Chapter XII
A Repeatable Collaboration Process for Incident Response Planning

Alanah Davis
University of Nebraska at Omaha, USA

Gert-Jan de Vreede
University of Nebraska at Omaha, USA

Leah R. Pietron
University of Nebraska at Omaha, USA

ABSTRACT

This chapter presents a repeatable collaboration process as an approach for developing a comprehensive Incident Response Plan for an organization or team. Despite the process of incident response planning being an essential ingredient in security planning procedures in organizations, extensive literature reviews have not yielded any collaborative processes for such a crucial activity. As such, this chapter will discuss the background of incident response planning as well as Collaboration Engineering, which is an approach to design repeatable collaborative work practices. We then present a collaboration process for incident response planning that was designed using Collaboration Engineering principles, followed by a discussion of the application process in three cases. The presented process is applicable across organizations in various sectors and domains, and consist of codified “best facilitation practices” that can be easily transferred to and adopted by security managers. The chapter describes the process in detail and highlights research results obtained during initial applications of the process.
INTRODUCTION

Today, many organizations have connected their systems and networks to the outside world, as is the case of e-business. This brings with it special requirements on computer and information security. Most organizations have to handle security risks such as viruses and worms, theft of proprietary information, financial fraud, system penetration by outsiders, sabotage of data or networks, to mention but a few. Therefore, organizations need to have Incident Response Plans in place to be able to respond efficiently when an incident occurs (Soper, 2003). However, experience shows that creating a high quality Incident Response Plan is a complex task. Creating a comprehensive and useful plan requires the input from many security professionals (Foix, 2004; Sausner, 2007). It is often a time-intensive process as groups of professionals have to share relevant information, deliberate on preventive and reactive measures, and achieve agreement on strategies and policies. To ensure that this collaboration is as efficient and effective as possible, many groups would benefit from a structure, purposeful team process that is guided by an expert facilitator. Yet surprisingly, an extensive literature review did not reveal any reported standard collaborative processes for this critical security activity. Therefore, the goal of this chapter is to present a collaborative team process for the creation of an Incident Response Plan. This process was designed using Collaboration Engineering principles and tested in three case situations. The collaborative Incident Response Plan process consists of codified ‘best facilitation practices’ that can be easily transferred to and adopted by security managers. Hence, security managers can execute the process by themselves without the support from expensive, expert facilitators. This use of Collaboration Engineering does not suggest that facilitation is easy; however it illustrates how a step-by-step plan using best facilitation practices can be completed by security managers who are novice facilitators.

The chapter begins with a background of incident response planning and Collaboration Engineering. This background provides the basis and information necessary for the design of a collaboration process for incident response planning. Next, the chapter describes the designed process in detail and highlights the research results obtained during initial applications of the process. The chapter then presents a discussion of future trends and research issues which when explored may offer potential for further strengthening these results. The chapter concludes with a discussion of how the presented process can be used across organizations in various sectors and domains.

BACKGROUND

There is a significant amount of research in the area of IT contingency planning and, as a part of that, incident response planning. However, based on our research of existing literature we conclude that no collaborative process has been presented for security practitioners. The background in this chapter will first discuss relevant research related to incident response planning. Then we discuss the Collaboration Engineering approach that was used to design the repeatable incident response planning process.

Incident Response Planning

IT contingency planning supports the development of thorough plans and procedures to recover from an IT service disruption and/or a disaster in an organization. IT comprehensive contingency planning consists of several major planning documents including: (a) Business Impact Analysis (BIA); (b) Incident Response Plan (IRP); (c) Business Contingency Plan (BCP); and (d) Disaster Recovery Plan (DRP) (Swanson et al., 2002). Of specific interest to this chapter is the IRP. An IRP covers the planning process associated with the definition, identification, classification,
Related Content

Malware Detection by Static Checking and Dynamic Analysis of Executables
[www.igi-global.com/article/malware-detection-by-static-checking-and-dynamic-analysis-of-executables/181546?camid=4v1a](www.igi-global.com/article/malware-detection-by-static-checking-and-dynamic-analysis-of-executables/181546?camid=4v1a)

Efficient Authentication Scheme with Reduced Response Time and Communication Overhead in WMN

Comparing the Security Architectures of Sun ONE and Microsoft .NET
[www.igi-global.com/chapter/comparing-security-architectures-sun-one/23197?camid=4v1a](www.igi-global.com/chapter/comparing-security-architectures-sun-one/23197?camid=4v1a)

Security Awareness: Virtual Environments and E-Learning
[www.igi-global.com/chapter/security-awareness-virtual-environments-learning/20673?camid=4v1a](www.igi-global.com/chapter/security-awareness-virtual-environments-learning/20673?camid=4v1a)