Enterprise Security Management

Penetrate*

©HackersCenter

http://www.hackerscenter.com

18/12/05

* Penetrate@hackerscenter.com

1. Introduction

An enterprise consists of lot many resources. The management of such resources is a huge task. It requires considerable amount of funds and skilled manpower. Securing such huge resources is a challenging job.

In this paper I have tried to bring out difficulties faced in this regard, solutions available and best practices to follow when it comes to securing the resources.

An enterprise doing some business, works based on a well-defined infrastructure. The infrastructure is built after making some complex decisions around cost allocation, technology investment, process and strategy. Further the complexity is increased by disconnection between the management and the IT team who must align with each other to create a successful program.

In an effort to improve security in a largely reactive environment, some organizations are forced to invest in disparate security measures to counter specific threats. While this approach may provide isolated pockets of protection organizations are seeking a coherent security strategy that serves the business as a whole.

2. Providing Point Solution

By Point Solution I mean reacting to the security threat when the loophole has been exploited. For example running anti virus software after the virus is hit. Here the solution does not take care of long term consequences rather it just fixes the problem at hand.

Advantage of this approach is that it solves the problem quickly. When relying on point solutions, organizations certainly have protection against some vulnerability. Yet without coordinated policies, processes and assurance mechanisms, they have no way of knowing for sure that their most critical information and assets are being protected.

There is a need to formalize steps taken for security measures and document it so that in rapidly changing business environments tracking security loopholes becomes an easy job.

The organization must have a security strategy that can be implemented, measured, and revised as the business climate and operational environment change. In the long run, the effectiveness of the security strategy depends on how well it is aligned with and supports the organization's business drivers.

3. Formalizing

After deciding to formalize, one must ask the question, " When to start?"
The answer is very simple, it should start when the structuring of the business model itself starts. Depending on the nature of the business, the risk factors are identified. One of the important risk factor considered must be the security measures to be taken to secure the various resources that may be used.

These security measures are formally called as Security Policies. The Security Policies must cover possibly all the risks and counter measures to be taken to avoid those risks. Also Security policies must be scalable, so that they are very effective against varied security threats like Exploits.

The Security Policies can be divided in to two categories

1. **External:** which deals with the threat coming from outside the corporate network. It can be referred as Securing Perimeter. The main focus here is to segregate the resources in to different zones called as Demilitarized Zone (DMZ) environments with the help of Firewalls. For example in Figure 1 a

network is set up having Internal and External DMZ environments. Setting up VPN is one more way to secure the perimeter. In this method a secure tunnel is created between the corporate server machine and the client system, which is outside the corporate network and using public network (Internet). This secure tunnel or

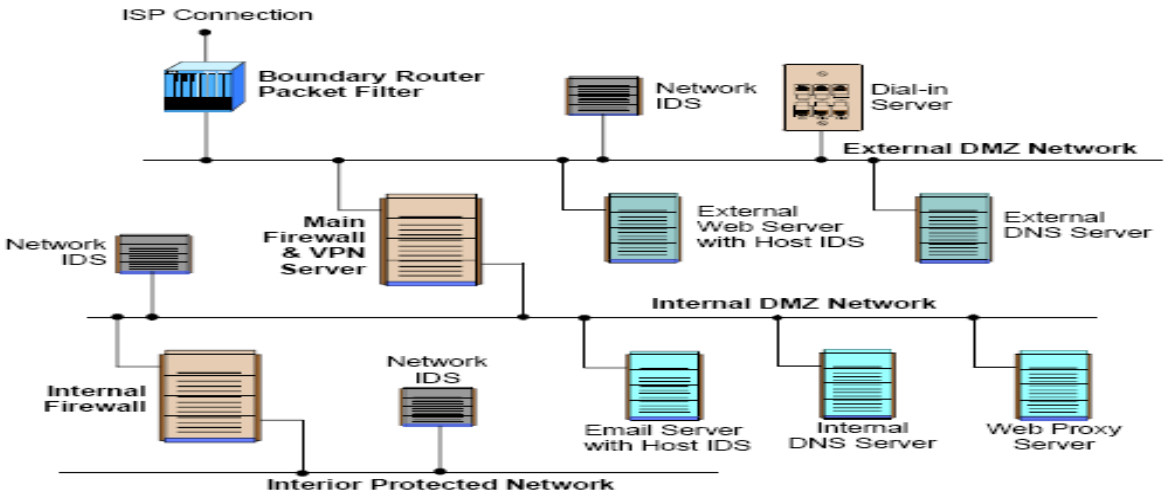

Figure 1

channel is created by using protocols like PPTP, L2TP and authentication methods like MS-CHAP and EAP-TLS and authentication servers like RADIUS and IAS.

The VPN security policies provide more secured implementation of VPN.

The Intrusion Detection Systems play a major role in detecting a security breach. Implementing and configuring an effective Intrusion Detection system is necessary for a corporate network security. Intrusion detection systems are capable of performing real-time traffic analysis and packet logging on IP networks. Also they can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI (Common Gateway Interface) attacks, SMB (System Message Block) probes, and OS fingerprinting attempts.

2. **Internal:** which deals with security breaches within the corporate network. The focus here is on Application security. An application makes use of system resources (eg. Processor, memory, I/O system etc) as well as Data Base. An application can be exploited and can be made to execute some malicious code. To secure the application against such exploits, the application code must be written in such a way that it leaves no loopholes in the code, which can be exploited. The design of the application code must take care of some measures to ensure application security.

   Most of the applications running under windows make use of Registry. This is exploited by some viruses and Trojans to crash the application or make it work in favor of them. So it's important to write the application code, which does not rely much on registry.

   One more major cause for application crash is Buffer Overflow. This has to be taken care while writing the code.

   The next thing to consider in internal security polices are :

   - Defining Password policies (eg. Min password length, complex password creation, Minimum password age)
   - Using secure protocols for authentication (Kerberos, MD5)

- Securing Files and Folders by giving permissions to individual files and folders
- Auditing the object access (Monitoring who accesses what resource at what time)
- Regular review of Logs on the server
- Securing the Web servers
- Securing email servers
- Regular backup of critical data
- Anti-virus policies (Regular scanning and updating anti-virus software)
- Applying operating system patches and updates regularly.

The approach to consolidate the overall security, Security Policies must be combined with procedures and appropriate technology. Combined all forms what is called as *Enterprise Security Architecture*. There must be some kind provision for scaling and revising the architecture, which can be put together as *Security Lifecycle*.

The Security Life Cycle can be roughly put together as follows. This can be taken as a reference to build more elaborated and organization specific Life Cycle.

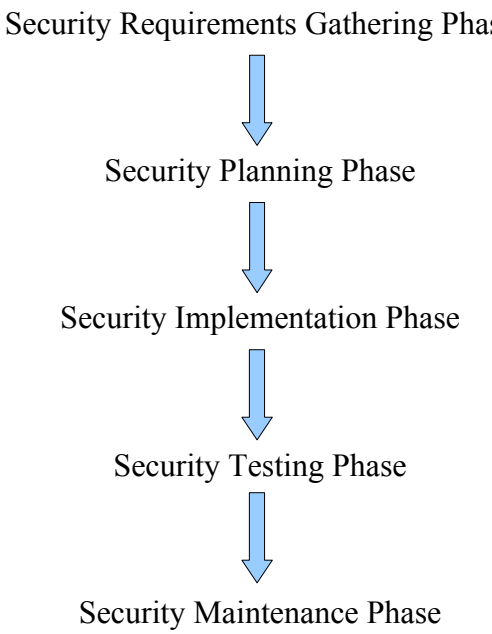

Figure 2

Figure 2 represents a typical security life cycle. As you can see, from the name itself the functionality of each phase is evident.

The Requirement gathering phase starts when the business model itself is getting created. Depending on the type of the business the security requirements are documented.

Looking at the security requirements document, a full-fledged plan is created where in the Security Policies, procedures and the technology required to implement the policies are analyzed and documented.

Next come the most important and somewhat time-consuming phase, Implementation Phase. Here the technology is put in place in accordance to the policies. The steps taken to implement, technology used (hardware and software) and plan to test the implementation are documented.

In Security Testing Phase (second important and time-consuming phase) the whole Security Architecture is put in to test. A formal testing method known as Penetration Testing is used to carry out thorough testing of security implementations.

After the testing begins the Maintenance. We cannot sit relaxed just implementing and testing the security implementations. The whole architecture must be kept under observation all the time as the hackers are finding new ways to penetrate in to the secured Systems. Therefore it become very important to assess the security implementations time to time so that if there is any loophole unpatched, it can be detected and fixed before a hacker finds it and exploits it.

As I said, this life cycle can be taken as a reference to build much more complex and elaborated life cycle which suites a particular type of organization. This paper remains unfinished if I don't mention about Penetration Testing. Penetration Testing is a formal method of attacking the organization network to test its security implementations. This attack is done with prior knowledge of the security implementation and even IT department of the organization knowing about it. This test is also

conducted without any prior knowledge of security implementations and without the IT department knowing about this attack. Both the forms of attacks need to be done because these two forms of attacks are closely related with the kind of attacks a hacker may launch against the organization.

There are many organizations now has come up providing penetration testing services. These service providers have their own way of penetrating and their own way of documenting it. Typically these service providers have skilled people who are experienced and have some security related certificates (CEH, CISSP, CCIE, CCSP) and they follow some well defined standards set by security organizations like NIST, ISACA, CHECK, OSSTMM, OWASP etc. These penetration testers use tools, which are typically used by hackers. Some of the tools used are as follows.

- File Integrity Checkers
  Aide, LanGuard, TripWire
- Network Sniffers
  Dsniff, Ethereal, Sniffit, Snort, TcpDump, WinDump
- Password Crackers
  Crack 5, IMP 2.0, L0pht Crack, NwpCrack
- Scanning and Enumeration Tools
  DUMPsec, FireWalk, Fscan, LanGuard Network Scanner, NDS Snoop, Nmap, SloarWinds, SuperScan
- Vulnerability Assessment Tools
  CyberCop Scanner, ISS Internet Scanner, Nessus, SecureScanNX, SAINT, SARA, SATAN
- Wireless Networking Tools
  Aerosol, AirSnort, Kismet, NetStumbler, Sniffer Wireless, WEPCrack, WaveStumbler

After doing all kinds of tests, the penetration testers prepare a document containing the details of type of test conducted, the outcome, loophole found and recommendation to patch that loophole. This document is presented to the management of the organization and its left to them to decide upon the course of action.
Before letting a penetration tester in, some kind of background analysis of the company providing penetration testing services must be done to make sure that the testing is done by trust worthy and skilled people.

4. Conclusions

The Enterprise Security Management is a huge and challenging task. Prior experience and well-planned approach to secure the resources is mandatory. Following some well-defined security life cycle which suites a particular organization type reduces the risk. Most important is assessing the security architecture on a regular basis, constantly updating and evaluating knowledge and skill sets of IT department (system administrators and network administrators).