SAN DIEGO: AUDIT & MANAGEMENT ADVISORY SERVICES
0919

August 27, 2014

Min Yao
Assistant Vice Chancellor
Administrative Computing and Telecommunications
0928

Subject: ***Enterprise Security – Administrative Computing and Telecommunications***
Audit & Management Advisory Services Project 2014-05

The final audit report for Enterprise Security – Administrative Computing and Telecommunications, Audit Report 2014-05, is attached. We would like to thank all members of the department for their cooperation and assistance during the audit.

Because we were able to reach agreement regarding corrective actions to be taken in response to the audit recommendations, a formal response to the report is not requested.

UC wide policy requires that all draft audit reports, both printed (copied on tan paper for ease of identification) and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to AMAS personnel or destroy them at the conclusion of the audit. We also request that draft reports not be photocopied or otherwise redistributed.

David Meier
Director
Audit & Management Advisory Services

Attachment

cc: J. Bruner
E. Deere
B. DeMeulle
J. Denune
D. Rico
E. Strahm
S. Vacca

UC San Diego

AUDIT & MANAGEMENT ADVISORY SERVICES

Enterprise Security –Administrative Computing and Telecommunications

August 2014

Performed By:

Daren Kinser, Auditor
Greg Buchanan, Manager

Approved By:

David Meier, Director

Project Number: 2014-05

Enterprise Security –Administrative Computing and Telecommunications
Audit & Management Advisory Services Project 2014-05

Table of Contents

Enterprise Security –Administrative Computing and Telecommunications
Audit & Management Advisory Services Project 2014-05

I. Background

Audit & Management Advisory Services (AMAS) has completed a review of Enterprise (Logical) Security – Information Technology (Administrative Computing and Telecommunications) as part of the approved audit plan for Fiscal Year 2013-14. This report summarizes the results of our review.

Administrative Computing and Telecommunications (ACT) creates and supports the information technology (IT) environment used by the UC San Diego community. There are seven divisions within ACT, as follows:

- Campus Web Office
- Finance, Administration, & Help Desk
- IT-Infrastructure
- Information Technology Application Group (ITag)
- Middleware & Identity Management (IdM)
- Project Management Office (PMO) & Communications
- Telecom Planning

The services provided by ACT include maintenance and support for UCSD Active Directory and the Web Farm.

Active Directory

The ACT IT-Infrastructure division is responsible for implementation, administration, and maintenance of Active Directory (AD). From a technical perspective, AD is a Microsoft directory service that runs on Microsoft server operating systems starting with Windows 2000 Server. AD stores information about objects on the UCSD network and makes them available to network administrators and users. Objects include servers and printers as well as user accounts, user groups and computer accounts. AD allows simplified network resource management while providing robust authentication and authorization services.

AD is used by UCSD staff, faculty and students to authenticate and authorize access to a number of centralized and distributed systems and applications, as well as the Campus and Health System wireless and virtual private networks. AD is analogous to a tree-like structure, with members of the ACT IT-Infrastructure groups residing at the top level. Access to resources propagates from the top down. The extent to which users can access resources contained within AD depends on a user's group membership, and the level of access that is assigned to that group.

Because of the sensitivity of some of the resources contained within AD, it is imperative that user membership at the highest levels is limited to the appropriate individuals, and that high level administrator accounts are adequately secured. It is also important that group membership for all users is appropriate.

Web Farm

The ACT managed Web Farm is a group of Linux web servers configured into a redundant cluster hosting a large number of campus business and academic web applications. All Link family applications are internally developed by ACT Enterprise Information Services, and are hosted on Web Farm servers. These applications include TritonLink and FinancialLink, as well as business and personal tools like MyTravel and MyTraining. Beyond the firewall rules in place at the campus border, the Web Farm servers are protected by a set of host based IPTables firewall rules.

II. Audit Objective, Scope, and Procedures

The objective of this review was to evaluate the effectiveness of practices implemented by ACT for logical security of AD and the Web Farm. The scope of our review was limited to AD account management practices, and application level security of Web Farm hosted applications.

To achieve our objectives pertaining to security of AD we completed the following:

- Interviewed the Director of Enterprise Infrastructure and the AD Manager;
- Reviewed border and host based firewall rules designed to protect AD servers;
- Ran a Microsoft Baseline Security Analyzer and Best Practices Analyzer test on an AD server to identify possible common security misconfigurations;
- Tested two-factor authentication to determine proper functionality as well as appropriate user account membership in level one and level two groups; and
- Reviewed a sample of ACT user accounts and groups for inappropriate members.

To achieve our objectives pertaining to security of the Web Farm we completed the following:

- Interviewed the following individuals from ACT:
  - Director of Enterprise Infrastructure,
  - Manager of Network Applications,
  - Executive Director of the IT-Applications Group,
  - Director of Academic Applications,
  - FinancialLink Manager, and
  - an IT-Applications Group Programmer Analyst;
- Completed a web application vulnerability scan using Hewlett-Packard WebInspect tool on three web applications internally developed and maintained by ACT;
- Reviewed UCS user list for inappropriate accounts; and
- Reviewed host based firewall rules protecting the Web Farm.

III. Conclusion

We concluded that ACT's implemented security practices were generally adequate to provide logical security for AD and the Web Farm. ACTs management of high level AD users and groups appeared sufficient to ensure access to resources was appropriate. In addition, host based firewall rules appeared to be appropriately configured to protect AD servers. Further, access to the Cisco Unified Computing System (UCS), which is the architecture ACT maintains to house the virtual environment utilized by AD and the Web Farm, appeared reasonable.

However, our web application vulnerability scans found that some essential and sensitive Web Farm applications contained a small number of high risk vulnerabilities. Details of the vulnerabilities identified by the web vulnerability scan was provided by ACT management under separate cover.

IV. Observation and Management Corrective Action

A. Web Application Security

Essential and sensitive web applications developed and maintained by ACT were found to contain a small number of high risk vulnerabilities.

ACT develops web applications that support a wide variety of different business and academic processes. Some of the internally developed web applications are considered essential to the campus in that if there is a loss of confidentiality, availability or integrity of the application or underlying database, one or more business processes could be significantly impacted.

Another consideration is the sensitivity of the underlying data that is used or processed by a web application. Web developers must be especially careful to develop secure applications that use or handle personal identity information (PII), or student records that may be covered under the Family Educational Rights and Privacy Act (FERPA).

During the review, AMAS completed web application vulnerability scans on three judgmentally selected web applications that were developed and maintained by ACT. Based on the nature of these applications, they are highly utilized by faculty, staff and students, and process sensitive information. The web application vulnerability scan reported a small number of high level vulnerabilities. ACT web developers have acknowledged that some of the reported vulnerabilities exist, and were working on remediating the vulnerabilities.

Management Corrective Action:

ACT web application developers have addressed the vulnerabilities identified during the web application scans. AMAS has rescanned and validated that the vulnerabilities were remediated.