Implementation of System and Network Security for an Enterprise

Dr. Sandeep Kumar*

MCA from Kurukshetra University Kurukshetra, PhD from Singhania University

Abstract - Networks today run mission-critical business services that need protection from both external and internal threats. In this paper we proposed a secure design and implementation of a network and system using Windows environment. The basic reasons we care about information systems security are that some of our information needs to be protected against unauthorized disclosure for legal and competitive reasons; all of the information we store and refer to must be protected against accidental or deliberate modification and must be available in a timely fashion. We must also establish and maintain the authenticity (correct attribution) of documents we create, send and receive. Finally, the if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings: if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems. Another issue that is emerging in e-commerce is that good security can finally be seen as part of the market development strategy. Consumers have expressed widespread concerns over privacy and the safety of their data; companies with strong security can leverage their investment to increase the pool of willing buyers and to increase their market share. We no longer have to look at security purely as loss avoidance: in today's marketplace good security becomes a competitive advantage that can contribute directly to revenue figures and the bottom line. Reviews of latest product with an application to an enterprise with worldwide branches are given.

Keywords: Network Design, LAN, WAN, Security, Encryption, VPN, IPSec, Active Directory.

1. INTRODUCTION

Information security means protecting information and information systems from unauthorized access, disclosure. disruption, modification, destruction. terms information The computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms [8]. Governments, military, financial institutions, hospitals, and businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about businesses customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. For the individual, information security has a significant effect on Privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. As a career choice there are many ways of entering the field. It offers many areas for specialization including Information Systems Auditing, Business Continuity Planning and Digital Forensics Science, to name a few.

2. SECURITY SERVICES AND PROCESSES

Security is fundamentally about protecting assets. Assets may be tangible items, such as a Web page or our customer database — or they may be less tangible, such as our company's reputation. Security is a path, not a destination. As we analyse our infrastructure and applications, we identify potential threats and understand that each threat presents a degree of risk. Security is about

risk management and implementing effective countermeasures.

Authentication

Authentication addresses the question: who are you? It is the process of uniquely identifying the clients of our applications and services. These might be end users, other services, processes, or computers. In security parlance, authenticated clients are referred to as *principals*.

Authorization

Authorization addresses the question: what can you do? It is the process that governs the resources and operations that the authenticated client is permitted to access. Resources include files, databases, tables, rows, and so on, together with system-level resources such as registry keys and configuration data. Operations include performing transactions such as purchasing a product, transferring money from one account to another, or increasing a customer's credit rating.

Auditing

Effective auditing and logging is the key to nonrepudiation. Non-repudiation guarantees that a user cannot deny performing an operation or initiating a transaction. For example, in an e-Banking system, non-repudiation mechanisms are required to make sure that a client cannot deny ordering to pay a bill from his account.

Confidentiality

Confidentiality, also referred to as *privacy*, is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users or eavesdroppers who monitor the flow of traffic across a network. Encryption is frequently used to enforce confidentiality. Access control lists (ACLs) are another means of enforcing confidentiality.

Integrity

Integrity is the guarantee that data is protected from accidental or deliberate (malicious) modification. Like privacy, integrity is a key concern, particularly for data passed across networks. Integrity for data in transit is typically provided by using hashing techniques and message authentication codes.

Availability

From a security perspective, availability means that systems remain available for legitimate users. The goal for many attackers with denial of service attacks is to crash an application or to make sure that it is sufficiently overwhelmed so that other users cannot access the application.

3. WAN PROTECTION

All companies should protect its wide area network 'WAN' to make the connections between all their branches secure, and all sending data reach in safe hands as recipients. To let the external network of any company protected and high level secured, the virtual private network 'VPN' is a good solution to organize a secure access to the internal network remotely. Internet protocol security 'IPSec' is configured with VPN to have more security to the network. The encryption is a good process to support the communication to be secret by using a private key.

3.1 Virtual Private Network 'VPN'

One of the most important solutions to viruses and hackers' threats is VPN [4] that makes the network between companies and users secured; it is also authenticated and encrypted for security. VPNs provide the ability for two offices to communicate with each other in such a way that it looks like they're directly connected over a private leased line. Basically, a VPN is a private network that uses a public network "usually the Internet" to connect remote sites or users together. Instead of using a edicated, real world connection such as leased line, a VPN [11] uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. Three types of tunnelling or encryption protocols Windows Servers use for secure communication: L2F, L2TP and PPTP.

Layer 2 Forwarding "L2F": it creates network Access Server (NAS), initiated tunnels by forwarding Point-to-Point (PPTP) sessions from one endpoint to another across a shared network infrastructure. Because L2F is not client-based, systems do not need L2F client software of configuration. However, this also means that communications between the users, systems and the ISP are completely unprotected. L2F can use authentication protocols such as RADIUS and TACACS+. However, L2F does not support encryption.

Layer 2 Tunnelling Protocol "L2TP": it is IETF standard tunnelling protocol that tunnels PPP traffic over LANs or public networks. L2TP was developed to address the limitations of IPSec for client to gateway and gateway to gateway configuration, without limiting multivendor interoperability. In these configurations, all traffic from the client to a gateway, and all traffic between two gateways is encrypted. L2TP uses its own tunnelling protocol, which runs over UDP port 1701. Because of this, L2TP may be easier to pass through packet filtering devices than PPTP. L2TP can support multiple sessions within the same tunnel.

Point-to-Point Transfer Protocol "PPTP": it provides a protected tunnel between PPTP enabled client "personnel computer" and a PPTP enabled server. It is not a standard tunnelling protocol. It employs Microsoft Point-to-Point Encryption (MPPE) for data encryption. Microsoft developed PPTP, which like L2TP, tunnels Layer 2 PPP traffic over LANs or public networks. Microsoft has also created MS-CHAP to provide stronger authentication than PAP and CHAP. PPTP creates client-initiated tunnels by encapsulating packets into IP datagrams for transmission over the Internet or other TCP/IP based networks. So L2TP is more secured than PPTP. VPN services for network connectivity consist of authentication, data integrity, and encryption [11]. The two basic VPN types are remote access and site-to-site:

4. LAN PROTECTION

We have described previously our secure design for external network between companies. In this part we explain our secure design for the internal network of a branch and figure 3 below shows how our design of the local area network 'LAN' inside the office works step by step and organized in a way that allows secured and protected data communication to occur between users through security servers control inside the office. Therefore, the system protection includes a special care for users, computers and information under main servers' control such the Active Directory 'AD', Windows Server Update Services 'WSUS', the Symantec Update, Windows Right Management Services 'WRMS', and Self-control E-mail and Web Filtering 'SCEF'. In order to make the LAN safe during sending and receiving messages, and during systems' job administrator's control, there are many essential steps that keep the whole network process and users' access avoiding infections' threats, using specific protection's servers:

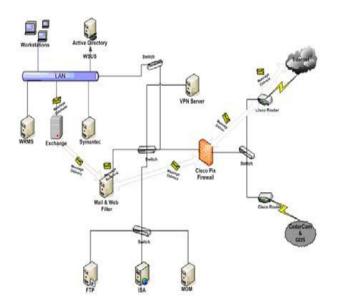


Figure 3: Proposed Security Design for LAN Topology

4.1 Active Directory

Active Directory 'AD' server is a common repository for information about objects that reside on the network, such as users and groups, computers and printers, and applications and files. Administrators put all users in the office under control and give them permissions through the Active Directory 'AD' server's configuration which stores data about user, computers and network Resources such as shared files, and printers, and lets only authorized users to access the AD. The Group Policy Object 'GPO' is configured in the Active Directory and gives various permissions to all users depending on each user's job level. The GPO lets the administrator gives permission for users such as password policies to define its complexity and its length and age, and it can remove the run command from the start menu to restrict modifying the windows' system, also the most important policy is that it can restrict CDROM and floppy access to locally logged on, and to disable media source for any install to avoid having viruses problems and system's infection.

4.2 WSUS

To keep office systems protected and updated, the Windows Server Update Services 'WSUS', which is configured in the Active Directory server, provides a capacity to download updates from Microsoft or from another WSUS server within user organization, and distributes these to its clients. WSUS provides a number of new features including targeting of patches to specific groups of machines, support for more products (e.g. Office), and improved reporting. WSUS is a service administrator run inside his organization — on one or more servers which he configures to serve software updates to one or more AU clients.

4.3 SurfControl E-mail and Web Filter

When the message gets inside the network, then the Pix Firewall scans and filters it against viruses. Therefore the SurfConftrol E-mail and Web Filter server gets the message and starts analysing and checking if it contains any spam or sex and adult words and any unsecured attachments, if the message is clean and clear, then the message continues on to reach the exchange server which provides a reliable messaging system that also protects against spam and viruses and finally the server distributes messages to all users in the office. SurfControl E-mail Filter is a part of the SurfControl Enterprise Protection Suite, a unified threat management solution that also employs advanced Web and endpoint threat protection, to provide comprehensive protection against today's known, emerging and internal threats that increasingly exploit multiple threat points.

4.4 Symantec Antivirus

The Symantec antivirus server monitors, configures and updates each computer on the office's LAN network, also helping users to make their files better fortified against risks and viruses. Then the Symantec Antivirus main purpose is to protect files on your network and client computers from viruses and others risks, such as spyware and adware. Each client on the network can be monitored, configured, and updated from a single computer by installing Symantec administrator tool that is called the Symantec System Center to verify which computers in the network are protected and working properly. The administrator can install and upgrade Symantec Antivirus clients and servers from the Symantec System Center.

5. CONCLUSION

This article proposed a secure design for network and system in windows environment using the latest technology. The security of networks always faces new potential threats as hackers and viruses advance. The design shows how the network can be more secure by encrypting the sending data using internet protocol security between user and server. The purpose of network security is to provide availability, integrity, and confidentiality. Thus, the main objective of VPN is to prevent outsiders (hackers) from interfering with messages sent among hosts in the network, and to protect the privacy and integrity of messages going through untrusted networks. The active directory manages all network resources such as servers, shared files, and printers, through authorization access resources. In addition to Active Directory, the main protection's servers such as WRMS, and WSUS, and Symantec make the internal network 'LAN' protected and secured against threats and viruses. After applying our proposed design and these concepts to an enterprise with worldwide branches, they proved efficient and highly reliable as network security mechanism. Therefore, all the mechanisms thoroughly discussed in this project proved to work well together and provide the needed security in any professional setting.

REFRENCES

- [1]. Allen R. and Alistair G. (2003). Active directory. O'Reilly.
- [2]. Fox C. (2006). Essential Microsoft Operations anager. O'reily.
- [3]. Munasinghe K. S. and Shahrestani S. A. (2004). "Evaluation of an IPSec VPN over a Wireless Infrastructure," in Proceedings of the Australian Telecommunication Networks and Applications Conference (ATNAC 2004), pp. 315-320, December 2004a.

[4]. Munasinghe K. S. and Shahrestani S. A. (2004). "Analysis of Multiple Virtual Private Network Tunnels over Wireless LANs," in Proceedings of the 3rdInternational Business Information Management Conference (IBIMA 2004), pp. 206-211, December 2004b.

Corresponding Author

Dr. Sandeep Kumar*

MCA from Kurukshetra University Kurukshetra, PhD from Singhania University