UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

Office of the
Inspector General

October 13, 2016

MEMORANDUM FOR BETH F. CORBERT
Acting Director

FROM: NORBERT E. VINT
Deputy Inspector General

Norbert E. Vint

SUBJECT: Web Application Security Review (Report No. 4A-CI-00-16-061)

The purpose of this memorandum is to communicate to you the results from our review of the U.S. Office of Personnel Management's (OPM) security controls surrounding public facing web applications. We submitted a draft copy of our conclusions and recommendations to OPM's Office of the Chief Information Officer (OCIO) representatives to elicit their comments. The OCIO's comments on the draft memorandum were considered in preparing the final report and are attached as an Appendix to this report.

Executive Summary

Our review determined that there are multiple opportunities for improvement regarding the policies, procedures, and controls surrounding OPM's web applications that face the public Internet. OPM does not maintain an adequate inventory of web applications or have policies and procedures specific to web application development or security. In addition, OPM has not historically conducted web application vulnerability scans, and the scans conducted by the Office of the Inspector General (OIG) during this engagement discovered multiple vulnerabilities in OPM's web applications and the servers hosting those applications.

As a result, we recommend that OPM create a formal web application inventory, create or enhance policies and procedures to address web application development and security, and implement a comprehensive web application vulnerability scanning program.

Background

The OPM OIG volunteered to participate in a government-wide project to examine the controls used to manage and secure the Federal government's publicly accessible web applications. This project was led by the Council of Inspectors General on Integrity and Efficiency. The three main objectives of the review were to: 1) develop a scope and methodology for conducting a review of Federal agency public Internet facing web applications, 2) determine the extent and efficiency of agencies' efforts to identify and assess vulnerabilities on publicly accessible web applications and mitigate the most severe vulnerabilities, and 3) assess efforts to control or reduce the number of publicly accessible web applications and services.

Scope and Methodology

The scope of this review included OPM's publicly accessible web applications that met the criteria defined by the U.S. Office of Management and Budget's Memorandum M-15-13, which states that "Publicly-accessible websites and services are defined here as online resources and services available over HTTP or HTTPS over the public Internet that are maintained in whole or in part by the Federal Government and operated by an agency, contractor, or other organization on behalf of the agency."

We evaluated the accuracy and completeness of OPM's web application inventory using our existing knowledge of the OPM network environment and through the use of automated scanning tools connected to the OPM network. We then performed vulnerability scans on a sample of public facing web applications and the computer servers hosting those applications, and compared these results to historical vulnerability scans run by OPM's security operations team.[1] We also interviewed OPM subject matter experts to determine what policies and procedures are in place to develop and secure OPM's web applications.

Our review was not conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). The nature and scope of the work performed was consistent with that expected of a GAGAS audit; however, because we consider this to be a limited-scope review and not an audit, the documentation, reporting, and quality control standards are not as stringent.

Review Results

Our review indicated that OPM could improve its web application security program in several areas, as described in the sections below.

A. Web Application Inventory

OPM does not maintain an adequate inventory of web applications. OPM's OCIO has developed an inventory of servers, databases, and network devices, but the inventory does not identify the purpose, role, or owner of each device. At the beginning of this review, we

[1] Throughout this report, the term "server" refers to the computer hardware and the operating system (e.g., Windows) that hosts web applications.

requested an inventory of OPM's public facing web applications and were informed that a formal inventory did not exist. We proceeded to work collaboratively with representatives from the OCIO to determine how many public facing web applications exist in OPM's network environment, where the applications reside, who owns the programming code, and where the data used by the web application is located. While we were eventually able to collect enough information about OPM's public facing web applications to proceed with this review, it is clear that OPM does not have a centralized process to track or monitor web applications.

The National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 4, requires organizations to develop and document an inventory of information system components that accurately reflects the current information system, includes all components within the authorization boundary, and includes the information necessary for information system component accountability.

Failure to maintain an adequate inventory of web applications increases the risk that applications could exist in OPM's network environment without the OCIO's knowledge, which could result in these applications not being scanned, patched, and monitored as part of the OCIO's continuous monitoring program.

Recommendation 1

We recommend that OPM create a formal and comprehensive inventory of web applications. The inventory should identify which applications are public facing and contain personally identifiable information or sensitive agency information, identify the application owner, and itemize all system interfaces with the web application.

OCIO Response:

"OCIO concurs with the recommendation. The web team will work with application owners to update the inventory of web applications and maintain relevant inventory data on these applications."

OIG Comment:

As part of the audit resolution process, we recommend that the OCIO provide evidence to OPM's Internal Oversight and Compliance office that it has fully implemented this recommendation. This statement applies to all subsequent audit recommendations that the OCIO agrees to implement.

B. Policies and Procedures

OPM maintains information technology (IT) security policies and procedures that address NIST SP 800-53 security controls. OPM also maintains system development policies and standards. While these policies, procedures, and standards apply to all IT assets, they are written at a high level and do not address some critical areas specific to web application security and development. Specifically, the following policy related documents either do not exist or do not adequately address web applications:

- Procedures or standards for hardening web server operating systems (e.g., documented configuration security standards and configuration baselines); and
- Procedures or standards for secure design and coding of web-based applications.

NIST SP 800-53, Revision 4, provides criteria and guidance that Federal agencies must follow regarding hardening web server operating systems and secure design and coding of web applications. Control CM-6, Configuration Settings, states that organizations must establish and document configuration settings for information technology products using security configuration checklists that reflect the most restrictive mode consistent with operational requirements. "Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system." Control SA-8, Security Engineering Principles, states that organizations must apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system. "Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions."

Failure to establish adequate guidance related to hardening web server operating systems and the secure design and coding of web applications increases the risk that web applications and the servers that host them could contain weaknesses that could be exploited by an adversary.

Recommendation 2

We recommend that OPM create or update its policies and procedures to provide guidance specific to the hardening of web server operating systems and the secure design and coding of web-based applications.

OCIO Response:

"OCIO concurs with the recommendation. The Office of the Chief Information Security Officer (OCISO) will incorporate requirements specifically associated with the hardening of web based applications and host operating systems into the policies and associated procedures as part of its effort to update the Information Security and Privacy Policy Handbook."

C. Web Application Vulnerability Scanning

We requested the results of recent vulnerability scans conducted by the OCIO for a sample of public facing web applications and the servers hosting those applications. We also performed our own vulnerability scans on those same web applications and servers using automated scanning tools. While the OCIO was able to provide historical server vulnerability scan results, we were told that there is not a formal process in place to perform routine credentialed web application vulnerability scans (however, ad-hoc non-credentialed scans were performed). Scans performed without user credentials that allow the scanning tool to authenticate to the scan target may not be able to collect the information necessary to fully analyze the system.

NIST SP 800-53, Revision 4, states that organizations must scan information systems and hosted applications for vulnerabilities. It also states that organizations must implement privileged access authorization for vulnerability scanning activities. Privileged access authorization (i.e., running the scan with user credentials) facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning. Failure to perform vulnerability scanning with sufficient access increases the risk that system flaws can go undetected, leaving the organization exposed to security threats.

Furthermore, the results of the credentialed web application scans that we performed during this review indicate that several applications and the servers hosting these applications contain security weaknesses. Due to the sensitive nature of the specific vulnerabilities identified in the scans, they will not be discussed in this report. We directly provided the OCIO with the full scan results of our scans for review.

Our fiscal year 2015 Federal Information Security Modernization Act audit reported that OPM did not have a process to centrally track the current status of security weaknesses identified during server vulnerability scans, and we had concerns that OPM was not remediating known vulnerabilities in a timely manner. The results of our server vulnerability scans performed during this review indicate that this situation still exists. Specifically, server vulnerability scans are routinely conducted, but the results are not adequately tracked to ensure the weaknesses are corrected.

Recommendation 3

We recommend that OPM implement a process to perform credentialed web application vulnerability scans and track any identified vulnerabilities until they are remediated.

OCIO Response:

"OCIO concurs with the recommendation. OCISO will standardize its process for conducting credentialed web application vulnerability scans and incorporate the tracking and remediation of identified vulnerabilities into its risk management processes."

Recommendation 4

We recommend that OPM analyze our scan results to identify false positives and remediate any verified vulnerabilities.

OCIO Response:

"OCIO concurs with the recommendation. OCISO will work with application owners to review the web application scans, identify false positives, and remediate any verified vulnerabilities."

Attachment

cc: Kiran Ahuja
Chief of Staff

David L. DeVries
Chief Information Officer

[redacted]
Chief Information Security Officer

Mark W. Lambert
Associate Director, Merit Systems Accountability and Compliance

Janet L. Barnes
Director, Internal Oversight and Compliance

Clifton N. Triplett
Senior Cybersecurity and IT Advisor

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

MEMORANDUM FOR [redacted]
CHIEF, INFORMATION SYSTEMS AUDIT GROUP
OFFICE OF THE INSPECTOR GENERAL

FROM: DAVID L. DEVRIES
CHIEF INFORMATION OFFICER

David DeVries
29 Sep 2016

Subject: Office of the Chief Information Officer Response to the Office of the Inspector General Web Application Security Review (Report No. 4A-CI-00-16-061)

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report for the Web Application Security Review for the U.S. Office of Personnel Management (OPM). The OIG comments are valuable to the office of the Chief Information Officer (OCIO) as they afford us an independent assessment of our operations and help guide our improvements to enhance the security of the data furnished to OPM by the Federal workforce, the Federal agencies, our private industry partners, and the public.

We welcome a collaborative dialogue to help ensure we fully understand the OIG's recommendations as we plan our remediation efforts so that our actions and the closure of the recommendations thoroughly address the underlying issues. I look forward to continued discussions during our monthly reviews to help ensure we remain aligned.

Each of the recommendations provided in the draft report is discussed below:

Recommendation 1
We recommend that OPM create a formal and comprehensive inventory of web applications. The inventory should identify which applications are public facing and contain personally identifiable information or sensitive agency information, identify the application owner, and itemize all system interfaces with the web application.

CIO Response: OCIO concurs with the recommendation. The web team will work with application owners to update the inventory of web applications and maintain relevant inventory data on these applications.

Recommendation 2
We recommend that OPM create or update its policies and procedures to provide guidance specific to the hardening of web server operating systems and the secure design and coding of web based applications.

CIO Response: OCIO concurs with the recommendation. The Office of the Chief Information Security Officer (OCISO) will incorporate requirements specifically associated with the hardening of web based applications and host operating systems into the policies and associated procedures as part of its effort to update the Information Security and Privacy Policy Handbook.

Recommendation 3
We recommend that OPM implement a process to perform credentialed web application vulnerability scans and track any identified vulnerabilities until they are remediated.

CIO Response: OCIO concurs with the recommendation. OCISO will standardize its process for conducting credentialed web application vulnerability scans and incorporate the tracking and remediation of identified vulnerabilities into its risk management processes.

Recommendation 4
We recommend that OPM analyze our scan results to identify false positives and remediate any verified vulnerabilities.

CIO Response: OCIO concurs with the recommendation. OCISO will work with application owners to review the web application scans, identify false positives, and remediate any verified vulnerabilities.

Again, thank you for the opportunity to provide comment. Please contact me or [redacted] if you have questions or need additional information.

cc:
[redacted]
Chief Information Security Officer

Dovarius L. Peoples
Associate Chief Information Officer

Mark W. Lambert
Associate Director, Merit Systems Accountability and Compliance

Janet L. Barnes
Director, Internal Oversight and Compliance

Clifton N. Triplett
Senior Cybersecurity and IT Advisor