2011 International Conference on Information and Electronics Engineering
IPCSIT vol.6 (2011) © (2011) IACSIT Press, Singapore

An IT Security Investigation into the Email Systems of Selected Local Government Councils in WA

Sunsern Limwiriyakul and Craig Valli

School of Computer and Security Science, Edith Cowan University, Perth, Western Australia
slimwiri@our.ecu.edu.au

Abstract. This paper investigated information technology (IT) security on the email systems at three selected Western Australian (WA) local government councils. The study was based on several industries and national benchmarking standards and investigated the email system security. The scope of the analysis included the architecture, the infrastructure devices, port scanning and vulnerabilities on the email server, email spoofing and email vendor auditing. The study aims to provide an email security framework which can be easily adopted and is flexible enough for use in any city councils or other organizations.

Keywords: email system, IT security, framework

1. Introduction

Electronic mail (email) is a common and widely used internet related technology throughout industry and government organizations such as WA's local government councils. Other internet related technologies that are being used in these councils, are voice over internet protocol (VoIP), geographic information system (GIS), global position system (GPS) and online services systems. These technologies are used to provide both data and voice services to the councils and their residents. Specialist online services such as web information, library and payment systems are also being provided by the WA's councils to its residents and the public.

A major concern of all the selected WA's councils in the provision of these internet services is the information and communications technology (ICT) security system. The ICT security imperative includes both confidentiality and privacy of users' information over the internet especially in relation to the online payments, online library and email systems.

This paper aims to investigate the IT security of the email system which is currently deployed at the selected WA councils, in order to investigate whether the system has been implemented securely in a way that meets national and international security standards.

Three WA local government councils were selected based on their willingness to provide sufficient and relevant data for testing and analysis. Reciprocally, this study provided feedback and security enhancement recommendations to the selected councils. The tests were collected on a real-time basis for all three selected councils. In addition, the testing analysis and implementation framework, results findings and discussions were also included as report submissions to the individual councils for which the study was undertaken.

2. Methodology: Implementation framework

The implementation framework was based on the level of security of the council's email system. There were various testing techniques which were adapted for use as components within this framework. The testing techniques included were Section C of Open Source Security Testing Methodology (OSSTMM) 2.2 [7], the Center for Internet Security (CIS) Benchmark for Exchange 2007 for Windows Server 2003 Version 1.0 [1], Information Systems Security Assessment Framework (ISSAF) version 0.2.1 [2], National Institute of Standards and Technology (NIST) and other related testing information from various sources such as World Wide Web (WWW), journal, books and personal interviews.

The implementation framework for the testing of the security of the email system consisted of five stages, which included (1) network surveying; (2) internetwork infrastructure review; (3) services and system identification, port scanning and vulnerability detection of the email system servers; (4) spoofing testing and vendor security benchmarking; and (5) email system security policy review. See Fig.1 for more details.

Stage1: The network surveying stage was used to collect information on the council's email system through the use of the following two artifacts:

- Overall network diagram for the internetwork linkages, including the Demilitarized Zone (DMZ) infrastructure connectivity of the email system; and
- Configuration codes and device specifications of all internetworking devices such as the internet border router, the internet firewall(s), the external/DMZ/internal switch(s), the reverse proxy server and the related email system.

In addition, in this stage the overall email system architecture including its internetwork infrastructure was also reviewed.

Stage 2: The internetwork infrastructure devices review was used to review the related specification and configuration codes as part of the data collection of the internetwork infrastructure devices of the email system of the three selected councils. The internetwork infrastructure devices consisted of the internet border router, the IDS/IPS, the firewall(s), the DMZ switch(s) and the reverse proxy server (Council C only).

Stage 3: In this stage, both network mapper (NMAP) [4] and GFI LANguard [3] network scanning tools were used for scanning the council's email system (email server and in-house spam blocker(s)). NMAP with GUI standard (open source Zenmap version 5.0) for Windows XP version with slow comprehensive scan option, and GFI LANguard version 9.0 with the full scan option, were run for all three testing steps (services and system identification, port scanning and vulnerabilities testing), at all of the three selected councils.

Stage 4: This testing stage involved two steps which included the email spoofing testing and the email vendor security auditing as follows:

- Email spoofing testing which was adapted from the OSSTMM 2.2 email spoofing template as a guideline. The purpose of this testing was to test the email server against any spoofing attacks; and
- Email vendor security auditing which was specifically modified to suit the email application server system of each selected council. However, the CIS Benchmark for Exchange 2007 for Windows Server 2003 version 1.0 (recommended Security Setting for Exchange Controls template) was modified and used at all three selected councils. This was due to the fact that the MS Exchange 2007 email server platform was being used in all three selected councils.

Stage 5: The email system security policy review; the intention of this stage was to review the IT security policy in relation to the email system which covered the internetwork architecture and its devices, the email server(s), the authorization, the authentication and the accounting of the email system in each of the selected councils.

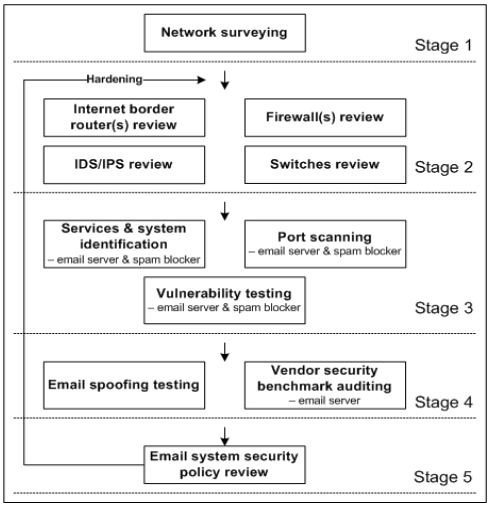

Fig. 1: An implementation framework

3. Current email system architecture and email protocols

Council A

Council A's email system has one MS Exchange 2007 email server which was located in the council's internal network and one appliance Symantec Mail Security Suite 5.0 spam blocker server which was located in the council's DMZ network. The internetwork infrastructure consists of a Cisco 2811 internet border router, two Cisco ASA (5520) firewalls and three Cisco Catalyst 3650SM switches. See Fig. 2 for more details.

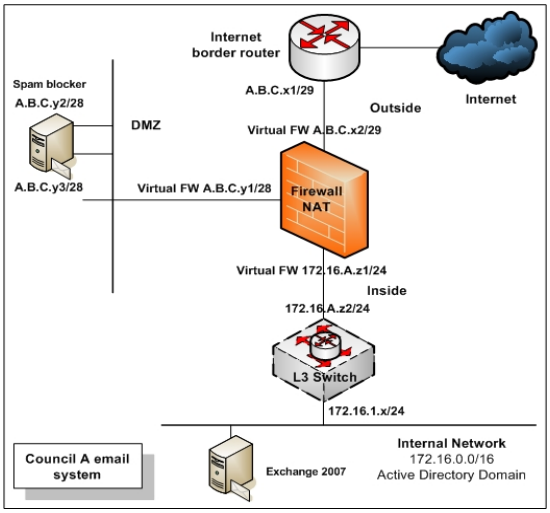

Fig. 2: Council A's current email network diagram

Council B

Council B's email system consists of one MS Exchange 2007 email server, and two Cisco IronPort C150 spam blocker servers. The email server was located in the council's internal network while the two spam blockers were in the DMZ area. The council's internetwork (DMZ) infrastructure devices consists of one Cisco 2811 internet border router, two CheckPoint Firewalls 1 (UTM-1 272) and one Cisco Catalyst 3750G switch. The switch serves the internetwork, DMZ and internal network connectivity. See Fig. 3 for more details.

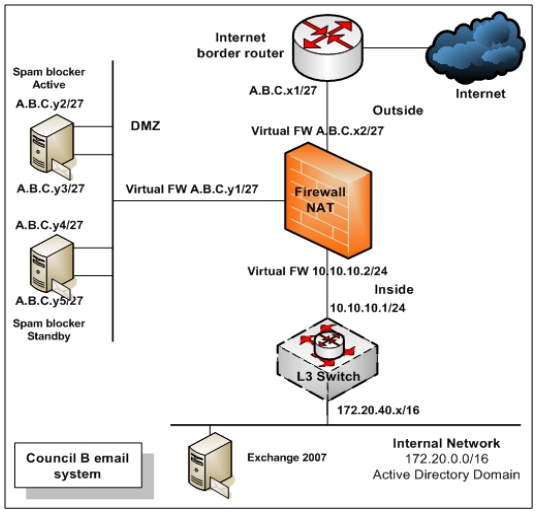

Fig. 3: Council B's current email network diagram

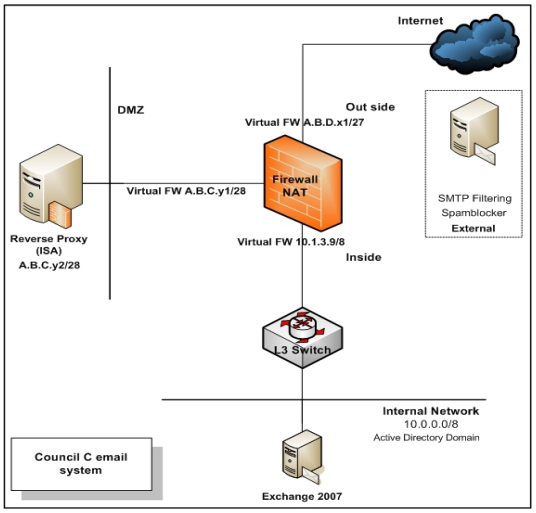

Fig. 4: Council C's current email network diagram

Council C

Council C's email system consists of one MS Exchange 2007 email server and one ISA 2006 reverse proxy server which were located in the internal network and the DMZ network respectively. Council C uses an external spam blocker service for scanning unwanted spam mail. See Fig. 4 for more details.

The infrastructure consisted of two Juniper (SSG-350M) firewalls and one HP (E5412zl) switch. The switch provides connectivity for the internetwork, the DMZ and the internal networks. The switch also acts as an internal central core switch which connects to all the council's access switches. See Fig. 4 for more details.

Email protocols

Currently Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol Secure (HTTPS) are used for standard email and webmail respectively at all three selected councils. However, other related email protocols such as Post Office Protocol (POP3) and Internet Message Access Protocol (IMAP) were not used at any of the three selected councils.

4. Data analysis and results finding

Data was collected, analysed and tested using the five stages of the implementation framework as described in Section 2. The results and findings of all the five stages on each the email systems are displayed in a table format for each stage for simplicity.

Stage 1: Network surveying – The email related technical network documentation was gathered for each of the selected councils. They were found to be only partly updated. The MS Exchange 2007 email server was deployed as part of a single server architecture which was not according to the best practice recommendations for larger organizations [5], [6] at all three selected councils.

Stage 2: Internetwork infrastructure reviews

Table 1: Internet border router review

Email system infrastructure review: Internet border router			
Descriptions	***Council A***	***Council B***	***Council C***
Internet border router deployed	Yes	Yes	No
Internet border router redundancy/alternative internet link deployed	No	No	No
The router configured against IP spoofing attacks	No	No	NA
Access Control List (ACL) rule to allow ONLY permitted related email protocols for in/out	No	No	NA
Best practice user name and/or password and strong password encryption (MD5) used	Yes	No	NA
Allow administration of the router via unsecured communications (HTTP and Telnet)	Yes	Yes	NA

Table 2: IDS/IPS review

Email system infrastructure review: IDS/IPS			
Descriptions	***Council A***	***Council B***	***Council C***
IDS feature/device in existence	Yes, on the internet border router	Yes, on the internet border router	No
IDS enabled	No	No	NA
IPS feature/device in existence	Yes, on the firewall	No, but can be added on to the firewall	Yes, on the firewall
IPS enabled	No	NA	Yes
IPS depth inspection on SMTP and HTTPS enabled	NA	NA	Yes

Table 3: Firewall review

Email system infrastructure review: Firewall			
Descriptions	***Council A***	***Council B***	***Council C***
Firewall deployed	Yes	Yes	Yes
Firewall redundancy deployed	Yes	Yes	Yes
Stateful firewall	Yes	Yes	Yes
Firewall configuration rule to allow ONLY permitted related email protocols for in/out	No	No	No

Best practice user name and/or password and strong password encryption (MD5) used	Yes	No	No
Allow administration of the firewall via unsecured communications (HTTP and Telnet)	Yes	Yes	Yes

Table 4: Switches review

Email system infrastructure review: Switches			
Descriptions	***Council A***	***Council B***	***Council C***
Standalone external gateway switch deployed	Yes	No	No
Standalone DMZ switch deployed	Yes	No	No
Appropriate VLAN used	Yes	Yes	Partly
ACL applied to block unwanted devices	Yes	No	No
Anti ARP spoofing and poison attacks enabled	No	No	No
Port broadcast-storm control enabled	No	No	No
Port security limits MAC address to a port enabled	No	No	No
Best practice user name and/or password and strong password encryption (MD5) used	Yes	No	No
Allow administration of the firewall via unsecured communications (HTTP and Telnet)	Yes, HTTP only	Yes	Yes

Stage 3: Auditing review of the email servers of the three selected councils (services and system identification, port scanning and vulnerability detection).

Table 5: Audit review on the council email servers

Auditing review on the councils' email servers			
Descriptions	***Council A***	***Council B***	***Council C***
Best practice user name and/or password used on the operating system (OS)	No	No	No
Best practice used on OS password policy	No	No	No
Unnecessary TCP and UDP services ports opened	Yes	Yes	Yes
Missing patches	Yes	Yes	Yes
Missing service packs	Yes	No	Yes

Table 6: Audit review on the council spam blockers

Auditing review on the councils' spam blockers			
Descriptions	***Council A***	***Council B***	***Council C***
Best practice user name and/or password used	Yes	Yes	NA
Allow administration of the spam blocker via unsecured communications (HTTP and Telnet)	No	No	NA
Unnecessary TCP and UDP services ports opened	No	No	NA

Stage 4: Spoofing testing and vendor security benchmarking

Table 7: Spoofing review

Spoofing review on the councils' email servers			
Descriptions	***Council A***	***Council B***	***Council C***
Using the email server, sending an email from one internal address to another internal address	Yes	Yes	Yes
Using the email server, sending an email from one external address to another external address	No	No	No
Using the email server, sending an email from one internal address to an external address	No	No	No
Using the email server, sending an email from one external address to an internal address	Yes	Yes	Yes

Table 8: Vendor security benchmarking review

MS Exchange 2007 benchmark review on the councils' email servers			
Descriptions	***Council A***	***Council B***	***Council C***
Configuration of the council's Mailbox server role as per recommended best practice	Partly	Partly	Partly
Configuration of the council's Hub Transport server role as per recommended best practice	Partly	Partly	Partly
Configuration of the council's Client Access server role as per recommended best practice	Partly	Partly	Partly

Stage 5: Email system security policy review

Table 9: Email systems security policy review

Email systems security policy review on the selected councils			
Descriptions	***Council A***	***Council B***	***Council C***
General email usages policy in use	Yes	Yes	Yes
General email related (internet) usages policy in use	Yes	Yes	Yes
Information security policy (email related) to the councils' staff in use	No	No	No
Information security policy – technical to the councils' IT staff in use	No	No	No
Regular update or review the email related policy	No	No	No
Advise general email usages including security awareness to new starter	Yes	Yes	Yes
Frequently advise their staff for IT security information including email related	No	No	No

5. Discussion

As per recommendations to best practice, there were inadequate settings, configurations and implementations of the related email system devices in all five testing stages based on the results presented earlier. These shortcomings are a possible cause of concern for potential risks in the three selected WA council's email systems.

With respect to these inadequacies in the operation of the related email system devices, there were six main factors uncovered in this study. They include (1) the lack of IT security standards awareness of industrial best practices by staff, (2) inadequate specific knowledge, (3) inefficient communication between the staff, (4) limited IT training for staff as a result of limited budget, (5) staff not having enough time for task completion and (6) reliance on external consultants for specific IT projects.

1) The lack of IT security standards awareness of industrial best practices by staff: There were two audits conducted which included several discussions and meetings for each of the selected councils. For example, there was no standalone DMZ switch deployed at both Councils B and C. In addition, the following lists summarises the overall common findings which related to the first factor from the three selected councils:
   - There was no internet border router redundancy/alternative internet link deployed at all selected councils; and
   - The architectural design of the email servers was not in line with the MS Exchange 2007 recommendations of best practices [5] [6] at all selected councils.
2) Inadequate specific knowledge: There was evidence of missed and inadequate configuration of the internet border router's ACL, the DMZ switch's codes, the firewall rules, the unnecessary ports and the services installed on the email servers at all three selected councils. This was due to the fact that the staff were not well versed in these technical areas for the correct implementation. See Tables 1 to 5 for more details.
3) Inefficient communication between the IT staff: It was evident that the firewalls for the email servers were inadequately configured. For example, wrong port numbers were assigned as a result of oral miscommunication between the IT staff at all three selected councils. In addition, the lack of a

change management process at all three selected councils also contributed to the potential for inefficient communication between the IT staff.

4) Limited IT training for staff as a result of a limited training budget: There were limited IT training budgets allocated at all three selected councils. Typically, the IT administrator was able to attend only one or less related IT training course per year. This occurred at all three selected councils over the past five years. This training policy may be directly attributed to insufficient knowledge for managing the email system. In addition, all the IT administrators at all selected councils have never attended specific industry or equivalent training in both firewall and MS Exchange 2007 related courses.
5) Insufficient time for task completion by the IT staff: At all three selected councils, the IT staff had several duties and diverse tasks which sometimes resulted in some of the tasks being continuously left incomplete or unattended. Additionally, there was also no time left for proper documentation at all three councils as presented in Stage 1.
6) Reliance on external consultants for specific IT projects: The three selected councils reliance on outsourcing to solve the expertise problem may be a possible disadvantage in terms of a lack of knowledge transfer for the IT staff. This is evidenced by the fact that the firewall systems at all three selected councils were implemented by external consultants. In addition, the email servers (MS Exchange 2007) at all three selected councils were also deployed by external consultants. Consequently, historical records of implementation and maintenance were deficient and not readily available.

6. Conclusion

As a result of this study, the implementation framework, presented here can be used to audit an email system, particularly MS Exchange 2007. It is also possible for this framework to be adopted by any councils or organizations with similar architecture. The adoption of the framework may be used as a guideline in auditing or testing the security of their email system provided that it is in compliance with their existing ICT policies. Furthermore, the framework may also be used as a basis for documentation of their email system.

7. References

[1] CIS, “Center for Internet Security Benchmark for Exchange 2007 for Windows Server 2003 Version 1.0,” 2007, http://www.cisecurity.org/tools2/exchange/CIS_Benchmark_Exchange2007_1.0.pdf.

[2] B. Rathore, O. Herrera, S. Raman, M. Brunner, P. Brunati, U. Chavan, M. Dilaj, and R. Subramaniam, “Information Systems Security Assessment Framework (ISSAF) draft 0.2.1 Information System Security Groups,” 2006, http://www.oissg.org/downloads/issaf-0.2/index.php.

[3] GFI, “Network vulnerability scanner, security scanner and port scanner,” 2009, http://www.gfi.com/lannetscan/.

[4] G. Lyon, “Nmap Security Scanner,” 2008, http://nmap.org/download.html.

[5] Microsoft Exchange Documentation Team, “Exchange Server 2007 Planning,” 2007, http://www.microsoft.com/downloads/details.aspx?FamilyID=1A6EFDD6-D80E-489D-9A1D-8F3E01BAA3C5&displaylang=en&displaylang=en.

[6] Microsoft TechNet, “Exchange Server 2007 Design and Architecture at Microsoft,” 2007, http://www.microsoft.com/downloads/details.aspx?FamilyID=98C522BC-814A-421A-99C0-D964ED119C0D&displaylang=en&displaylang=en.

[7] P. Herzog, “OSSTMM 2.2 Open-Source Security Testing Methodology Manual,” 2006, http://isecom.securenetltd.com/osstmm.en.2.2.pdf.