THE UNIVERSITY OF TEXAS-PAN AMERICAN
OFFICE OF AUDITS & CONSULTING SERVICES

Server Management-Scans & Patches

Report No. 14-11
June 5, 2014

Dr. Robert S. Nelsen, President
The University of Texas-Pan American
1201 W. University Drive
Edinburg, TX 78539

Dear Dr. Nelsen,

As part of our fiscal year 2013 Audit Plan, we completed an externally required audit of Server Management-Scans & Patches. The objective of the audit was to evaluate server management to determine whether scans and patches are routinely performed to identify vulnerabilities and whether remediation plans are executed. The scope of the audit included all critical UTPA servers as determined by management.

We performed audit procedures that included reviewing server management documentation and procedures conducted by Data Center Services personnel; interviewed employees managing servers; reviewed scan results procedures conducted by Information Technology Security; and reviewed penetration tests conducted by a third party vendor. In addition, we used the National Institute of Standards and Technology (NIST) Special Publication 800-40 Version 2.0, Creating a Patch and Vulnerability Management Program as criteria for completing our work.

Overall, based on the processes and documentation reviewed, we concluded that the University has an adequate server management program. Employee responsibilities were defined, a system inventory exists, vulnerability and threats were monitored, remediation was tested, processes to deploy remediation existed, and remediation was verified. The detailed report is attached for your review.

We appreciate the courtesy and cooperation received from management and staff during our audit.

Sincerely,

Eloy R. Alaniz, Jr., CPA, CIA, CISA
Executive Director of Audits, Compliance & Consulting Services
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>1</td>
</tr>
<tr>
<td>BACKGROUND</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT OBJECTIVE</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT SCOPE AND METHODOLOGY</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT RESULTS</td>
<td>3</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>7</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Information resources play an important role in The University of Texas – Pan American’s (UTPA) processes. Uses of information resources include student recruitment and enrollment, student and employee records, online learning, classroom technology, internet, student and employee communications, financial management, and file sharing. Information technology resources need to be protected to ensure data integrity and availability and to prevent misuse of information.

UTPA employs several measures to protect information resources. Some of these measures include an information security program led by the Chief Information Security Officer (CISO), information security processes performed by Information Technology Security (ITS), the Access Administration Office, penetration tests, perimeter defenses, systems closed to outside networks, spam blockers, and password management. To complement these measures, UTPA performs several processes to manage servers that house information resources. A server is a computer system that provides shared services to other users.

The processes employed to manage servers include:

- Well defined employee responsibilities
- System inventory
- Monitoring for vulnerabilities and threats
- Remediation testing
- Deploying vulnerability remediation
- Verifying remediation

Proper server management ensures that the University complies with security requirements from the Texas Administrative Code (TAC) Rule 202.75 - Information Resources Security Safeguards. These requirements include: security policies and perimeter security controls.

The objective of the audit was to evaluate server management to determine whether scans and patches are routinely performed to identify vulnerabilities and whether remediation plans are executed.

Based on the processes and documentation reviewed, we concluded that the University has an adequate server management program. Employee responsibilities were defined, a system inventory exists, vulnerability and threats were monitored, remediation was tested, processes to deploy remediation existed, and remediation was verified.
BACKGROUND

Information resources are essential to daily operations of UTPA and include the student system, Banner, the financial and human resource system, Oracle E-Business, and many other systems that support daily operating processes. Some of these systems store confidential and sensitive information. It is crucial to University operations that the availability and protection of these systems is ensured.

There are several methods for protecting information technology resources. The first line of defense is properly managed servers. Proper server management ensures maximum security without affecting system performance. A server is a computer system that provides shared services to other users. The main services provided by University servers include enterprise-wide application hosting, database storage, file storage, email processing, and web hosting. All of these services are essential to key processes and any loss of service or misuse of confidential and sensitive information may have no adverse effects on the University.

Some of UTPA’s processes related to server management depend on vulnerability scans. ITS frequently performs vulnerability scans on servers and reports of vulnerabilities discovered are sent to server administrators, the Chief Information Security Officer, and the Vice President of Information Technology. Server administrators remediate vulnerabilities and request that ITS perform subsequent scans to verify that remediation was successful. In addition, Data Center Services (DCS) has vulnerability scanning tools they can use to search for vulnerabilities.

AUDIT OBJECTIVE

The objective of the audit was to evaluate server management to determine whether scans and patches are routinely performed to identify vulnerabilities and whether remediation plans are executed.

AUDIT SCOPE & METHODOLOGY

In performing this engagement we:

- Reviewed server management documentation and procedures conducted by DCS.
- Interviewed employees managing servers.
- Reviewed scan results procedures conducted by Information Technology Security.
- Reviewed penetration tests conducted by a third party vendor.

In addition we used the National Institute of Standards and Technology (NIST) Special Publication 800-40 Version 2.0, Creating a Patch and Vulnerability Management Program as criteria for completing our work.

The scope of the audit included all critical UTPA servers as determined by management.
We performed this audit in accordance with guidelines set forth in The University of Texas System’s Policy 129 and The Institute of Internal Auditor’s International Standards for the Professional Practice of Internal Auditing. The audit was conducted between the months of July 2013 through April 2014.

AUDIT RESULTS

Responsibilities

NIST Section 2.1 recommends that a patch management program have two groups of people. The first group should be responsible for implementing the patch management program. This group should include representatives from information security and operations. The second group should be responsible for monitoring vulnerabilities, testing remediation, and applying remediation.

At UTPA, the first group consisted of the Director of the Computer Center and staff from ITS. The Director of the Computer Center is responsible for maintaining server inventory and supervising server administrators. ITS is responsible for performing vulnerability scans and providing the Director of the Computer Center, server administrators, and the Office of the Chief Information Security Officer (OCISO) with scan results. ITS is also involved in the vulnerability remediation process. They provide subsequent scans to verify that remediation was successful.

The second group consisted of server administrators. Each server was assigned an administrator. Server administrators were in charge of maintaining their assigned servers and have the following vulnerability remediation responsibilities:

- Monitoring for vulnerabilities
- Testing remediation
- Deploying vulnerability remediation
- Distributing vulnerability and remediation information to other administrators
- Verifying remediation

Server administrators have participated in information technology security training to ensure that they have enough skills to meet their responsibilities.

The duties performed by ITS and server administrators are adequately segregated – ITS identifies vulnerabilities and server administrators remediate them. In addition, ITS verifies that vulnerabilities have been remediated.

System Inventory

NIST Section 2.2 recommends the creation and maintenance of an inventory of information resources to determine which hardware equipment, operating systems, and software applications are used within the organization and then group and prioritize those resources. Two tests were
performed to verify that the inventory exists, is accurate, and complete. In addition, we reviewed
documentation and processes to verify that a formal process existed to group and prioritize
inventory.

The first test was performed to verify that the server inventory list had enough information to
manage servers. We tested 17% of the servers listed in inventory. The information maintained
on the servers tested was complete and accurate.

The second test was performed to verify that the servers were in the locations stated in the
inventory list. We tested 3% of the servers listed in inventory. All of the servers tested were
found.

We reviewed documentation and processes and verified that DCS has a formal process to group
and prioritize inventory based on vulnerability remediation classifications. DCS uses three
classifications listed below to group and prioritize vulnerability remediation:

1. Server Status - determines the environment where the system is used, different
   environments include production, test, and development.
2. Infrastructure - determines if the server is for a system that supports University
   infrastructure.
3. Serves Students - determines if the server is for a system that directly serves students.

Based on the tests performed and documentation reviewed, we determined that the server
inventory exists, is accurate, and complete, and that DCS has grouped and prioritized the
University’s servers.

**Monitoring Vulnerabilities and Threats**

NIST Section 2.3 recommends monitoring security resources for vulnerability announcements
and threats that correspond to the software within the organizational software inventory. For this
NIST guideline we reviewed documentation and processes to verify that the University
employed adequate resources to monitor vulnerabilities and threats.

The University uses several tools to monitor vulnerabilities and threats. These tools include:

- Vulnerability scan tools
- Enterprise management patch tools
- Security bulletins
- Vulnerability mailing lists

ITS frequently performs vulnerability scans. Results from these scans are sent to server
administrators for mitigation. DCS uses enterprise management patch tools.
DCS checks the Microsoft’s security bulletins every second Tuesday of each month known as Microsoft’s “Patch Tuesday”, and any applicable security updates are applied. DCS installs updates on a monthly basis.

In addition, DCS is proactive in identifying emerging vulnerabilities and threats through its participation on several vulnerability mailing lists. These mailing lists include the Microsoft’s technical account manager, Oracle security bulletins, and ultimate Windows security.

Based on the documentation and processes reviewed, we determined that the University employed adequate resources to monitor vulnerabilities and threats.

**Testing Remediation**

NIST Section 2.6 recommends that system administrators test patches and non-patch remediation to mitigate vulnerabilities and threats identified. For this NIST guideline, we reviewed documentation and processes to verify that:

- Documentation for testing is maintained
- Patch and non-patch remediation are tested on non-production instances before they are applied to production instances.
- There is a process to review and approve testing performed before the remediation is applied to a production instance.

We determined that DCS did not maintain formal testing documentation and did not have a formal process to review and approve testing performed. Informal approval of testing was obtained through emails between the ITS and DCS. ITS and DCS sends each other emails on the status of vulnerability remediation.

According to the Director of the Computer Center, the process to test vulnerabilities on major systems involves first testing the vulnerability in a test environment. This step is performed by the assigned server administrator. Once it is verified that there are no adverse effects on server software, the remediation is applied to the production server. Smaller systems do not have test environments where remediation can be tested. In this case, remediation is applied straight to production environments. Regularly scheduled backups are used if something goes wrong and the system needs to be brought back to its original state. After the remediation is applied to the production environment, a new vulnerability scan is performed on the production server to verify that remediation tested was successful.

Based on the documentation and processes reviewed, we determined that remediation testing was adequate.
Deploying Vulnerability Remediation

NIST Section 2.7 recommends that organizations deploy vulnerability remediation to all systems that have vulnerabilities, even for systems that are not at immediate risk of exploitation. For this NIST guideline, we performed a test to verify that vulnerability remediation was deployed timely; backups were conducted before remediation was performed, and documentation existed for remediation exceptions.

We tested 3% of the servers listed in inventory. The documentation provided by DCS for this test consisted of vulnerability scans performed on sample servers. Before and after vulnerability scans were used to verify that vulnerabilities were deployed timely. Before scans showed vulnerabilities needed to be remediated and after scans showed vulnerabilities no longer present. Only three (3) of the servers in our sample had before and after scans. For these three (3) servers, the remediation was performed timely. The other 17 servers in our test sample only had one (1) vulnerability scan. These vulnerability scans were performed by DCS when audit documentation was requested.

Based on the number of servers in our test sample without remediation documentation, we could not determine whether remediation was deployed timely. This risk, however, was minimized with compensating controls performed by DCS. These controls, as previously mentioned, include vulnerability scan tools used by DCS, enterprise management patch tools, security bulletins, and vulnerability mailing lists.

We also noted that no documentation was maintained to verify that backups were conducted before remediation was performed on servers in our test sample. However, it is a common practice to conduct backups for University systems on regular basis. According to the Director of the Computer Center, backups are performed on major systems right before remediation is performed. For smaller systems no backups are performed right before remediation. If something goes wrong regular scheduled backups may be used to restore the system.

No evidence existed to support remediation exceptions on servers in our test sample. However, remediation exceptions discovered by ITS and not mitigated by server administrators are documented by the Office of the Chief Information Security Officer.

Verifying Remediation

NIST Section 2.9 recommends that organizations verify that they have remediated or mitigated vulnerabilities as intended. For this NIST guideline, we reviewed the vulnerability scan process, the penetration scan process, and patch log documentation.

Based on the processes and documentation reviewed, ITS and DCS adequately used several processes to verify that vulnerabilities were remediated or mitigated. In addition, ITS and DCS use vulnerability scans to verify that remediation was effective. After a remediation has been
implemented, a vulnerability scan is performed to verify that the vulnerability is no longer present. Lastly, third party penetration tests have been performed annually.

However, we could not determine if server patch logs were reviewed on a regular basis due to lack of documentation. Vulnerability scanning, penetration tests, and additional compensating controls described throughout this report help minimize this risk.

CONCLUSION

Based on the processes and documentation reviewed, we concluded that the University has an adequate server management program. Employee responsibilities were defined, a system inventory exists, vulnerability and threats were monitored, remediation was tested, processes to deploy remediation existed, and remediation was verified.

Isabel Benavides CIA, CGAP, CFE
Director, Audits and Consulting Services

Jose Gomez, MS
Information Systems Auditor III