Chapter 70
Insider Attack Analysis in Building Effective Cyber Security for an Organization

Sunita Vikrant Dhavale
Defence Institute of Advanced Technology, India

ABSTRACT

Recent studies have shown that, despite being equipped with highly secure technical controls, a broad range of cyber security attacks were carried out successfully on many organizations to reveal confidential information. This shows that the technical advancements of cyber defence controls do not always guarantee organizational security. According to a recent survey carried out by IBM, 55% of these cyber-attacks involved insider threat. Controlling an insider who already has access to the company's highly protected data is a very challenging task. Insider attacks have great potential to severely damage the organization's finances as well as their social credibility. Hence, there is a need for reliable security frameworks that ensure confidentiality, integrity, authenticity, and availability of organizational information assets by including the comprehensive study of employee behaviour. This chapter provides a detailed study of insider behaviours that may hinder organization security. The chapter also analyzes the existing physical, technical, and administrative controls, their objectives, their limitations, insider behaviour analysis, and future challenges in handling insider threats.

INTRODUCTION

Technology is a fundamentally essential part for securing organizational information assets; however organization's employees are equally responsible for design, implementation and operation of these technological tools. A recent attack against Morgan Stanley, one of the world's largest financial services firms that exposed hundreds of thousands of customer accounts was carried out by one of the trusted employee of the same organization (Seth, 2015). The Computer Emergency Response Team (CERT) survey found that,insider attack cases made up 28% of all cybercrimes and more than 33% of organizations reported insider attacks in 2013 (Sangiri, & Dasgupta, 2016). ISACA conducted a research on cyber

DOI: 10.4018/978-1-5225-8897-9.ch070

security in 2016, which was based on the research among 2,920 security professionals in 121 countries (CIO&LEADER, 2017). The respondents in this survey listed the insider threats as one of the top threats, along with social engineering attacks. Recently, Edward Snowden's case highlighted the risky side of the insider threats in highly secure government institutions (BBC News, 2013).

Human elements representing as insiderssignificantly affect the efficiency of implemented cyber security program in any organization. Recent critical security incidents have shown that, the successful insider intrusions induce a fear of significant financial and credibility loss in an organization; and can be more damaging than the outsider threats. These insider attacks can be characterized in following ways: 1) they are carried out by our trusted employees; 2) they are carried out inside the boundaries of the organization; 3) they are hard to detect and may go undetected for years; 4) they don't happen often; and 5) they can damage the reputation of an organization severely. However, there is still a lack of awareness in many organizations regarding severity of the insider threats, while implementing organizational security controls. There is a need to urge cyber security professionals, policymakers, law enforcement, government and private organizations to share their knowledge and experience related to the recent insider based security incidents. A detailed study of the insider behaviour patterns need to be carried out in order to provide a reliable comprehensive solution for handling insider attacks.

This book chapter is organized as, 1) Section 1 gives general introduction of the subject; 2) Section 2 discusses characteristics of trusted malicious insiders; 3) Section 3 explains existing security controls and their limitations in detail; 4) Section 4 provides possible solutions for mitigating insider attacks; 5) Section 5 provides complex human behaviour analysis followed by the conclusion in Section 6.

TRUSTED MALICIOUS INSIDERS

The human element can compromise almost anything including the most intelligently designed security system (Infosec Institute, 2012). In addition, current research shows that the most common types of attack are carried out by disgruntled or angry insiders. The malicious insiders can be trusted employees (former/current), contractors, business partners, consultants, auditors, or vendors who intentionally misuse their authorized access to organizational assets. Here, trusted means the insiders to whom organization normally provide credentials (e.g. user name and password) to access organizational information resources. Hence, we can say, an insider is a person: 1) who is trusted by the organization and given a permission to work within the security perimeter of an organization; 2) who has authorized full/partial access to the organizational information systems; 3) who has partial/full knowledge about the design and working of organization's information systems; and 4) who has a potential to launch malicious attacks against organizational resources.

In an organization, an insider may have; 1) one or more roles along with; 2) certain responsibilities;3) technical expertise and 4) a hold on certain critical resources; which gives him 5) a number of opportunities; to harm informational assets in 6) intentional or unintentional way. Out of these factors, roles and responsibilities are granted by the organization itself in an overt manner; while technical capabilities or opportunities can be generated by an insider in an overt or covert manner. All these six factors are interrelated (Matt, et al. 2010). Fewer roles or less responsibilities lead to less workload and in turn may result in boredom, de-motivation or dissatisfaction. Higher responsibilities or more roles may lead to high workload; but in turn may result in stress and frustration. In case of dissatisfaction due to reasons including; less number of roles/less number of responsibilities/unfair rewards when compared with