Creating and Communicating a Security Strategy

Your Name

Institution

Creating and Communicating a Security Strategy

Being an IT professional, author has to find out vulnerabilities in the company's network security. Once the vulnerabilities are found, they will be related to security policies and standards. In the end, recommendations and action needed to address the security issue will be discussed. Purpose of this memo is to find security risks, to provide a network security framework for hardware and software solutions developed within the company. The company provides online financial services to various banks within the State. Company is currently providing portals and server for the banks. Servers have sensitive data of loyal bank customers. As the company is dealing with confidential financial information, there are several security threats that it can face. Company’s network infrastructure is most vulnerable to cyber-attacks. Company’s network is based on Wireless Area Network (WAN), interconnecting many Local Area Networks (LANs).

Two major security risks which are associated with the company's network are shutting down of a system and loss of sensitive data. These losses can be caused by computer viruses, rogue security software, Trojan horse, adware or spyware, network worm, DDoS attack, Rootkit, and SQL Injection attack. Company’s servers store the sensitive data which makes them the primary target of cyber-attack. Suggested security measures in this memo must ensure the safety of servers from the internal and external breach. To address such cyber-attacks, a company needs a good security policy to ensure the safety of its network.

# Security policy

 Any secure network can be breached either form external or internal attack. To secure a system, different layers of security should be applied. The primary objective of layered security secures the primary asset, even if the attacker manages to breach the system. The policy will be designed by following the recognized standards which most of the private companies and government offices follow. There will be two main part of the suggested policy; security measures, strategies. Security measures are the steps which will help in securing the safety of the system. Strategies are the steps which will help when the security is compromised. These steps are designed by following the guidelines of the National Institute of Standards and Technologies (NIST) and National Security Agency (NSA). NIST provides supporting guidelines for NSA standards.

## Security Measures

To address all security threats and concerns, we have to search for weak spots within the network. The skilled workforce is essential for the security of the network, they should have technical skills and expertise over network security tools. There are network security courses and certification offered by CISCO. If a worker doesn't have such certifications, an enterprise should sponsor such courses for their IT technical staff.

A company should take the following key actions to prevent any internal or external cyber-attacks.

1. Understand common attacks. Good knowledge of cyber-attacks which targets weak network can be very helpful.
2. Establish a list of potential vulnerabilities, and look for anything suspicious or unknown to your network
3. Use vulnerability and network scanning tool
4. In case of an attack, the company should be able to access the risk and should be able to take reliable actions in such events.

## Strategies

Suggested defense strategy for the company's network is multi-layers of protector from external intruders. If one layer is compromised, there are more barriers that a hacker has to overcome before gaining excess to the company's servers or other components. This layer system not only slows down the hacker, but they can also be detected before achieving their goals. This section will briefly explain in this layered strategy

1. Every Component of the system should be VPN cable.
2. secure cables with a firewall
3. As shown in figure 1, install a firewall in every layer of the network. Separate firewall for each server, and each layer.
4. Install network security tool which will monitor the traffic within the server
5. Create strong passwords for every network devices
6. Only allow data to travel within the network in encrypted form
7. Install firewall management software
8. Strong authentication parameters, either NetScreen or F5 employ user-based authentication
9. For added security, access control and authentication should be as close to network as possible
10. Use XMP mapper in every IDSN adapter
11. Install NIC at the maximum number of junctions possible
12. Use network gateways even at endpoint access

These parameters/ measures are listed after careful understanding of NIST security testing guidelines publication 800-115All the parameters mentioned above a crucial for enterprise network security

Two techniques are used for security examination and testing. First one is white box testing, which associate examination of the application's source code. It is an efficient technique to detect security defects. Performing a white box technique is quite easy as the source codes of the applications are usually available. White box testing cannot detect thread during the compilation of the program. In addition, security threads linked between components are also hard to detect using white box testing.

The second Testing technique suggested by NIST is black-box testing, which involves analysis of an application's binary executable. This technique used to examine the security of individual components which have a high risk of getting infected/ attacked. This type of test also challenges the threats handling capabilities of the system, which results in finding out the limitation of the network system and its security status. Both white box and black box techniques can be used simultaneously in a combination called grey-box testing.

A person performing this kind of security assessment should have certain skills. He should have a good understanding of programming languages and network security protocols. Familiarity with application development, secure coding, and being able to use other security tool are great perks of a skilled employee which benefits the company.