Report on Web Applications #13-205

We have completed our audit of web application security. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

BACKGROUND

UTHealth’s Information Technology Security Department (ITS) estimated that more than 400 web applications could presently be deployed on UTHealth servers. These web applications can originate from several sources including: applications developed by UTHealth employees, custom applications developed by a vendor specifically for UTHealth, off the shelf web applications, web applications developed using open source code, and shareware. Each web application development process has a unique set of security concerns.

Web applications can expose UTHealth to different types of risks based upon their purpose. Web applications accept user input and process information which can expose the institution to: data loss or modification, denial of service attacks, compromised user login credentials, negative impact on reputation, and possible fines. A security breach at UTHealth could potentially lead to the compromise of research, personal health information (PHI), personally identifiable information (PII), or other forms of proprietary information. Security and oversight for web applications is distributed across several areas of the institution.

In 2013, SANS listed web application security as one of the top 20 controls needed for effective cyber defense. According to SANS:

"Attacks against vulnerabilities in web-based and other application software have been a top priority for criminal organizations in recent years. Application software that does not properly check the size of user input, fails to sanitize user input by filtering out unneeded but potentially malicious character sequences, or
does not initialize and clear variables properly could be vulnerable to remote compromise. Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery, and click-jacking of code to gain control over vulnerable machines. In one attack, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites using SQL injection. During that attack, trusted websites from state governments and other organizations compromised by attackers were used to infect hundreds of thousands of browsers that accessed those websites.”

OBJECTIVES

The objective of this audit was to review the controls in place to ensure the confidentiality, integrity, and availability of information processed through web applications.

SCOPE AND METHODOLOGY

Through interviews and documentation review, Auditing and Advisory Services (A&AS) assessed the adequacy of departmental and institutional processes and controls in place to secure web applications. Our fieldwork included: assessing the adequacy of web application policies, identifying areas that develop web applications, determining if there is a process for inventorying web applications and identifying web developers. We reviewed the adequacy of the web application scanning process and efforts to deploy the web application firewall (WAF). A&AS, with the assistance of ITS, scanned and evaluated the security of 11 internally developed web applications that were accessible from the public internet.

AUDIT RESULTS

Areas Developing Web Applications
A&AS interviewed key personnel throughout the institution and identified at least 11 separate areas that developed or managed web applications.

Identification of Web Developers
A complete list of web developers did not exist. However, a manager in Academic Technology maintains an informal list of web developers and shares this list with other areas. This list is used as a means to communicate web application security issues throughout the institution. The lack of a complete list of developers inhibits the ability of management to adequately train and provide oversight to the developers.

Web Application Inventory
UTHealth does not maintain a complete list of web applications. The lack of a complete inventory affects management's ability to ensure the web applications are adequately secured.

During our review, A&AS noted an outdated web application (with no apparent business purpose) that was still accessible to the public. Based upon our inquiry, a process did not exist to identify outdated web applications, to ensure they were appropriately taken out of service, and to secure the associated information stored by the web applications.
Web Application Policy
Several Information Technology (IT) policies address the elements needed for web application security. However, there are no policies that specifically address the development, management, and security of web applications.

Institutional Oversight of Security Policy
Texas Administrative Code (TAC) 206 requires the institution to implement security and privacy safeguards prior to providing information services on a website. TAC 206 also requires new or updated websites to comply with Federal accessibility requirements.

The Director of Web Communications, the Chief Information Officer (CIO), and the Chief Information Security Officer (CISO) have varying degrees of responsibility over the web application security process. They are responsible for ensuring security is built into the web application during the development process and maintaining security throughout the useful life of the application. However, those tasked with overseeing web application security stated an adequate reporting structure for the development and oversight of web applications did not exist.

A manager in Academic Technology, with the cooperation of other departments, has been instrumental in establishing a voluntary web application programming group. His efforts have resulted in the creation of both informal and indirect reporting structures that provide a more uniform approach to web application security.

Scanning and Remediation Process
The only mandatory control for web application security is enforced through the firewall process. ITS is responsible for maintaining the institution’s firewalls. A firewall controls the flow of data to and from an information resource. In the case of web applications, a specific set of ports (communication channels) are opened up so the web applications that are housed on a server are available to internal and external users. Once a server is allowed to communicate with the Internet, the web application programmer has the ability to add additional web applications without further oversight from ITS.

Web application scanning is coordinated by ITS using the Qualys scanning application. The Qualys application ranks all vulnerabilities on a scale of 1 to 5 (low to high). ITS will not open the needed ports for a new server to communicate with the users without scanning the application. Due to the potential for loss of protected information, ITS stated all vulnerabilities, no matter the level, must be assessed and remediated as appropriate.

A&AS selected a sample of 10 in-house developed web applications to test that an initial security review was performed. Documentation showing a scan was performed was available for only 2 of the 10 web applications from our sample.
Scan of Sampled Applications
A&AS selected a judgmental sample of 11 existing web applications for testing. With the assistance of ITS, the web applications were scanned to identify whether any vulnerabilities existed. We conducted unauthenticated scans, which would confirm the existence of risks that could be potentially exploited by an unauthorized external attacker. Of the 11 web applications scanned, we noted 70 LOW vulnerabilities and 34 MEDIUM vulnerabilities. ITS stated they had documentation that only three of the sampled applications were previously scanned.

Some areas interviewed during the audit stated they either: placed new web applications on a server without having ITS review the security, did not conduct security scans after changes were made, or did not scan web applications on a regular basis to ensure new vulnerabilities did not exist on a server.

Segregation of Duties
A&AS asked areas that developed web applications if controls exist to prevent an individual from independently testing and migrating changes to production. Most areas stated preventative controls do not exist to enforce segregation of duties in the web application process.

Recommendation 1: We recommend Information Technology, Information Security, Web Communications, the applicable schools, and departments work together to create, implement, and maintain a web application security policy or policies to address (at a minimum) the following:

- Establish oversight of the web application development and security process, which defines the responsibility of Central IT, Information Security, Web Communications, and developers/developing departments as applicable.
- Implement and maintain a web application inventory process;
- Develop a process that would create, implement, and maintain a centralized and complete list of web developers;
- Secure in house and vendor developed web applications;
- Follow UTHealth's System Design Life Cycle policy or developing an appropriate SDLC for web applications;
- Establish adequate segregation of duties;
- Create a web application scanning policy that includes: frequency and type of scans, vulnerability mitigation, a record of application scans, and a risked based scan monitoring process;
- Establish security reviews/approval by Information Security and Web Communications;
- Establish accessibility reviews/approval by Web Communications; and
- Include applicable State and Federal guidelines and regulations.
Management's Response: The responsible parties will assemble and charge a leadership team from Information Technology, Information Technology Security, Web Communications and the web developers group to develop a 'Web Applications Developer’s Standards, Policy & Procedures Guide' which will include a definition of the terms ‘web application’ and ‘web developer’. The Web Developer’s Group will be formalized as the authority for maintaining and promoting the standards, policies and procedures in the Guide. An inventory of web applications and web developers will be completed. A process to keep the information up to date will be developed, documented and implemented.

Responsible Party: Rick Miller, CIO and Amar Yousif, CISO
Implementation Date: June 1, 2014

Web Application Firewall
SANS recommends the use of a WAF to protect web applications. A WAF provides protection when vulnerability cannot be removed from a web application. For example, a software vendor may be unwilling to remove a vulnerability from a web application. The WAF works by identifying known attack sites and signatures. The WAF shuts down the connection between the UTHealth web server that hosts a web application and attacker before the vulnerability is exploited. The WAF essentially works as a virtual patch for vulnerabilities that cannot be removed from a web application. UTHealth implemented a WAF approximately one year ago and is currently providing active protection to 22 web applications or sub applications. Most of the web applications protected by the WAF process PHI or are connected to applications that process PHI.

RECOMMENDATION 2: Information Security and the Office of the CIO should assess resources currently assigned to deploy the web application firewall and decide if the application is being deployed at an acceptable rate to cover the institution’s major web application risks.

Management’s Response: Information Technology Security and the office of the CIO will require the use of web application firewall as a matter of policy to protect the institution’s major web applications that provide access to patient data. The policy will be included in the ‘Web Applications Developer’s Standards, Policy & Procedures Guide’. Resources to deploy the web application firewall will be assessed and adjusted accordingly by the implementation date.

Responsible Party: Amar Yousif, CISO and Rick Miller, CIO.
Implementation Date: June 1, 2014
CONCLUSION

A&AS identified the need for improved oversight for the web application security process. Areas of improvement included: creating and implementing a reporting structure to oversee the web application process, creating a web application policy that addresses maintaining a web application inventory, identifying web developers, accelerating the deployment of the web application firewall, and creating an ongoing security scanning and vulnerability mitigation process. We would like to thank the individual web developers and departmental managers that assisted A&AS during this audit.

Daniel G. Sherman, MBA, CPA CIA
Assistant Vice President

DGS:twb

cc:
Audit Committee     Kevin Dillon     Jennifer Canup
Rick Miller          Amar Yousif

Audit Manager:      Tim Burr, MBA, CISA, CIA, CFE
Auditor Assigned:   Lieu Tran, MS

Issue Date: November 12, 2013