A PROPOSED FRAMEWORK FOR NETWORK SECURITY AUDIT TRAIL FOR MINISTRY OF DOMESTIC TRADE & CONSUMER AFFAIRS

A thesis submitted to the Graduate School in partial
Fulfillment of the requirement for the degree
Master of Science (Information Technology)
Universiti Utara Malaysia

By

Fara Binti Jamal

PUSAT PENGAJIAN SISWAZAH
(Centre For Graduate Studies)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

FARA BINTI JAMAL

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/ her project paper of the following title)

A PROPOSED FRAMEWORK FOR NETWORK SECURITY AUDIT TRAIL FOR MINISTRY OF DOMESTIC TRADE & CONSUMER AFFAIRS

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **PM DR SUHAIDI HASSAN**

Tandatangan
(Signature) : _____

Tarikh
(Date) : 8/12/2006

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to

Dean of Graduate School
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.

ABSTRACT

Perkembangan Internet yang pesat terutamanya dalam aplikasi web pada tahun 1989, telah mendorong kepada penggunaan rangkaian secara berleluasa. Organisasi tidak mengira kerajaan atau swasta bergantung kepada rangkaian dalam menguruskan perniagaan harian. Ancaman komputer seperti virus, *worms* dan serangan seperti DDOS, penggodam, berkembang selari dengan perkembangan rangkaian. Banyak organisasi yang menghadapi masalah rangkaian sama ada rangkaian dalaman ataupun rangkaian luaran. Pemasangan peralatan rangkaian untuk melindungi rangkaian dari serangan adalah tidak memadai sekiranya organisasi tidak dapat mencari punca utama masalah keselamatan pada rangkaian. Ini boleh dilakukan dengan melaksanakan audit keselamatan rangkaian. Ia adalah satu cara terbaik untuk memahami kedudukan semasa sesebuah organisasi dan masalah yang dihadapi berkaitan dengan rangkaian. Untuk melaksanakan audit ini bergantung kepada organisasi itu sendiri sama ada untuk menggunakan rangka kerja audit sedia ada atau mereka bentuk rangka kerja audit sendiri mengikut keperluan organisasi.

ABSTRACT

The tremendous growth of the Internet, and particularly the World Wide Web (The Web) on 1989, has led to mass usage of networking. Organization regardless of government or private sector depends on their network to run the business. Computer threats such as virus, worms and attack like DDOS, hackers emerge align with the improvement of network. Many organization face problems on their network regardless of Local or Wide area network. Deployment of security equipments to protect the network is useless if the organization cannot track the root of the security problems. This can actually be done by conducting a network security audit. It is the best way to understand the organization security stand and the problem involve with the network. It depends on the organization weather to use the framework design by other researcher or customize their own framework in order to conduct network security audit in the organization.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I wish to thank all the people that involve direct or indirectly in helping me to complete this paper. A special thanks to my supervisor, Associate Professor Dr Suhaidi Hassas whom had guide me throughout this project, my parent En Jamal Mohamad and Puan Sham Mohamed for all the support given to me and my MscIT collogues who give me some guide regarding the report. Thank you also to Tuan Haji Mohamed Adani Bin Haji Ahmad, IT Manager in MDTCA whish had allowed me to conduct the network in the organization and give full support to me as well as other MDTCA officer. Special thanks also to Sapura engineer, MAMPU officer and Puan Nor'Azuwa Muhamad Pahri from NISER who had helped me completed this project.

I also want to thanks my friend En Roslan Bin Jali, En Mohd Hasnulmisam Bin Hassim, En Salim Mohamad Ghani (3COM), En Mohd Hasdi Bin Abdul Halim (MMA) and Mr Manwin Ang (BigFIX) who had help me a lot through the implementation stage.

Also thanks to the survey group that give full cooperation in answering questions given. It was greatly appreciated. I will not forget all helped and thank you very much.

1.0 INTRODUCTION

Securing a system always means considering vulnerabilities, threats, countermeasures and acceptable risk. If the system is connected to the network, it automatically becomes vulnerable to threat. Simply shutting down a system when attack occurs, particularly in the case of network, is not a practical approach.

Computers are portable devices that connect from network to network. Most computer users usually use at least two or more networks to access data services on a consistent basis [Michael, 2005]. Organization must deal with the threats by tighten the security aspect of the system as well as the network. There are three concurrent trends that are placing network security as an increasingly strategic imperative for organization. They are:

i . Enterprise networks are becoming more open,

ii. Security threats are advancing in speed, sophistication, and potency, and

iii. The penalties for inadequate network protection are rising.

The scope of, and urgency for, security management is on the increase. It is important to know where is our organization currently stands on security practice because it can be our first step in proactive security management, and the best way to identified it is by conducting a full security audit. A security audit is the best and systematic way of testing for vulnerabilities or weaknesses in the IT system, policies and procedures in the organization. When completed, an audit will provide a comprehensive picture of the organization security status and stands.

Most common audit failure points are not grounded in poor technology. Most failure, in fact, can be attributed to poor compliance with practice and procedures. The purpose of this project is to conduct a network security audit in the Ministry of Domestic Trade and Consumer Affairs (MDTCA). The aim is to identify how well the network security in the organization and to point out the problem that might lead to the poor network security.

The contents of the thesis is for internal user only

10.0 REFERENCES

Adam P. (15 August 2006) . Developing a BCM framework from an Implementer's perspective, IT Asia Congress Presentation , Astro.

Computer security institute, (2002). Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row. Retrieved June 14, 2006 from http://www.gocsi.com/press/20020407.jhtml;jsessionid=WR5ISWRT1IU1GQSNDLOSKHSCJUNN2JVN?_requestid=23180

Baharin N., Md Din, K., Jamaludin, Z., and Md Tahir, M. Third party security audit procedure for network environment; Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on 14-15 Jan. 2003 Page(s):26 - 30

Budgen, P.J .Why risk analysis?.;Risk Analysis Methods and Tools, IEE Colloquium on 3 Jun 1992 Page(s):2/1 - 2/4.

Fallara, P Disaster recovery planning,.; Potentials, IEEE, Volume 22, Issue 5, Dec 2003-Jan 2004 Page(s):42 - 44 Digital Object Identifier 10.1109/MP.2004.1301248 IEEE JNL.

Gray, T. (2002). Network security credo. Retrieved June 14, 2006 from http://staff.washington.edu/gray/papers/credo

Hayes, B. (2003). Conducting a security audit: An introductory overview Retrieved June 12, 2006 from www.securityfocus.com/infocus/1697

Info~Tech research group. Security Auditing: An eight –Steps guide. Retrieved June 13, 2006 from http://www.knowledgestorm.com/shared/write/collateral/ANL/50845_92116_87646_Security_Audit_-_An_8_Step_Guide.pdf?ksi=1279585&ksc=1249778904

Kurniawan D. (14 August 2006). How Secure Are You, IT Asia Congress Presentation, fortinet.

Le Grand, C. H. (2005). Software Security Assurance: A framework for software vulnerability management and audit Retrieved June 10, 2006 from http://www.knowledgestorm.com/shared/write/collateral/WTP/51265_19677_51585_SoftwareSecurityAssuranceFramework.pdf?ksi=1279585&ksc=1249753632

Lo, E.C. and Marchand, M Security audit: a case study [information systems],.; Electrical and Computer Engineering, 2004. Canadian Conference on Volume 1, 2-5 May 2004 Page(s):193 - 196 Vol.1

Martin, K. (2005). Complexity kills innovation. Retrieved June 12, 2006 from http://www.securityfocus.com/columnists/300

Michael , M. J. (2005). Router Expert: Why you need a network services audit. Retrieved Jun 13, 2006 from http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1026349,00.html

Mitnick , K. D. , & Simon W. L. (2005). The art of intrusion: The real stories behind the exploits of hackers, intruders & deceivers. John Wiley & Sons

Ounce Labs Inc January 2005) , A framework for software vulnerability management and audit White paper, , Retrieved July 2006 from http://www.knowledgestorm.com/shared/write/collateral/WTP/51265_19677_51585_SoftwareSecurityAssuranceFramework.pdf?ksi=1279585&kse=1249753632

Prolexic Technologies, Inc. (2004). Distributed Denial of Service Attacks. White paper of Prolexic Technology, Inc., Q4:2004. Retrieved Jun 10, 2006, from http://newsite.prolexic.com/downloads/whitepapers/Prolexic_WhitePaper-DDoS-Q4-2004.pdf#search='distributed%20denial%20of%20services%20white%20paper.

Schneier, B. (2000). Secrets and Lies: Digital security in a networked world. John Wiley & Sons.

Tan J.(14 August 2006) Fraud & Cyber-Terrorism, Tapping on essential security measure to protect your enterprise, , IT Asia Congress Presentation, Extol.

Wikipedia. Primary Domain Controller. Retrived June 14, 2006 from http://en.wikipedia.org/wiki/primary domain controller

Wikipedia. Operating System, Retrived June 14, 2006 from http://en.wikipedia.org/wiki/operating system