OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Internet-Facing Devices

Audit Report

Report Number
IT-AR-17-001

November 3, 2016

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

Our objective was to identify Internet-facing hosts connected to the Postal Service network and determine if a complete inventory exists.

Background

A complete inventory of Internet-facing devices (hosts) is essential for information system security. Internet-facing hosts are entry points that are typically the most attacked hosts on an organization's network. An inventory of these hosts and their associated Internet Protocol addresses provides visibility into and control over an organization's information systems.

During fiscal year 2015, the U.S. Postal Service's USPS.com website – an Internet-facing host – had an average of 3 million daily visits from customers, resulting in more than 50 million transactions that generated over $1 billion in revenue. In addition, over 493,000 Postal Service employees use web-based (Internet-facing) hosts for Human Resources transactions such as enrolling in direct deposit or changing retirement contributions or tax withholdings. Accordingly, it is critical for the Postal Service to be aware of and monitor its Internet-facing hosts and restrict visibility to reduce the risk of unauthorized access to data and disruption of critical operations.

Our objective was to identify Internet-facing hosts connected to the Postal Service network and determine if a complete inventory exists.

What the OIG Found

The Postal Service does not have a complete inventory of Internet-facing hosts. While management has a process to identify the host name and Internet Protocol address, the process does not capture other key data elements such as system owner, operating system, and location. The lack of a complete inventory prevents an organization from maintaining visibility and control over its Internet-facing hosts.

In addition, management does not update firewall rules when configuration changes are made to Internet-facing hosts. Specifically, we identified [redacted] of [redacted] firewall rules ([redacted] percent) that allowed unnecessary traffic to Internet-facing hosts.

We further identified firewall rules that allow [redacted] of [redacted] hosts ([redacted] percent) to respond to potentially inappropriate communication requests. [redacted]

These issues occurred because instead of scanning the entire network to identify Internet-facing hosts, management relied on scans of known Internet-facing hosts used to support their vulnerability assessment process. In addition, cybersecurity

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

managers did not document all data elements because the information is contained in many non-integrated systems.

Finally, management does not have an effective process for updating firewall rules when configuration changes are made and services are no longer required on a host.

Obsolete firewall rules that allow inappropriate traffic to Internet-facing hosts weaken the Postal Service's security posture by allowing outsiders to discover entry points into the network. This significantly hinders the Postal Service's ability to detect and recover from security incidents and increases the risk of unauthorized access to data and disruption of critical operations.

What the OIG Recommended

We recommended management update procedures to require a complete centralized inventory of Internet-facing hosts be documented and maintained; develop a report that allows managers to review the inventory of Internet-facing hosts; and review and enhance standard operating procedures to include an escalation process to resolve any data gaps in the Internet-facing host inventory. We also recommended management complete enumeration scans of the entire network on a regular basis; review and enhance procedures for updating firewall rules to reflect configuration changes made to Internet-facing hosts; and review firewall rules to determine if the services and traffic to Internet-facing hosts are appropriate.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

November 3, 2016

MEMORANDUM FOR: GREGORY S. CRABB
ACTING CHIEF INFORMATION OFFICER AND DIGITAL SOLUTIONS EXECUTIVE VICE PRESIDENT

JEFFREY C. JOHNSON
VICE PRESIDENT, INFORMATION TECHNOLOGY

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskt

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology

SUBJECT: Audit Report – Internet-Facing Devices
(Report Number IT-AR-17-001)

This report presents the results of our audit of the U.S. Postal Service's Internet-Facing Devices (Project Number 16TG015IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

A complete inventory of Internet-facing hosts is essential for information system security. Internet-facing hosts are typically the most attacked hosts on an organization's network; therefore, organizations should identify these hosts and secure them and their supporting network infrastructure.

Introduction

This report presents the results of our audit of the U.S. Postal Service's Internet-facing devices (hosts) (Project Number 16TG015IT000). Our objective was to identify Internet-facing hosts connected to the Postal Service network and determine if a compete inventory exists. See Appendix A for additional information about this audit.

A complete inventory of Internet-facing hosts is essential for information system security. Internet-facing hosts are typically the most attacked hosts on an organization's network; therefore, organizations should identify these hosts and secure them and their supporting network infrastructure.

During fiscal year 2015, the USPS.com website – an Internet-facing host – had an average of 3 million daily visits from customers, resulting in over 50 million transactions that generated more than $1 billion in revenue. In addition, over 493,000 Postal Service employees use web-based (Internet-facing) hosts for Human Resources transactions that involve sensitive data such as enrolling in direct deposit or changing retirement contributions and tax withholdings. It is vital for the Postal Service to be aware of and monitor its Internet-facing hosts and restrict visibility to reduce the risk of unauthorized access to data and disruption of critical operations.

Summary

The Postal Service does not have a complete inventory of Internet-facing hosts. While management has a process to identify the Internet Protocol (IP) address and host name, it does not capture other key data elements such as system owner, operating system, and location. In addition, management does not update its firewall rules when configuration changes are made to Internet-facing hosts. Specifically, we found that [redacted] out of [redacted] firewall rules [redacted] percent) allowed unnecessary traffic to Internet-facing hosts.

We also identified firewall rules that allow [redacted] of [redacted] hosts ([redacted] percent) to respond to potential inappropriate communication requests. [redacted]

These occurred because the Postal Service relies on scan results used to support its vulnerability assessment process to identify Internet-facing hosts. This process does not provide an official inventory because it does not capture key data elements such as the physical location of the host and system administrator and may not detect all hosts on the entire Postal Service network. Additionally, management does not have an effective process for updating firewall rules when configuration changes are made and services are no longer required on a host.

Obsolete firewall rules that allow inappropriate traffic to Internet-facing hosts and hosts that are not properly configured could enable outsiders to discover entry points to the network. This weakens the Postal Service's security posture by increasing the risk of unauthorized access to data and disruption of critical operations.

Inventory Process

The Postal Service does not maintain a complete inventory of Internet-facing hosts connected to its network. While management has a process to identify the IP address and host name, it does not provide other key inventory data. According to best practices,[1] a complete inventory allows an organization greater visibility into and control over its Internet-facing hosts and should contain the following data elements:

- Unique identifier and/or serial number
- Role of information system (e.g., server, desktop, application)
- Operating system type and version/service pack level
- Physical location
- Primary and secondary administrators
- Owner and primary user

These issues occurred because instead of scanning the entire network to identify Internet-facing hosts, management relied on scans of known Internet-facing hosts used to support their vulnerability assessment process. These scans are not a complete inventory because they do not capture all information and may not detect all hosts on the entire Postal Service network. Additionally, cybersecurity managers stated they did not document all data elements — such as system administrator and location — because the information is in many non-integrated systems.[2] Furthermore, policy does not clearly define the roles, responsibilities, and processes for identifying, managing, and maintaining Internet-facing hosts.

An incomplete inventory of Internet-facing hosts increases the risk of unauthorized connectivity to the Postal Service network. A complete Internet-facing host inventory would increase the Postal Service's ability to quickly detect cybersecurity incidents.

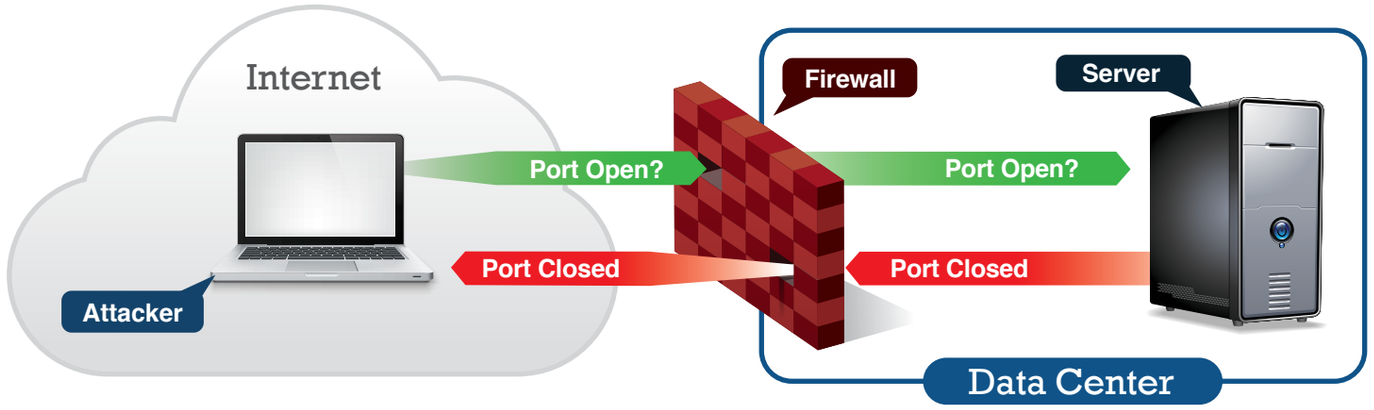
Authorization and Approval Process

During our enumeration[3] scanning, we identified [redacted] of [redacted] firewall rules ([redacted] percent) that allow traffic to a closed port on the host, indicating the firewall did not filter unnecessary traffic. Closed ports indicate that no services are running on the port, but the

1 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-128, *Guide for Security- Focused Configuration Management of Information Systems*, Section 3.1.2, August 2011.
2 Enterprise Information Repository, Internet Protocol Address Management.
3 Enumeration is a method used to identify devices on a network with the goal to discover possible points of entry to the network. In contrast, vulnerability scanning is intended to identify weaknesses in security configurations.

firewall allows the connection to go through from the Internet to the host. [redacted] (see Figure 1).

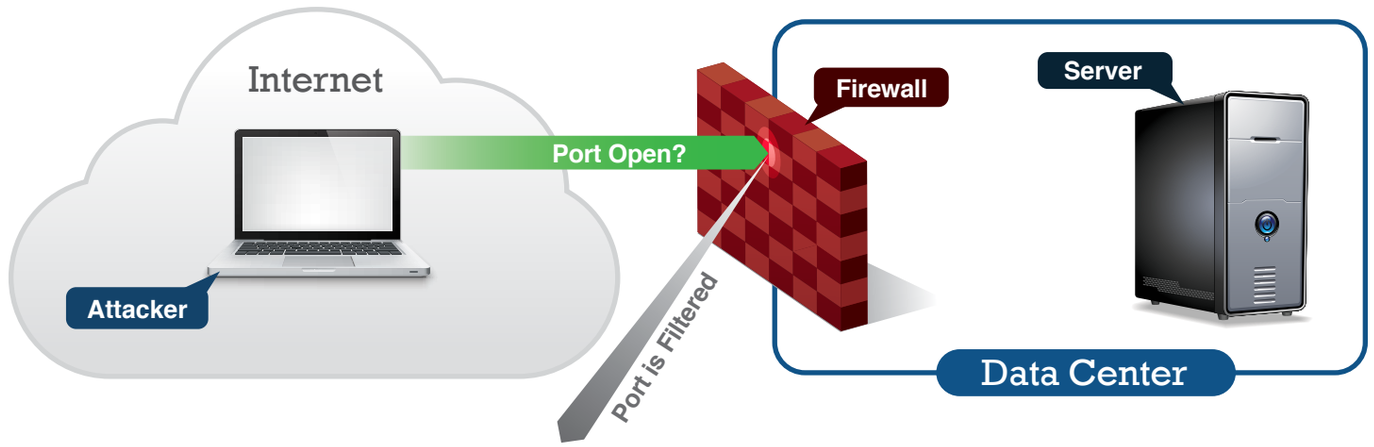
Figure 1. Misconfigured Firewall Allowing Unnecessary Traffic to Host



Source: Source: U.S. Postal Service Office of Inspector General (OIG) illustration of firewall configuration based on analysis of enumeration data.

Filtered[4] ports indicate a firewall prevents probing of closed ports. Postal Service hardening standards[5] and industry best practices[6] state that firewall rules should only allow necessary network traffic (see Figure 2).

Figure 2. Properly Configured Firewall That Does Not Allow Traffic to Host with Closed Ports



Source: OIG illustration of firewall configuration based on analysis of enumeration data.

This occurred because management does not have an effective change management process for updating firewall rules when configuration changes are made to Internet-facing hosts. Specifically, when a host system owner submits a change request to close an active port on an Internet-facing host, the system administrator will make the configuration change; however, the request is not forwarded to the Network Connectivity Review Board[7] (NCRB) to ensure that corresponding firewall rules are updated. A change

4 Filtered ports indicate a firewall is present, and prevents probing of open or closed ports.
5 [redacted]
6 NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, Section 4 Firewall Policy, dated September 2009.
7 NCRB is responsible for developing system connectivity requirements for Postal Service connections to external systems, externally facing applications, and connections via the Internet.

management process that does not include changes to both host and firewall rules significantly impacts the Postal Service's network security posture, which increases the risk of unauthorized access to data and disruption of critical operations.

Internet Control Messaging Protocol

We identified [redacted] of [redacted] Internet-facing hosts [redacted] percent) that respond to Internet Control Messaging Protocol (ICMP) due to outdated firewall configuration settings. Hosts use ICMP to communicate updates or error information to other hosts. According to industry best practices,[8] ICMP should not be allowed through Internet-facing firewalls because these requests can identify and discover hosts on the network. [redacted]

The firewall configuration settings were outdated because management developed current firewall rules based on a legacy firewall environment and did not review rules to determine if traffic was still necessary when the environment changed. Because obsolete firewall rules can allow inappropriate traffic to Internet-facing hosts, outsiders might discover entry points on the network.

During our audit, management began reviewing the [redacted] firewall rules and submitting change requests to remove any rules deemed unnecessary. Management expects to complete the review and necessary firewall updates by December 31, 2016.

8 SANS Institute, *Methodology for Firewall Reviews for PCI Compliance*, March 2013.

Recommendations

We recommend management update procedures to require a complete centralized inventory of Internet-facing hosts be documented and maintained; and define the roles, responsibilities, and processes for identifying, managing, and maintaining Internet-facing hosts.

We recommend the vice president, Information Technology, and acting chief information security officer and vice president, Digital Solutions, direct the managers, Enterprise Access Infrastructure and Cybersecurity Engineering, to:

1. Update procedures to require a complete centralized inventory of Internet-facing hosts be documented and maintained; and define the roles, responsibilities, and processes for identifying, managing, and maintaining Internet-facing hosts.

We recommend the vice president, Information Technology, and acting chief information security officer and vice president, Digital Solutions, direct the managers, Enterprise Access Infrastructure and Cybersecurity Engineering, to:

2. Develop a report for management to review the inventory of Internet-facing hosts. In addition, review and enhance standard operating procedures to include an escalation process to resolve any data gaps in the Internet-facing host inventory.

We recommend the acting chief information security officer and vice president, Digital Solutions, direct the manager, Cybersecurity Risk, to:

3. Complete enumeration scans of the entire Postal Service network on a regular basis.

We recommend the vice president, Information Technology, direct the manager, Enterprise Access Infrastructure, to:

4. Review and enhance the process for updating firewall rules to reflect configuration changes made to Internet-facing hosts; and review firewall rules to determine if the service and traffic to Internet-facing hosts are appropriate.

We recommend the vice president, Information Technology, direct the manager, Enterprise Access Infrastructure, to:

5. Continue reviewing current firewall rules to determine if Internet control messaging protocol traffic should be allowed from the Internet and remove any deemed unnecessary.

Management's Comments

Management agreed with all of the findings and recommendations in the report. See Appendix B for management's comments in their entirety.

Regarding recommendation 1, management stated they are enhancing standard operating procedures in order to produce a complete report of Internet-facing devices. The target implementation date is December 15, 2016.

Regarding recommendation 2, management stated they have begun to develop standard operating procedures to include the escalation process to resolve any data gaps in the inventory of Internet-facing devices. The target implementation date is December 15, 2016.

Regarding recommendation 3, management stated they currently execute enumeration scans on a bi-weekly basis and have partnered with the Department of Homeland Security (DHS) National Cybersecurity Assessment and Technical Services (NCATS) Cyber Hygiene Program to perform enumeration scans. Management stated they have received the results of initial DHS scans of the entire Postal Service network and request this recommendation to be closed upon issuance of the report.

Regarding recommendation 4, management stated they have updated standard operating procedures for more in-depth quarterly firewall configuration reviews and governance of the current process. The target implementation date is December 15, 2016.

Regarding recommendation 5, management stated they have begun remediation activities and plan to perform scans to confirm closure of unnecessary connections and continue periodic reviews for any unnecessary connections. The target implementation date is January 30, 2017

Evaluation of Management's Comments

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

Management requested closure of recommendation 3 with issuance of the report; however, the OIG needs a copy of the completed DHS scans of the entire Postal Service network before closing this recommendation. As stated in the report, we disagree that the bi-weekly scans the Postal Service conducted address the recommendation to scan the entire network rather than a subset of the network.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

Click on the appendix title to the right to navigate to the section content.

Appendix A: Additional Information

Background

Cyber attacks on government networks are growing more sophisticated, frequent, and dynamic. It is paramount that organizations protect networks, systems, and information from unauthorized access or disruption while continuing to provide essential services to the public and protect customer and employee data. Identification and discovery of hosts on a network are initial steps attackers use to exploit vulnerabilities. Internet-facing hosts are typically the most attacked hosts on an organization's network; therefore, it is important for the Postal Service to identify these hosts and secure them and their supporting network infrastructure.

Network enumeration is the process used to identify and discover network hosts. Attackers also use this process to gain unauthorized access to a network to exploit existing vulnerabilities such as hosts without security updates.

The Postal Service is implementing multiple strategic programs to improve its cyber security posture. The *CyberSecurity Decision Analysis Report* (DAR II) improved the Postal Service's ability to prevent, detect, and respond to cyber-related events. It will also help execute strategic activities such as:

- Enhancing security by following a consistent change and configuration management process, and monitoring the network continuously to identify potential abnormal activity.
- Improving host security through the development and implementation of processes that ensure threats are proactively identified, vulnerabilities are remediated timely, and events are logged and analyzed appropriately.

Through collaboration with the DHS, the Postal Service also participates in the Continuous Diagnostics Mitigation (CDM) and National Cyber Security Assessment & Technical Services (NCATS) Cyber Hygiene programs. The CDM program provides the Postal Service with capabilities and tools that identify, prioritize and mitigate cybersecurity risks on an ongoing basis. In addition, the April 2016 implementation of the NCATS improves the Postal Service's security posture by proactively identifying and reporting on vulnerabilities and configuration issues present on Internet-facing hosts before those vulnerabilities can be exploited by a malicious third party.

Objective, Scope, and Methodology

Our objective was to identify Internet-facing hosts connected to the Postal Service network and determine if a complete inventory exists. We performed our scans from April 25 through June 21, 2016. The scope of our scans included using the Nmap[9] scanning tool to scan 21 open Transmission Control Protocol (TCP)[10] ports (see Table 1) and identify hosts connected to the Postal Service (56.0.0.0/8) network.

To accomplish our objective, we:

- Documented the enumeration scan objective, scope, methodology, and approval to scan the Postal Service network.
- Conducted enumeration scans of the Postal Service network to identify Internet-facing hosts.
- Reviewed Postal Service policies, procedures, and standards related to managing and supporting Internet-facing hosts; and interviewed key officials from the Chief Information Security Office and Information Technology to gain an understanding of the processes.

9 A security scanner used to discover hosts and services on a computer network.
10 Basic communication language or protocol of the Internet.

- Obtained Postal Service discovery scan data to review and assess sufficiency against industry best practices for inventory management.
- Analyzed enumeration scan output and performed root cause analysis by interviewing key Postal Service officials.

Table 1 identifies the [redacted] ports judgmentally selected for scanning to identify hosts connected to the [redacted]

Table 1. TCP Ports

Port Number	Port Name	Port Description
[redacted]		

Source: www.adminsub.net, www.speedguide.net, www.techopedia.com, www.wikipedia.com.

We conducted this performance audit from March through November 2016, 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on September 28, 2016, and included their comments where appropriate.

We assessed the reliability of enumeration scan results by comparing it with key data elements stated and agreed to in the test plan. Additionally, we performed a limited validation test by examining IP addresses and their associated ports. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
U.S. Postal Service Cybersecurity Functions	To determine whether at the time the cyber intrusion was identified, the Postal Service's cybersecurity functions aligned with industry best practices for determining whether the structure, operations, and resourcing effectively support the enterprise.	IT-AR-15-008	7/17/2015	None

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

October 28, 2016

LORI LAU DILLARD
Director, Audit Operations

SUBJECT: Response to Draft Report: Internet-Facing Devices (IT-AR-17-DRAFT)
Project Number 16TG0151T000

Thank you for the opportunity to review and comment on the subject draft audit report. Management understands the intent of the draft report is to help improve the overall posture and capabilities of the U.S. Postal Service (USPS) to enhance their cybersecurity processes.

Protecting the privacy of customer, employee, supplier and Postal Service information has been and always will be a priority for the Postal Service. USPS takes the protection of its systems and data very seriously and has been implementing a robust cybersecurity transformation program to further enhance existing technologies, policies and procedures.

To combat cybersecurity threats, the Postal Service is investing in additional resources to strengthen cybersecurity strategies, policies and risk management frameworks. Furthermore, USPS is rigorously developing and improving capabilities to provide network visibility, better performance and efficient management of information systems as part of its current efforts under Initiative #6 (Application, Host and Network Security) and Initiative #14 (Asset, Change and Configuration Management), in addition to the Vulnerability Assessment team that was operational prior to this audit.

The Postal Service is aware of the risks and vulnerabilities associated with Internet-facing hosts and already had resources dedicated to the monitoring and reporting of these hosts prior to the initiation of this audit through initiatives #6 & #14. USPS has always taken Internet-facing security seriously, as evidenced by the following activities:

1. Enforcing AS-805 policies for enterprise software inventory management
2. Storing the data elements for Internet-facing devices in multiple repositories to eliminate the potential of a single point of failure and reduce cyber risks as the maintenance of a single repository could create a system/database that may be highly targeted by attackers
3. Performing enumeration scans across all Internet-facing devices twice a week using industry-leading software tools designed for scanning Internet-facing hosts from an external network perspective

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260
WWW.USPS.COM

4. Partnering with the Department of Homeland Security National Cybersecurity Assessment and Technical Services (NCATS) Cyber Hygiene program since March of 2016:
    a. The Cyber Hygiene Program performs vulnerability scans and tracks mitigation and Common Vulnerability Scoring System (CVSS) scored risks over time
    b. Using USPS software, in combination with externally-hosted cloud software, and DHS security efforts help ensure that USPS minimizes risk. This includes risks that occur by having a single source of information to work from and having several vantage points to obtain information, which has served to mature network perimeter response efforts for continuous remediation and improvement
5. Continuing to strengthen that already robust process for updating firewall rules and documenting configuration changes via the Network Connectivity Review Board (NCRB), which reviews and approves any changes to Internet-facing device firewalls

The combination of these efforts between the USPS Corporate Information Security Office (CISO) and Information Technology (IT) and partnering with DHS help USPS ensure that protection and security of information maintains a priority, and as attacks in the cyber landscape continue to advance, USPS will improve its security posture to continue the defense against ongoing threats.

Recommendation [1]:
Update procedures to require a complete centralized inventory of Internet-facing hosts be documented and maintained; and define the roles, responsibilities and processes for identifying, managing and maintaining Internet-facing hosts.

Management Response/Action Plan:
Management agrees with the intent of the recommendation to always be able to view an inventory of Internet-facing devices and the procedures for this should be documented to include defined roles, responsibilities and processes for maintaining Internet-facing hosts. Management does not agree at this time that a centralized inventory is required as long as a report with this information can be accurately and timely produced. The Postal Service is currently able to produce a report that inventories Internet-facing devices and addresses over 85 percent of the data elements the OIG has highlighted. The USPS is enhancing standard operating procedures maintenance of the inventory in order to produce a report with 100 percent of the data elements consistently captured.

Target Implementation Date:
December 15, 2016

Responsible Official:
Vice President, Information Technology
(A) Vice President, Chief Information Security Officer & Digital Solutions
Manager, Enterprise Access Infrastructure
Manager, Cybersecurity Engineering

Recommendation [2]:
Develop a report for management to review the inventory of Internet-facing hosts. In addition, review and enhance standard operating procedures to include an escalation process to resolve any data gaps in the Internet-facing host inventory.

Management Response/Action Plan:
As noted in the Recommendation and Management Response for #1, Management agrees with the development of a report and standard operating procedure (SOP) and has already started the process of making these updates. The recommendation to review and enhance the standard operating procedures to include an escalation process to resolve any data gaps in the Internet-facing host inventory will be included in the combined remediation for recommendations #1 and #2.

Target Implementation Date:
December 15, 2016

Responsible Official:
Vice President, Information Technology
(A) Vice President, Chief Information Security Officer & Digital Solutions
Manager, Enterprise Access Infrastructure
Manager, Cybersecurity Engineering

Recommendation [3]:
Complete enumeration scans of the entire Postal Service network on a regular basis.

Management Response/Action Plan:
Management agrees with the intent of this recommendation and understands the importance of completing enumeration scans of the Postal Service network on a regular basis. The USPS already executes enumeration scans on a bi-weekly (two times a week) basis and partners with the Department of Homeland Security (DHS) National Cybersecurity Assessment and Technical Services (NCATS) Cyber Hygiene Program, which performs vulnerability scanning as well.
Management requests the closure of this recommendation upon issuance of the final report as the USPS performs enumeration scans regularly and DHS has completed its scan of the entire USPS network.

Target Implementation Date:
N/A

Responsible Official:
(A) Vice President, Chief Information Security Officer & Digital Solutions
Manager, Cybersecurity Risk

Recommendation [4]:
Review and enhance the process for updating firewall rules to reflect configuration changes made to Internet-facing hosts; and review firewall rules to determine if the service and traffic to Internet-facing hosts are appropriate.

Management Response/Action Plan:
Management agrees with this recommendation and has already updated the standard operating procedure (SOP) for quarterly firewall configuration reviews to allow for a more in-depth, recurrent review and governance of the current process. Management agrees that reviews and enhancements to SOPs for updating firewall rules will further strengthen an already comprehensive process. The Network Connectivity Review Board (NCRB) reviews and approves any changes to Internet-facing devices prior to any implementation of changes. The Network Perimeter team also does an annual review of the firewall reviews.

Target Implementation Date:
December 15, 2016

Responsible Official:
Vice President, Information Technology
Manager, Enterprise Access Infrastructure

Recommendation [5]:
Continue reviewing current firewall rules to determine if internet control messaging protocol (ICMP) traffic should be allowed from the Internet and remove any deemed unnecessary.

Management Response/Action Plan:
Management agrees with this recommendation and has already initiated remediation activities.
Management is planning to perform scans to confirm closure of unnecessary ICMP connections and will continue to review periodically for any additional unnecessary connections.

Target Implementation Date:
January 30, 2017

Responsible Official:
Vice President, Information Technology
Manager, Enterprise Access Infrastructure

Gregory S. Crabb
Acting Chief Information Security Officer
and Digital Solutions Vice President

Jeffrey C. Johnson
Vice President, Information Technology

cc: *Manager, Corporate Audit Response Management*

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100