INTERNAL AUDIT
IAS
ADVISORY SERVICES

Internal Audit Report

DATA CENTER LOGICAL SECURITY

Report No. SC-12-06
June 2012

David Lane
Principal IT Auditor

Jim Dougherty
Principal Auditor

Approved
Barry Long, Director
Internal Audit & Advisory Services

UC SANTA CRUZ

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Internal Audit & Advisory Services (IAS) has completed an audit of Data Center Logical Security. The purpose of the audit was to evaluate the adequacy of logical security controls over the UCSC Data Center Windows virtual environment.

In general, logical security controls over the Data Center Windows virtual environment were adequate in the areas of system patching, account permissions, change controls, and the software resided behind a firewall.

However, opportunities were identified for improving logical security controls within the Data Center including system activity monitoring and intrusion detection; plans to implement improved controls over Data Center firewalls, including the virtual private network; and adding reporting functionality for the Support Center to more effectively and efficiently identify employee access privileges to information system resources.

The following issues requiring management corrective action were identified during the review:

A. **Review of Information System Activity Records:** There is not an adequate log management infrastructure to allow for an effective and efficient review of audit logs of the virtual environment, nor is there an intrusion detection or prevention system in the Data Center that generates reports tracking malicious traffic or security incidents.

B. **Firewall/VPN management:** There was no standardized user vetting process or predefined user groups, resulting in overly complex access control lists with little assurance that all user permissions were appropriate for their job duties.

C. **Account Access Management System:** The campus does not have an account management system to efficiently identify and tract employee access privileges to campus computing resources.

Management has agreed to all corrective actions recommended to address risks identified in these areas. Observations and related management corrective actions are described in greater detail in section III of this report.

II. INTRODUCTION

Purpose

The purpose of the audit was to evaluate the adequacy of logical security controls over the UCSC Data Center Windows virtual environment.

Background

Logical security consists of software safeguards for an organization's systems, including user identification and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or securely access information in a network or a workstation. It is a subset of computer security.

At UCSC, the Data Center Operations (DCO), a unit of Information Technology Systems (ITS) Core Technologies, manages the campus' data center resources and provides support services for enterprise applications and server hosting.

The Unix and Windows virtual environment platforms are maintained within the UCSC Data Center. The Unix platform includes most campus enterprise systems; and the Windows virtual environment hosts many other systems including the campus data warehouse and Infoview.

The term "virtual environment" refers to a software implementation of computers that execute programs like physical computers. A virtual environment configuration allows a more efficient use of the physical space in the Data Center, as multiple virtual computers, also known as virtual machines (VM), can be hosted by a single physical computer/server. This efficiency has allowed ITS to host more campus systems on virtual servers within the Data Center, which can provide them with a safe and secure location and operational support.

Scope

We reviewed documentation and interviewed management and staff of ITS units, including Core Technologies departments, e.g. Data Center Operations, and Windows Systems, including the VMware System; the Architecture & Infrastructure Group; and the ITS Support Center department of Client Services and Security; and the Data Warehouse unit of Planning & Budget.

Our review of systems, procedures and practices included:

- VCenter control environment, permissions, change management, patch management, audit and password policies, audit log review, and intrusion detection;
- Data Center firewall access control lists (ACL), including VPN policy and plans to update the VPN and firewalls;
- Data Warehouse user accounts and procedures for granting permissions;
- ITS Support Center account provisioning through the IT Request system.

As the physical servers that host the virtual environment are housed in the Data Center, we examined the logical controls for access to virtual systems through the Data Center firewalls, including virtual private networks (VPN). We focused our review on the logical security applicable to the virtual environment in general and to system hosted within that environment.

We also examined the access controls that were applied to the command center (VCenter) used to manage the Windows virtual environment. We then tested the access controls of a specific system hosted in that environment and how users generally obtain access to campus systems that are included in that environment. This involved a review of account provisioning through the IT Request system managed by the ITS Support Center that receives requests for access to campus systems.

As logical security pertains to every system and workstation on campus, we restricted our scope to the Data Center and within it the Windows virtual environment; an area we have not reviewed previously.

III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

A.	Review of Information System Activity Records	
There is not an adequate log management infrastructure to allow for an effective and efficient review of audit logs of the virtual environment, nor is there an intrusion detection or prevention system in the Data Center that generates reports tracking malicious traffic or security incidents.		
Risk Statement/Effect		
1. Analysis of the large volume of computer-generated log messages may not identify security threats timely. 2. Data Center systems may be attacked without detection and preventable attacks may succeed.		
Agreements		
A.1	ITS Core Technologies will communicate log review responsibilities to system administrators; provide appropriate training for effective log review; provide guidance on tools for efficient log review; and implement procedures for regular log review.	Implementation Date July 1, 2013 Responsible Manager Infrastructure Security Manager
A.2	ITS Core Technologies will acquire appropriate intrusion detection or prevention systems and implement a procedure to regularly review their records of information system activity.	Implementation Date July 1, 2013 Responsible Manager Infrastructure Security Manager

A. Review of Information System Activity Records – Detailed Discussion

Log Management

Computer security log management is the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management helps to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems.

Logs are also useful for establishing baselines, performing auditing and forensic analysis, supporting internal investigations, and identifying operational trends and long-term problems. Organizations may also store and analyze certain logs for compliance.

At the present time, the VMware systems administrator does not review system audit logs. While the current log review policy is to review logs in response to security incidents the VMware administrator has not been made aware of such incidents.

The fundamental problem with log management is balancing a limited amount of log management resources with the continuous supply of log data. Log management is particularly critical when dealing with restricted information.

Core Technologies has plans to utilize the virtual environment to transmit and store electronic protected health information (ePHI) which is considered restricted information and protected by federal law (HIPAA) and University policy and procedures. HIPAA, section §164.308(a)(1)(ii)(D) – "Information System Activity Review" (Required) states:

> Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

To enhance the level of log management controls particularly critical when hosting restricted data, Core Tech should consider a strategy for log review within a wider log management protocol depending on the number, volume, and variety of computer security logs under its purview.

We encourage Core Technologies to plan for an appropriate log management infrastructure that includes tools to help the VMware system administrator (and others) analyze and report on the data that logs accumulate.

Intrusion Detection System

The ITS Data Center does not have an intrusion detection or prevention system (IDPS). Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

An intrusion detection system (IDS) is software that automates the intrusion detection process. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents automatically.

Because of the increasing dependence on information systems and the prevalence and potential impact of intrusions against those systems, IDPS have become a necessary addition to the security infrastructure of nearly every organization. Core Technologies plans to acquire and install an IDPS within the next 12 months.

B.	Firewall/VPN Management	
There was no standardized user vetting process or predefined user groups, resulting in overly complex access control lists with little assurance that all user permissions where appropriate for their job duties.		
Risk Statement/Effect		
Overly complex VPN configuration increases the likelihood that user's permissions are not the least required to do their job and the workload in managing the VPN is significantly increased. Static IP addresses are unencrypted connections that expose communication to unauthorized access, which potentially allow hackers to steal passwords and obtain restricted information.		
Agreements		
B.1	ITS will complete plans to decommission the DC5 firewall, eliminate all privileged user permissions from the campus VPN, and eliminate all static IP addresses that allow datacenter access bypassing the VPN.	Implementation Date November 1, 2012 Responsible Manager Infrastructure Security Manager
B.2	ITS will implement existing plans so that all user requests for privileged access to datacenter assets will be vetted by an approving authority, who shall obtain appropriate authorizations, assign appropriate rule groups, and enter work orders in the ITR so that technical staff can configure the datacenter VPN to provide appropriate permissions.	Implementation Date February 1, 2013 Responsible Manager Infrastructure Security Manager

B. Firewall/VPN Management – Detailed Discussion

At the time of the audit, the campus had three firewalls and VPNs controlling access to Data Center systems. These firewall/VPNs are referred to as the Data Center VPN, the Campus VPN and the DC5 VPN. All three function as both a VPN and a firewall. ITS is in the process of implementing plans to harden, standardize and streamline the use and administration of these systems.

The plan will introduce new methodology for the Architecture & Infrastructure Group to define group roles and user needs for the Data Center VPN and the security team to appropriately configure the Data Center VPN. One part of the plan is to decommission the DC5 VPN and convert all the current DC5 users to the Data Center VPN. The Architecture & Infrastructure Group is currently contacting DC5 users via phone and email to get them moved to the campus VPN.

The project plan also calls for configuring the Campus VPN to provide users with an on-campus internet protocol (IP) address, but not privileged access to any Data Center systems. Many campus systems and file servers can only be accessed via an on-campus IP address which can be obtained securely via the campus VPN. Eventually it is expected that all new employees will automatically receive a campus VPN account as part of the hiring process.

Currently the Campus VPN is often used to obtain privileged access to Data Center systems. Part of the challenge in moving all privileged users to the Data Center VPN is determining the appropriate permissions for each user and creating rule groups to match those permissions. For many years, specific rule groups were not defined or used to configure firewalls. ACLs were simply added as access requests were received. This resulted in over 18,000 ACLs with much duplication.

In the past year, the security team has eliminated 16,000 ACLs as part of this project. They have also implemented a firewall management tool that will allow them to assign permissions based on well-defined groups and identify users whose permissions do not match group roles. This process lacked a good vetting procedure to assure permissions were always appropriate, based on a user's needs and job functions.

In the new procedure, the Architecture & Infrastructure Group will vet each user's needs and job duties, assign the appropriate rule group(s) for the Data Center VPN on a tracking spreadsheet, and enter an IT Request ticket that the IT security staff will use to configure the Data Center VPN. This process should provide better review and separation of duties so that privileged access is appropriately controlled.

Most campus VPN users who obtain privileged access have not yet been informed that they will need to move to the Data Center VPN, but as the vetting process is completed and rule groups are created the Architecture & Infrastructure Group will contact this group of users as well. The same VPN client is used to access both the Campus and Data Center VPNs, so users will only need to connect to a different server once their permissions are in place.

In our review of the existing VPN/firewall ACLs, we found numerous employees had static IP addresses hard coded in the firewall which allowed privileged Data Center access without going through a VPN. These connections were not encrypted so any data transmissions between the workstation and the Data Center system, potentially including passwords and restricted data, were plain text and could have been compromised by network sniffing utilities and/or web based malware.

The static IP address connections we reviewed in detail for Data Warehouse accounts all used channels that were encrypted by the protocols employed, e.g. secure file transfer protocol (SFTP), Secure

Sockets Layer (SSL), or similar technologies. However, by not enforcing encryption at the initial authentication (VPN) stage it is unknown if all Data Center connections were encrypted.

C.	Account Access Management System	
The campus does not have an account management system to efficiently identify and tract employee access privileges to campus computing resources.		
Risk Statement/Effect		
Limited assurance that employees have appropriate access to computer accounts according to the principle of least privilege.		
Agreements		
C.	ITS Client Services & Security will conduct a cost/benefit analysis for implementing an employee account reporting system, such as one that would interface with the IT Request system to efficiently record and report on employee access to campus computing system accounts.	Implementation Date July 1, 2013 Responsible Manager Director - Client Services & Security

C. Account Access Management System – Detailed Discussion

One aspect of effective logical security control includes knowing what systems access employees have been granted. At the present time, controls over account access management are lacking as the campus does not have the capacity to report out on the access rights of employees to various campus systems.

Without an adequate account management system that enables an efficient way to record and report on accounts that employees are assigned, it is difficult to ensure that accounts an employee has are appropriate. Inappropriate accounts would allow access to information and perhaps its manipulation that would violate the basic principle of information security - that of least privilege, i.e. that people should be assigned the fewest privileges consistent with their assigned duties and functions.

IT Request, the campus system used to request system access centrally, is a primary source of information on changes to employee access, but does not have an adequate reporting functionality. Developing and implementing a functionality that reports on employee information system accounts using the information contained in IT Request would be an incremental step in having an efficient and effective way to obtain information on employee account access to campus systems and to help ensure that accounts are appropriate.

There are other steps needed to improve logical security access controls, including:

- Automatic notification of changes in employee status. Currently, we rely on employee supervisors to provide timely notification of employee status changes. As these changes occur, whether to different positions within the campus or separation from the university, their need to

access systems based on job duties is likely to change. UC Path offers the promise of automatic notification of status change.

- Efficient onboarding and offboarding of accounts. The campus has developed a consistent authentication method in CruzID that more systems are using. Consequently, access to these systems can be disabled by the centrally administered CruzID.
- Consistent use of a centralized method for requesting and receiving account access. Increasingly, the campus is using IT Request to request account access. The Support Center, which manages IT Request, is in partnership with system owners who grant access, and is therefore well positioned to identify accounts of individual employees. The more the campus makes use of IT Request for this purpose the more comprehensive will be its reports on employee accounts.

In a campus with diverse and distributed IT systems, it may never be possible to centrally track all employee accounts. However, we have an opportunity to improve account management for those accounts that are setup centrally.

The Support Center has developed a compensating control to email a group of system owners monthly of employee separations based on PPS reports, but this does not address position changes within the campus or timely account closure.

****