Chapter 77
Threats Classification:
State of the Art

Mouna Jouini
ISG Tunis, Tunisia

Latifa Ben Arfa Rabai
ISG Tunis, Tunisia

ABSTRACT

Information systems are frequently exposed to various types of threats which can cause different types of damages that might lead to significant financial losses. Information security damages can range from small losses to entire information system destruction. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system. Currently, organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary means to combat them which continues to pose a challenge. To improve our understanding of security threats, we propose a security threat classification model which allows us to study the threats class impact instead of a threat impact as a threat varies over time. This chapter deals with the threats classification problem and its motivation. It addresses different criteria of information system security risks classification and gives a review of most threats classification models. We present as well recent surveys on security breaches costs.

INTRODUCTION

With the development of Information and Communication Technologies and increasing accessibility to the Internet, organizations become vulnerable to various types of threats. In fact, their information becomes exposed to cyber attacks and their resulting damages. These threats are due to the interaction of the system's actors, their motivation and the system vulnerabilities. Indeed, security threats can be observed and classified in different ways by considering different criteria like source, agents, and motivations. They come from different sources, like employees' activities or hacker's attacks. Moreover, managers need to evaluate as well the extent of the damage they inflict to the organization and its systems. Based on the obtained assessment, it is necessary to have an understanding of the threats and the

DOI: 10.4018/978-1-5225-3923-0.ch077

vulnerabilities. Security threat classification allows detecting, understanding, and evaluating threats in order to propose appropriate security solutions. In fact, security threats can be observed and classified in different ways by considering different aspects of the system like its source code, or its users or their roles. Threats classification helps identify and organize security threats into classes to assess and evaluate their impacts, and develop strategies to prevent, or mitigate the impacts of threats on the system (Tang et al., 2012; Farahmand, 2005). There are several known computer system attacks classifications and taxonomies in these references (Geric & Hutinski, 2007 ; Chidambaram, 2004 ; Maheshwari & Pathak, 2012 ; Alhabeeb et al., 2010; Ruf et al., 2006).

This chapter gives an overview of most common classifications used in literature and in practice. We define a common set of criteria that can be used for information system security threats classification, which will enable the comparison and evaluation of different security threats from different security threats classifications. In fact, the chapter deals with threats modeling by the classification the threats into classes in order to define and understand their characteristics.

The first part deals with security threats braches and introduces the problem of threats classification.

The second and the third parts illustrate a review of threat classification models.

The fourth part discusses limits of exiting threats classification models.

1. SECURITY THREATS CLASSIFICATION

We show in this section a general overview of security threats classifications. In fact, we illustrates based on some statistics often security threats incidents cause damage to organizations. Then we present the merits and motivations of threats classifications model. Finally, we enumerate some principles that a threat classification should meet in order to evaluate the threats classifications models.

1.1 Costs Resulting from Information Security Incidents

The financial losses caused by security breaches (Farahmand, 2005; Shiu et al., 2011; Ben Arfa Rabai e al., 2012; Jouini e al., 2012; Ben Arfa Rabai e al., 2013) usually cannot precisely be detected, because a significant number of losses come from smaller-scale security incidents, caused an underestimation of information system security risk Geric & Hutinski, 2007). Thus, managers need to know threats that influence their assets and identify their impact to determine what they need to do to prevent attacks by selecting appropriate countermeasures.

The financial threat loss to organizations could be significant. A physical breach of security involves actual damage to, or loss of the computer hardware or media on which data are stored. A logical breach affects the data and software without physically affecting the hardware. Recent literature (Jianping et al., 2012; Tsiakis, 2010; Min et al., 2011) has also documented significant costs related to information systems security breaches.

1.1.1 Computer Security Institute Survey

The Computer Security Institute (CSI) (Robert, 2010) has for ten years, in conjunction with the Federal Bureau of Investigations (FBI) Computer Intrusion Squad in San Francisco, conducted and released the results of the annual Computer Crime and Security Survey, which aims to raise the level of security