UNIVERSITI TEKNOLOGI MARA

CASE STUDY ON WEB ICT SECURITY INCIDENTS IN GOVERNMENT SECTOR: GUIDELINE OF LOG FILE ANALYSIS

MOHD AZRAI BIN MANAP

Dissertation submitted in partial fulfillment of the requirements
for the degree of
Master (Sc) In Computer Networking

Faculty of Computer and Mathematical Sciences

JANUARY 2012

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful.

Alhamdulillah, thanks to the Almighty for blessing me with strength and courage to complete this thesis. In the midst of preparing and completing this thesis, I have the privilege of obtaining assistance and guidance from various sources. Therefore, I would like to express my deepest appreciation to those involved in this project.

First and foremost, I would like to express my appreciations and millions of thanks to my project supervisor, Puan Zolidah Bt. Kasiran who had sacrificed his precious time and effort in providing me with ideas and guidance in order to complete this dissertation. All of her contributions will be kept in my mind and in my heart, will be remembered and appreciated, as it is such a priceless effort for me.

I also would like to express my appreciation to the members of PRISMA and GCERT, especially for making this research to be augmented with their priceless guidance, ideas and critics to make the best of this research.

Last but not least, I would like to express my appreciation to my beloved parents as without their moral and financial support, I would not make it until today. For all my friends in CS778, I would like to thank for their help, friendship and countless support to me. May Allah S.W.T. bless all of them for their kindness and supported.

ABSTRACT

Website and online application is one of the most important elements in our life. The development of these elements change the way we live our life to make so much things easier such as every manual procedure that we have turned into computerized environment and the delivering of services to target group no matter where and when. There are so many benefits that we can gain from the developer perspective and the target group which is the end user. From a user perspective, it provides a means of acquiring computer services with simpler way than before. From an organizational perspective, it delivers services for consumer and business needs in simplified way, providing scalability and availability for providing their services. The Malaysian Government also aggressively promotes the use of website to offer their services to public. In recent years they are a lot of online services created such as My E-Government, My ID and many more. One of the important aspects of developing the website is security. However, most of the security aspect in developing website that offers such an online application is always been ignored. Some of government agencies thought that the security is not important because of lack of financial resource and knowledge also security it's not the main aspect in the development process. As evidence, there was an increase in number the number of web defacement incidents recorded each year. One of the factors to contribute in this increasing number of incident is there no proper action taken after security incident happen. Usually they just restore the latest backup available rather than to investigate the root cause of the incident. In this research, we will focus on two mechanisms that can be use for analyze the intruders activities and the vulnerability that lead to web defacement which are Intrusion Detection System and Log File Analysis. For ID technology, it has been used in government of Malaysia since 2004 but only covers 177 agencies out of 724 agencies today. Nowadays in the critical security environment, the use of this technology must be use widely to covers all the agencies. For the log file analysis, this is an alternatives to analyze the intruder's activities without investing any money on it. Later on, we will compare the outcome result of these two mechanisms to determine the effectiveness to identify the intruder's activity and type of attacks so the agencies will take necessary action based on the finding to secure from future attacks.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

This chapter describes an overview or brief introduction of the research conducted. The important aspects of the research such as problem statement, objectives, scope and significance of research will be included in this chapter.

1.0 Introduction

Nowadays web site and online application has been one of the most important elements in our life. Since internet has been introduce to the world, there are so many website and online application have been build offering so many type of services such as online application, sharing information and social networking. There are so many benefits that we can gain from the developer perspective and the target group which is the end user. From a user perspective, it provides a means of acquiring computer services with simpler way than before. From an organizational perspective, it delivers services for consumer and business needs in simplified way, providing scalability and availability for providing their services.