Montgomery County, Maryland
Office of the County Executive
Office of Internal Audit

Information Technology Audit: Patch Management

January 31, 2021

MCIA-21-3

Highlights

Why MCIA Did this Review

The Montgomery County Office of Internal Audit (MCIA) conducted an Information Technology (IT) audit of patch management processes within Montgomery County Department of Technology Services (DTS). DTS is a fully integrated County department that provides support to all Montgomery County departments and offices and is organized into multiple divisions. The audit assessed the Enterprise Applications and Solutions Division (EASD) and Enterprise Systems and Operational Division (ESOD) policies and procedures surrounding the County's patch management processes. The EASD network team manages Microsoft, Adobe, Java, and third-party browser (i.e., Google Chrome and Mozilla Firefox) patch updates for over 10,000 devices across the County. EASD also delivers data services, device management, and provides device updates and patch management processes through Microsoft's System Center Configuration Management (SCCM) software.

The ESOD server team manages security updates for over 800 servers across the County. It also provides updates and patch management manually for all servers maintained by DTS.

This audit was conducted as a result of MCIA's 2019 IT risk assessment. The focus was to evaluate the current internal control environment of the County's patch management processes. The audit was conducted by the accounting firm SC&H Group, Inc., under contract with MCIA.

MCIA is making six recommendations to DTS to strengthen the existing control environment within the County's patch management processes.

January 2021

IT Audit of the County's Patch Management Processes

What MCIA Found

The audit of the County's patch management processes identified several opportunities to mitigate risks. The risks can be addressed by enhancing or implementing internal controls within the patch management processes.

We identified six recommendations to strengthen controls and mitigate risks within the County's patch management processes:

1. Developing and/or enhancing detailed procedural documents
2. Implementing periodic user access reviews of administrative and service accounts
3. Enhancing the monitoring of exemption tickets
4. Developing and implementing a defined frequency of security reviews on devices
5. Developing and implementing a defined frequency of patching for exempt devices
6. Developing and implementing a device monitoring program

TABLE OF CONTENTS

Objectives

This report summarizes the information technology (IT) audit of Montgomery County's (the County) patch management processes (audit). The audit was performed by SC&H Group, Inc. (SC&H), under contract with the Montgomery County Office of Internal Audit (MCIA).

The audit included meeting with members of the Enterprise Applications and Solutions Division (EASD) and Enterprise System and Operations Division (ESOD) within the County's DTS to build upon the knowledge obtained through the County's Information Technology Risk Assessment (ITRA), and to understand the following specific to each division within DTS:

1. Patch management processes responsibilities between departments and DTS
2. Documented policies, procedures, standards, and/or guidelines
3. Frequency of patches for critical systems
4. How patches to critical information systems are managed and tracked

The audit's objective was to evaluate the efficiency and effectiveness of the County's internal controls for patch management processes including identification, assessment, verification, and management of patches at the server and workstation level.

Background

County-wide Information Technology Overview

The County manages hardware, software, and technology through a combination of centralized and decentralized functions to enable employees to provide quality services to citizens and businesses, deliver information and services to citizens, and increase productivity.

Centralized IT Functions

DTS provides certain IT services and communication services necessary to support the daily operation of County departments through seven divisions, offices, and programs, including:

1. Office of Broadband Programs (OBP)
2. Office of the Chief Information Officer (CIO)
3. Office of the Chief Operating Officer (COO)
4. Enterprise Applications and Solutions Division (EASD)
5. Enterprise Systems and Operations Division (ESOD)
6. Enterprise Telecommunications Services Division (ETSD)
7. Enterprise Resource Planning Division (ERPD)

DTS is responsible for assisting the County's departments with identifying innovative technology solutions, helpdesk support, security, etc. EASD and ESOD were in scope of this audit.

The EASD network team manages Microsoft, Adobe, Java, and third-party browser (i.e., Google Chrome and Mozilla Firefox) patch updates for over 10,000 devices across the County. EASD also delivers data services, device management, and provides device updates and patch management processes through Microsoft's System Center Configuration Management (SCCM) software.

The ESOD server team manages security updates for over 800 servers across the County. It also provides updates and patch management manually for all servers maintained by DTS.

Patch Management Overview

Patch management is the overall process of monitoring, distributing, and applying patches to applications, operating systems, and network equipment to limit exposure to vulnerabilities or bugs in software. Established patch management processes and controls reduce the likelihood of critical systems and applications being vulnerable to bugs, malware, and functionality issues. Failure to follow sufficient processes and controls could result in successful attacks from threat actors and other internal or outside forces, increased downtime in critical information systems, and the breach of sensitive information.

Patch Management Processes

The County creates an annual calendar detailing scheduled workstation and server patches in order to limit downtime for County employees. The calendar includes time to test, deploy, and monitor the effects of patches for each department. The County utilizes Qualys, an IT security company that provides cloud security and compliance services, to run weekly vulnerability reports to detect potential security vulnerabilities that companies have disclosed that may require patch updates. The Qualys report scans and identifies potential vulnerabilities on IT assets. Departments can request to delay deployment of a scheduled patch/update by completing an exemption ticket that details the reasoning for the requested exemption. The DTS security team reviews each ticket and approves or denies the request.

The County utilizes Microsoft Power BI to monitor the status of patch implementations. The County also uses Power BI to monitor if BitLocker, a Microsoft Windows encryption feature, is enabled on County devices. BitLocker encrypts devices to help secure the data stored on the device.

Scope and Methodology

The audit was conducted from March 2020 to September 2020. The audit focused on the current patch management processes administered by EASD and ESOD. Processes included the following:

1. Identification of patching completeness and accuracy.
2. Review, prioritization, and approval of patches.
3. Testing patches prior to deployment.
4. Applying patches.
5. Tracking and monitoring approved patches to ensure patches are implemented within 90 days of release.
6. Monitoring post implementation of applied patches.

The audit also included an analysis of the following aspects related to the patch management processes:

1. Maturity of the process
2. Number of critical systems
3. Ownership of the various functions within the process
4. Estimated number of patches per year
5. Applicable NIST 800-53 rev. 4 controls[1]

[1] Security and Privacy Controls for Federal Information Systems and Organizations. https://nvd.nist.gov/800-53/Rev4. Issued by the non-regulatory agency of the United States Department of Commerce, NIST 800-53 contains a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. This standard contains best practices as a guideline for IT security and privacy controls.

Scope criteria included patches implemented from January 1, 2020 to July 31, 2020.

Scoping

SC&H performed the following procedures to obtain a preliminary understanding of the County's patch management function.

Interviews

SC&H conducted detailed interviews and walkthroughs with EASD and ESOD staff. The purpose was to observe and document the internal controls and related risks associated with each of the following domains:

1. Governance
2. Asset Management
3. Access Management
4. Configuration Management
5. Awareness Training (Network)
6. Exemption Policies and Procedures

Policy and Procedure Review

SC&H reviewed the County's patch management policies and procedures at the server and workstation level. SC&H also reviewed Qualys vulnerability scan reports to gain an understanding of monitoring vulnerabilities from discovery to remediation.

Test Plan Development

Utilizing the information obtained during scoping and preliminary department assessment, interview, and walkthrough procedures, SC&H developed an audit plan to test the operational effectiveness of internal controls.

Fieldwork

Fieldwork consisted of testing the operational effectiveness of internal controls identified during scoping and preliminary department assessment, interviews, and walkthrough procedures. SC&H prepared a document request listing for all information needed to satisfy the testing steps developed in the test plan, including populations needed to select samples for which additional information was requested.

Appendices A and B are provided as reference for all controls tested as part of the audit.

Findings and Recommendations

The following six findings were identified to strengthen and expand the County's patch management processes and controls.

Due to the sensitive nature of the findings, detailed information is not included in this report. DTS and the respective divisions received detailed findings and recommendations separately for review and response. For each of the divisions, specific recommendations have been developed to address the division-specific findings. DTS will be required to develop corrective action plans to timely and fully address the recommendations.

1. **Patch Management Policies**
   Sufficient patch management policies and procedures reflective of the current process and control environment have not been developed and/or formalized.

Failure to document the required procedures related to the patch management process could result in a security lapse within critical information systems. This could further result in breaches to sensitive information. Additionally, systems that are not properly updated could result in unauthorized access and successful attacks to sensitive information including, but not limited to, denial of services attacks, ransomware attacks, manipulation of data, and fraudulent activities that can be associated with fines and penalties.

2. **User Access Reviews**
   Periodic user access reviews are not conducted on a defined frequency to monitor administrative and/or service accounts.

   Inappropriate users having elevated access to critical information systems could expose the department and/or the County to vulnerabilities such as unauthorized access to data, manipulation of data, and/or denial of service attacks. Additionally, inappropriate users having patch access to critical information systems may expose the department and/or the County to unauthorized patches, data leakage, and fines associated with national and federal standards and regulations.

3. **Exemption Ticket Monitoring**
   Exemption tickets are not monitored and/or updated on a defined frequency.

   Information systems and assets that are not patched on a consistent interval could expose the County to disruptions and threats. Additionally, out of date systems could create negative effects in business and IT operations, the public's experience of County services, and/or breaches in data.

4. **Security Status**
   BitLocker is not enabled on all devices.

   Devices that do not have disk encryption could expose the County to disruptions and threats. Additionally, unencrypted devices could create negative effects in business and IT operations, the public's experience of County services, and/or breaches in data.

5. **Exempt Device Patch Frequency**
   Server exemptions are not maintained and monitored in accordance with a policy.

   Information systems and assets that are not patched on a consistent interval could expose the County to disruptions and threats. Additionally, out of date systems could create negative effects in business and IT operations, the public's experience of County services, and/or breaches in data.

6. **Client Device Management Tool Management**
   Client device management tools are not regularly monitored for device compliance and confirmation of updates.

   Information systems and assets that are not patched on a consistent interval could expose the County to disruptions and threats. Additionally, out of date systems could create negative effects in business and IT operations, the public's experience of County services, and/or breaches in data.

Comments and MCIA Evaluation

We provided the Department of Technology Services (DTS) with a draft of this report for review and comment. DTS responded with comments on January 25, 2021, and the response has been incorporated in the report at Appendix C. DTS concurred with the findings identified in the report, indicating that the department has taken steps to address some of the findings, and that additional steps will be taken to enhance the enterprise patch management process. No changes have been made in the report based on the response.

Appendix A – Areas of Focus: Network

Domain	Control #	Control Description
Governance	N1	Patch Management security roles and responsibilities are clearly defined.
Asset Management	N2	Physical devices, software platforms and systems within the organization are inventoried.
Access Management	N3	Administrative access to SCCM and Qualys is limited to appropriate patch management users that do not have conflicting IT, patch management, and financial functions within the organization.
Configuration Management	N4	The SCCM client is installed on devices to ensure that updates are distributed in a timely manner.
	N5	All devices inactive for 45 days are moved to the quarantined organization unit.
	N6	All devices inactive for 60 days are disabled in Active Directory.
	N7	All patch management exemptions are approved by the Information Technology Security Team and those devices are moved into the appropriate exemption folder.
	N8	All machines have BitLocker enabled.
	N9	All machines have anti-virus and anti-malware software on equipment connected to the network, including servers, production and training desktops to protect against potentially harmful viruses and malicious software applications.
	N10	SCCM scans clients daily and completes a full scan weekly on Saturdays.
	N11	SCCM Manager reviews weekly Qualys report to determine the number of high risk (categorized as 4 and 5) vulnerabilities and compares the number of affected devices with prior week's report to confirm that the number of vulnerabilities is reducing.
	N12	Patch Management configuration changes follow a change process based on type of patch and the vulnerability.
	N13	Windows builds are tested for a six (6) month period after release, prior to release through Auto Deployment Rules (ADR).
Awareness Training	N14	SCCM Manager performs ad hoc trainings regarding the use and function of the Security Dashboard to assist departments in monitoring vulnerabilities.

Appendix B – Areas of Focus: Server

Domain	Control #	Control Description
Governance	S1	Patch Management security roles and responsibilities are clearly defined.
	S2	Annually the Server team creates a calendar of all server updates.
Asset Management	S3	Physical devices, software platforms and systems within the organization are inventoried.
Access Management	S4	Administrative access to servers is limited to appropriate patch management users that do not have conflicting IT, patch management, and financial functions within the organization.
Configuration Management	S5	All patch management exemptions are approved by the Information Technology Security Team and those exceptions are communicated to the System Administrator in charge of updating that server.
	S6	All servers have anti-virus and anti-malware software to protect against potentially harmful viruses and malicious software applications.
	S7	Server Manager reviews weekly Qualys reports to determine the number of high risk (i.e., categorized as 4 and 5) vulnerabilities and compares the number of affected servers with prior week's report to confirm that the number of vulnerabilities is reducing.
	S8	Patch Management configuration changes follow a change process based on type of patch and the vulnerability.

Appendix C – Department Comments

DEPARTMENT OF TECHNOLOGY SERVICES

Marc Elrich
County Executive

Gail Roper
Chief Information Officer

MEMORANDUM

January 25, 2021

TO: William Broglie, Internal Audit Manager

FROM: Gail M. Roper, Director *Gail M. Roper*
Chief Information Officer

Subject: **Formal Comments on Draft Report:** Information Technology Audit: Patch Management Process

I have reviewed the recommendations detailed in the Information Technology Audit of Montgomery County's Patch Management Process performed by SC&H Group, Inc. (SC&H), under contract with the Montgomery County Office of Internal Audit (MCIA).

I agree with the documented findings of the audit in the following areas:

1. Patch management process responsibilities between departments and DTS
2. Documented policies, procedures, standards, and/or guidelines
3. Frequency of patches for critical systems
4. How patches to critical information systems are managed and tracked

I support the six recommendations to strengthen controls and mitigate risks within the County's patch management processes, including:

1. Developing and/or enhancing detailed procedural documents
2. Implementing periodic user access reviews of administrative and service accounts
3. Enhancing the monitoring of exemption tickets
4. Developing and implementing a defined frequency of security reviews on devices
5. Developing and implementing a defined frequency of patching for exempt devices
6. Developing and implementing a device monitoring program

To advance patch management, deployment, and accountability, there will be a patch execution process both central to DTS and for the enterprise organization. The standardization of patch management execution requires strategy, process, and resources. The original structure of the DTS organization supported client patching through our SCCM program and server patching through our Server team. We believe both processes to have been effective. What was not supported in the old organization structure was the development of more formal risk and review processes and formal standardized process documentation. This was acknowledged and incorporated into the DTS reorganization. Also, and as it relates to this audit, I have hired a policy analyst staff resource to work on DTS policy and procedure development. Specifically, the hiring of a policy analyst staff resource will help drive the development of more formal documented standards.

The enhanced security spending with our latest purchase of Microsoft Office 365 licenses is partly driven by the desire to use automated Active Directory group review and verification and the use of Privileged Identity Management (PIM) capabilities. These capabilities were purchased with the intent to review and validate administrator and group access. Both capabilities will apply in this area.

We plan to establish formal documentation for the enterprise for patch management. The enterprise patch management process will include:

- Formal process documentation for clients
- Formal process documentation for servers
- Documentation that defines roles and responsibilities for departments managing their departmental managed servers
- Formal documentation around the exemption process with the DTS security team
- Formal process around client and server administration access reviews