INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

EXPLORING VARIOUS ASPECTS OF ADMINISTERING NETWORK SECURITY

SNEHA. R. KAWARE[1] , PROF. K. G. BAGDE[2]

1. PG Students H.V.P.M's college of Engg. & Tech., Amravati, India.
2. Faculty in H.V.P.M's college of Engg. & Tech., Amravati, India.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Network security,
Security Planning,
Security Policies,
Risk Analysis,
Physical security

Corresponding Author

Ms. Sneha. R. Kaware

Abstract

As the world becomes more connected by networks, the significance of network security will certainly continue to grow. Network security is achieved through technology and depends on all cryptographic tools, trust, inference and aggregation controls. Important activities in security are picking the right IDS, configuring firewall properly and encrypting wireless link. But not all of security is addressed by technology. Many security losses come from trusted insiders. Security is a combination of technical, administrative, and physical controls. In this paper we examined how security is administered through security policies, user awareness and risk analysis, as a way to address the insider threat. Security policies should be viewed as key enablers for the organization. Security policies like information security policy, data sensitivity policy, internet security policy describe the nature of different audience and their security goals. The risk analysis identified the assets that are to be protected. The assets can be computers, networks, general data, and management data. Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks. Increasing the security awareness of the users is the best way to anneal the weakest link in the security.

1. INTRODUCTION

Network security is becoming more important as people spend more time connected. The introduction of personal computers and the general ubiquity of computing have changed the way many of us work and interact with computers. In particular, a significant amount of the responsibility for security has shifted to the user. But many users are unaware of this responsibility, so they do not deal with the risks posed or do not implement simple measures to prevent or mitigate problems. Many security losses come from trusted insiders- either honest people making honest, human mistakes or dishonest insiders able to capitalize on their knowledge or privileges [1]. To avoid this, every organization using computers to create and store valuable assets should perform thorough and effective security planning [2]. The administration of security draws on skills slightly different from the technical skills. Security Planning, Risk analysis, Organizational policy and physical control are just as important to achieving security as are the latest firewall or coding practice. Properly conceived and implemented security policies, programs and technologies are essential to ensure a facility's resistance to myriad threats while meeting demanding uptime, reliability and performance objectives[3].

2. NETWORK SECURITY

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources[2]. In large networks, a huge number of potential attackers can probe the software extensively [6]. There are three technical controls specific to networks, firewalls, IDS and secure e-mail.

2.1 Firewalls: A firewall is a special form of reference monitor. By carefully positioning a firewall within a network, we can ensure that all network accesses that we want to control must pass through it.[2]

2.2 Intrusion detection systems: An intrusion detection system is a device, typically another separate computer that monitors activity to identify malicious or suspicious events [1]. An Intrusion Detection System is a sensor, like a smoke detector, that raises an alarm if specific things occur.

2.3 Secure e-mail: E-mail is vital for today's commerce, as well a convenient medium for communications among ordinary users [1]. But, e-mail is very public, exposed at every point. Sometimes we would like e-mail to be more secure. Message confidentiality, integrity, sender authenticity, no repudiation are needed for every message to secure e-mail [1].

3. ADMINISTERING SECURITY

Technical controls may contain some flaws such as how effective is a public key infrastructure if someone can walk off with the certificate server. Therefore, there needs to be some kind of security to the organization's private resources from the Internet as well as from inside users as survey says that eighty percent of the attacks happen from inside users for the very fact that they know the systems much more than an outsider knows and access to information is easier for an insider [5]. Typically, physical security and administrative security are strong enough to protect transmission inside the perimeter of a network [1].There are four areas related to security controls by considering administrative and physical aspects are: planning, risk analysis, policy and physical controls.

3.1 Security Planning

A security plan is a document that describes how an organization will address its security needs. A good security plan is an official record of current security practices, plus a blueprint for orderly change to improve those practices. By following the plan, developers and users can measure the effect of proposed changes, leading eventually to further improvements. Thus, the security plan has to have the appropriate content and produce the desired effects [1].

Contents of Security Plan:

- Policy, indicating the goals of a computer security effort.
- Requirements, recommending ways to meet the security goals.

- Recommended controls, mapping controls to the vulnerabilities identified in the policy and requirements.

- Accountability, describing who is responsible for each security activity.

- Timetable, identifying when different security functions are to be done.

- Continuing attention, specifying a structure for periodically updating the security plan.

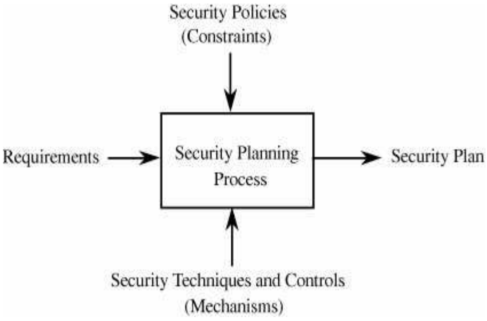

Fig: 3.1 Inputs to the security plan

3.2 Risk Analysis

Security risk analysis is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause [5]. There are two types of risk analysis; quantitative and qualitative [7]. We can quantify the effects of a risk by multiplying the risk impact by the risk probability, yielding the risk exposure. Risk leverage is [1]

$$\frac{(\text{risk exposure before reduction}) - (\text{risk exposure after reduction})}{(\text{cost of risk reduction})}$$

If the leverage value of a proposed action is not high enough, then we look for alternative but less costly actions or more effective reduction techniques [1].

Steps of a Risk Analysis:

1. Identify assets.

2. Determine vulnerabilities.

3. Estimate likelihood of exploitation.

4. Compute expected annual loss.

5. Survey applicable controls and their costs.

6. Project annual savings of control.

By following these well-defined steps, we can analyze the security risks in a computing system.

3.3 Organizational Security Policy

A good security policy is a set of documents, each addressing a specific need. By breaking your overall policy into smaller pieces, each managed separately; you greatly simplify the process of creating effective, consistent, relevant, and useable documents [3]. A security policy is a high-level management document to inform all users of the goals of and constraints on using a system.

Characteristics of a good security policy:

- Coverage: A security policy must be comprehensive.
- Durability: A security policy must grow and adapt well.
- Realism: The policy must be realistic.
- Usefulness: An obscure or incomplete security policy will not be implemented properly.

3.4 Physical Security

Physical security is the term used to describe protection needed outside the computer system. The objectives of physical security are to ensure the confidentiality, integrity, and availability of assets [4]. The physical security manager has to consider all assets and a wide range of harm. Typical physical security controls include guards, locks, and fences to deter direct attacks [8]. Keeping back up or offsite backup copy is used to protect data. But it is useless if it is destroyed in the crisis too. Networked storage, cold site and hot sites are also be used and better choice for protection critical data.

3.5 User Awareness

Preventing accidental or deliberate compromise, damage, theft or misuse of customer information and company results are critical success factors for the organization. As many losses can cause by trusted insiders like users or employees in the organization [7].Security awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical and, especially, information assets of that organization. Many organizations require formal security awareness training for all workers when they join the organization and periodically thereafter, usually annually.

4. COCLUSION

This paper discussed the various aspects of administering the network security by considering the technical as well as administrative and physical controls. We have seen that technical controls can prevent the system from outside attackers, it may contain some flaws. They cannot protect from trusted insiders. The administration of security has a strong human component, from the writing of plans and policies, to the mental work in performing a risk analysis, to the human guards that implement or reinforce many physical controls. We would administer the security policies and examine the risks so that the better control will be provided over the losses. Better awareness on security among users would improve the level of security.

5. REFERENCES

1. Pfleeger, Charles and Pfleeger, Shari, "Security in Computing." 4th edition

2. William stalling "Computer Network & security:" Pearson Education.

3. Frederick M. Avolio and Steve Fallin "producing your network security policy" July 2007

4. Justin Kallhof "physical security threats"

5. http://www.security-riskanalysis.com/index.htm

6. SANS institude infosec reading room, "intrusion detection system"(2011)

7. Security planning and risk analysis" CS461/ES442 Spring 2010 in computer security.

8. "Physical Security Threats and Controls",mar.17, 2008 in Physical Security.