Chapter 6

RESPONDING TO ATTACKS

INTRODUCTION

A series of questions will emerge from the need to support some combination of the Internet-based enterprise requirements discussed next; and, the major focus of this chapter:

- Identification and Authentication
- Software Import Control
- Encryption
- System/Architecture Level
- Incident Handling
- Administrative
- Awareness and Education [1]

What controls and procedures should be implemented to support your enterprise needs? What type of risk profile do you fall under? What is your style and culture of doing business? Who is responsible? The elements that drive the answers to such questions form the policy framework for the enterprise to respond to attacks [1].

SAMPLE POLICY AREAS

This first part of the chapter contains hypothetical sample policy statements that address Internet-based security. The policy elements are derived from the major sources of security controls (software import control, encryption [3], and system architecture). The rationale that drives the selection of certain policy is given, followed by the actual sample policy statement(s) [1].

Multiple sample policies are contained here for use at the different risk profiles as was previously discussed in Chapter 5. Some areas provide multiple examples at the same risk level to show the different presentation methods that might be used to get the message across [1].

Security policies fall into two broad categories: technical policies to be carried out by hardware or software, and administrative policy to be carried out by people using and managing the system. The following indicate each type of policy [1].

Identification And Authentication

Identification and Authentication (I&A) is the process of recognizing and verifying valid users or processes. I&A information is generally then used to determine what system resources a user or process will be allowed to access. The determination of who can access what should be part of a data categorization effort, described later in the chapter [1].

This chapter assumes that a decision has been made to allow connectivity to internal systems from the Internet. If there is no connectivity, there is no need for I&A. Many enterprises separate Internet-accessible systems from internal systems through the use of firewalls [2] and routers [1].

Authentication over the Internet presents several problems. It is relatively easy to capture identification and authentication data (or any data) and replay it in order to impersonate a user. As with other remote I&A, and often with internal I&A, there can be a high level of user dissatisfaction and uncertainty which can make I&A data obtainable via social engineering. Having additional I&A for use of the Internet may also contribute to I&A data proliferation which is difficult for users to manage. Another problem is the ability to hijack a user session after the I&A has been performed [1].

There are three major types of authentication available: static, robust, and continuous. Static authentication includes passwords and other techniques that can be compromised through replay attacks. They are often called reusable passwords. Robust authentication involves the use of cryptography or other techniques to create one-time passwords that are used to create sessions. These can be compromised by session hijacking. Continuous authentication prevents session hijacking [1].

Static Authentication

Static authentication only provides protection against attacks in which an imposter cannot see, insert or alter the information passed between the claimant and the verifier during an authentication exchange and subsequent session. In these cases, an imposter can only attempt to assume a claimant's identity by initiating an access control session as any valid user might do; and, trying to guess a legitimate user's authentication data. Traditional password schemes provide this level of protection, and the strength of the authentication process is highly dependent on the difficulty of guessing password values and how well they are protected [1].

Robust Authentication

Robust authentication mechanisms relies on dynamic authentication data that changes with each authenticated session between a claimant and verifier. An imposter who can see information passed between the claimant and verifier may attempt to record this information, initiate a separate access control session with the verifier, and replay the