policy[3] requires management to maintain an accurate inventory of modems to identify unauthorized modems. This occurred because Postal Service management was relying on contract service providers to properly account for the modems.[4] Unauthorized modems could provide users unintended – and potentially undetected – access to networked information resources.

We recommend the director, Information Technology Operations, direct the manager, Telecommunication Services, to:

2. Inventory and account for all modems installed at the [redacted]

3. Use the security assessment results to reconcile modem inventories and identify and remove unauthorized modems from the network.

[2] Handbook AS-805, Section 11-1.2 (i), Network Infrastructure.
[3] Handbook AS-805, Section 11-3.2, Maintaining Network Asset Control.
[4] Management could not readily identify whether they approved the use of these modems and the applicable contracts did not mention the modems. If management did approve the modems, they did so as part of a larger network configuration.

Management's Comments

Management agreed with the recommendations. In response to recommendation 1, National Information System Security will perform annual vulnerability assessments of all identified modems within the infrastructure and communicate these results to the manager, Telecommunication Services. Moreover, they will report unregistered modems to the Computer Incident Response Team. In response to recommendations 2 and 3, Telecommunication Services will reconcile and maintain an approved inventory of modems. Additionally, they will review modem inventories and remove unauthorized modems from the network.

The target completion date for recommendations 1 and 3 is September 30, 2010. The target completion date for recommendation 2 is June 1, 2010. See Appendix B for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and management's corrective actions should resolve the issues identified in the report.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Frances E. Cain, director, Information Technology, or me at 703-248-2100.

E-Signed by Darrell E. Benjamin, Jr
VERIFY authenticity with ApproveIt

Darrell E. Benjamin, Jr.
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: Ross Philo
Charles L. McGann
Raymond J. Iandolo
Larry K. Wills
Sally K. Haring

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

The [redacted] provides network infrastructure services to Postal Service business units at over 38,000 sites. Telecommunication Services is responsible for providing the Postal Service with voice and data communications. Corporate Information Security is responsible for ensuring Postal Service information resources operate in a secure and trusted environment.

Modems are devices that transmit data over telephone wires by modulating data into an audio signal to send information and demodulating an audio signal into data to receive the information. Modem security is essential to ensure the confidentiality and integrity of information resources. Postal Service policy prohibits accessing the intranet via modems without explicit approval of the manager, Corporate Information Security Office Information Security Services. Malicious users typically implement war dialing[5] to locate vulnerable modems and manipulate them to access the network. The presence of unsecure or unapproved modems attached to systems can provide users undetected and unauthorized access to information resources. PhoneSweep® is a security audit tool used to identify security risks such as unsecure modems within a predefined range of telephone numbers.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether controls over modems are adequate to protect information resources at the [redacted] To achieve our objective, we obtained a list of 4,906 telephone numbers dedicated to the [redacted] From March 4 to 8, 2010, we used PhoneSweep to assess these telephone numbers to identify active modems. Using manual and automated techniques, we attempted to penetrate the identified modems to determine whether the devices grant unauthorized access to Postal Service information resources. We interviewed key officials and reviewed applicable Postal Service policies, standards, and procedures.

We conducted this performance audit from February through May 2010 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. In addition, we used manual and automated techniques to analyze computer-processed data and concluded the data were sufficiently reliable to meet the report objective. We discussed our observations

[5] War dialing is a computer program used to identify telephone numbers that can successfully make a connection with a computer modem.

and conclusions with management officials on April 30, 2010, and included their comments where appropriate.

PRIOR AUDIT COVERAGE

Report Title	Report Number	Final Report Date
PhoneSweep Security Assessment at the [redacted] Information Technology and Accounting Service Center	IS-CS-08-002	9/22/2008
PhoneSweep Security Assessment at [redacted] Information Technology and Accounting Service Center	IS-CS-08-003	9/22/2008

The reports listed above were issued as technical reports and, therefore, did not contain formal recommendations. Instead, we urged system administrators to review and use the detailed information in the reports as tools to assist in establishing priorities for corrective action, and implementing repairs as necessary. Both reports noted management did not maintain a current inventory of modems.

APPENDIX B. MANAGEMENT COMMENTS

UNITED STATES POSTAL SERVICE

May 17, 2010

Lucine M. Willis
Director, Audit Operations
Office of Inspector General
1735 N. Lynn Street, Room 11044
Arlington, VA 22209-2020

SUBJECT: Transmittal of Draft Audit Report – Modem Security at the [redacted] (Report Number IS-AR-10-DRAFT), Project Number 10RG013IT000

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with recommendations 1 through 3 of the report; the response is attached.

[redacted]

If you have any questions or comments regarding this response, please contact Gerri Wallace, Corporate Information Security at (202) 268-6821.

Deborah J. Judy
Director, IT Operations

Attachment

cc: Ross Philo
Larry K. Wills
Charles L. McGann
Raymond J. Iandolo
Sally K. Haring

475 L'Enfant Plaza SW
Washington DC 20260

We recommend the manager, Corporate Information Security; direct the manager, National Information System Security, to:

1. Periodically identify and assess modems at the [redacted] and communicate the results to the manager, Telecommunication Services.

Management agrees with the recommendation and the manager, Corporate Information Security Office (CISO) will direct the manager, Information System Security (ISS) to perform security vulnerability testing on all identified modems within the USPS infrastructure on a yearly basis and communicate results to the manager, Telecommunications Services. This assumes that all modems have been registered and inventoried with Telecommunication Services, as required by policy, and any unregistered modems detected will result in an incident being reported to USPSCIRT.

Anticipated completion date: September 30, 2010

We recommend the director, Information Technology Operations; direct the manager, Telecommunication Services, to:

2. Use the security assessment results to reconcile modem inventories and identify and remove unauthorized modems from the network.

   Management agrees with the recommendation and the manager, Telecommunication Services will keep the approved inventory on the local file and print server. This effort will be completed by June 1, 2010.

   Anticipated completion date: Requesting closure upon receipt of this response.

We recommend the director, Information Technology Operations; direct the manager, Telecommunication Services, to:

3. Inventory and account for all modems installed at the [redacted]

   Management agrees with the recommendation and the manager, Telecommunications Services will review the inventories provided by CISO and remove any unauthorized modems from the network.

   Anticipated completion date: September 30, 2010