Managing the Organizational Network Security

Anamika Sharma
MTech Student
Lingaya's University, Faridabad
anamikaa2707@gmail.com

Neha Verma
MTech Student
Lingaya's University, Faridabad
nehasoni568@gmail.com

Abstract - Organizations daily face threats to their information assets. At the same time, they are becoming increasingly dependent on these assets. The rapid growth in the size and complexity of organizational networks will soon make the current way of manual management infeasible. Most information systems are not inherently secure, and technical solutions are only one portion of a holistic approach to information security. Recent years have seen many tools developed to automate this process. Establishing information security requirements is essential, but to do so, organizations must understand their own unique threat environment. There are also tools that scan networks and discover possible attack scenarios involving complex combination of multiple vulnerabilities. In this paper we are describing the network security followed by the management of that network security.

Keywords: Network Security; Information Security; Security Management; Security Infrastructure.

I. INTRODUCTION

It is not possible to protect anything unless one clearly understands WHAT one wants to protect. Organizations of any size should have a set of documented resources, assets and systems. Each of these elements should have a relative value assigned in some manner as to their importance to the organization. A key issue in network security management is how to define a formal security policy. A good policy specification should be easy to get right and relatively stable, even in a dynamically changing network. Much work has been done in automating network security management. But the policy languages used are usually operational and do not explicitly express the underlying security goal. Appropriate management of our computers (host, servers and desktops) and the network infrastructure interconnecting them is a critical information security requirement for the organization.

The underlying IT infrastructure must be designed, procured, deployed, operated and maintained in accordance with good information security principles. At the same time security systems must be maintained in a manner appropriate to the business requirements and commensurate with the value of data they contain and permit access to.

To prevent interruptions to business activities and ensure the correct and secure operation of computer and network facilities by:

- Minimizing the risk of systems failures (through use of appropriate operational procedures and plans)
- Safeguarding the integrity of the University's software and data
- Maintaining the integrity and availability of information services, networks and supporting infrastructure
- Preventing damage to assets by controlling and physically protecting computer media

II. DESIGNING SECURE NETWORKS

The architecture of a network includes hardware, software, information link controls, standards, topologies, and protocols. A protocol relates to how computers communicate and transfer information. There must be security controls for each component within the architecture to assure reliable and correct data exchanges. Otherwise the integrity of the system may be compromised.

In designing the network, it's necessary to consider three factors:

- The user should get the best response time and throughput. Minimizing response time entails shortening delays between transmission and receipt of data; this is especially important for interactive sessions between user applications. Throughput means transmitting the maximum amount of data per unit of time.
- The data should be transmitted within the network along the least-cost path, as long as other factors, such as reliability, are not compromised. The least-cost path is generally the shortest channel between devices with the fewest intermediate components. Low priority data can be transmitted over relatively inexpensive telephone lines; high priority data can be transmitted over expensive high speed satellite channels.
- Reliability should be maximized to assure proper receipt of all data. Network reliability

includes the ability not only to deliver error-free data, but also to recover from errors or lost data. The network's diagnostic system should be able to locate component problems and perhaps even isolate the faulty component from the network.

III. ORGANIZATIONAL NETWORK SECURITY

Organizational Security control addresses the need for a management framework that creates, sustains, and manages the security infrastructure, including:

- *Management Information Security Forum*
  Provides a multi-disciplinary committee chartered to discuss and disseminate information security issues throughout the organization.
- *Information System Security Officer (ISSO)*
  Acts as a central point of contact for information security issues, direction, and decisions.
- *Information Security responsibilities*
  Individual information security responsibilities are unambiguously allocated and detailed within job descriptions.
- *Authorization processes*
  Ensures that security considerations are evaluated and approvals obtained for new and modified information processing systems.
- *Specialist information*
  Maintains relationships with independent specialists to allow access to expertise not available within the organization.
- *Organizational cooperation*
  *M*aintains relationships with both information-sharing partners and local law-enforcement authorities.
- *Independent review*
  *M*echanisms to allow independent review of security effectiveness.
- *Third-party access*
  *M*echanisms to govern third-party interaction within the organization based on business requirements.
- *Outsourcing*
  Organizational outsourcing arrangements should have clear contractual security requirements.

IV. MANAGING NETWORK SECURITY

Managing computer and network security is easier than it may seem, especially if you establish a process of continual improvement—to keep the various requirements in perspective and to avoid forgetting about aspects of security. Security management centers on the concept of a security policy, which is a document containing a set of rules that describes how security should be configured for all systems to defend against a complete set of known threats. The security policy creates a balance between security and usability. The executive management team of your organization should determine where to draw the line between security concerns and ease of use. Just think of a security policy as the security rules for your organization along with policies for continual enforcement and improvement. The Management Security Forum consists of the Chief Information Officer, Engineering Manager, NOC or Data Center Manager, and the Information System Security Officer. Other members are included as required.

Management Security Forum duties include:

- Provide ongoing management support to the security process
- Serve as an alternative channel for discussion of security issues
- Develop security objectives, strategies, and policies
- Discuss status of security initiatives
- Obtain and review security briefings from the Information System Security Officer
- Review security incident reports and resolutions
- Formulate risk management thresholds and assurance requirements
- Yearly review and approval of the Information Security Policy

Network security management is by nature a distributed function. Applications that may utilize security management include firewalls, databases, Email, teleconferencing, electronic commerce, intrusion detection, and access control applications. Security management faces the same security threats as other distributed applications. Coordinated management of security is not feasible without a secure management infrastructure that protects in transit messages from modification, spoofing, and replay. Although end system security is beyond the scope of this discussion, it is clear that key management, access control, and reliable implementation of management software are critical also. In its crudest form, security management could require human presence at every security device and manual evaluation of all significant events. On the other hand, we believe that remote monitoring with computer assisted correlation and management of system events is just as viable for security management as it is for network management. In fact, it may be argued that detection of sophisticated attacks need the help of computer-assisted correlation tools even more

than network management systems. Here are some task which we have to perform for network security management.

- *Device configuration management*
  Centralized interface to quickly and easily deploy one or more devices provides a similar, intuitive interface across all device types and versions, along with complete support for all device features. Device templates enable administrators to define and maintain commonly used configurations in one place.
- *Policy management*
  Provides an intuitive, rule-based approach for all device families being managed, with a complete view of rule behaviors and options and powerful filtering capabilities. Allows network objects and services to be dragged and dropped directly into the policy rules from within the Policy or Object Manager window.
- *Centralized object management*
  Shared Object manager allows central administration of network, service, Network Address Translation (NAT), attack, antivirus/deep inspection objects from one interface that can be used by one or more policies.
- *Real-time monitoring*
  Enables administrators to actively monitor the status of large numbers of firewall/VPN and IDP Series devices, clusters, and VPN tunnels.
- *Intelligent security updates*
  An automatic, scheduled process updates the NSM attack object database, and new attack object databases can be automatically pushed to security devices.
- *Topology view*
  Centralized interface to discover and visualize a layer 2 topology on an Ethernet switched network. Discovered topology is automatically organized into sub networks, and network administrators can view the topology of each sub network as well as view the topology between sub networks. The zoom in and zoom out capability allows network administrators to easily navigate through the various parts of the network. The topology view also lists the various end hosts connected to the switch.
- *User activity management*
  Object locking allows multiple administrators to safely modify different policies or devices concurrently. Job Manager provides centralized status for all device updates, whether in progress or complete. Audit logs provide a record of configuration changes, supporting central oversight of business policy compliance.
- *Schema updates*
  Schema driven application that allows users to support updates and new devices quickly.
- *Log and report management*
  High-performance log storage mechanism allows collection and monitoring of detailed historical information on key criteria such as network traffic and security events. Using the complete set of built-in analysis tools, administrators can quickly generate reports for investigative or compliance purposes.

V. SECURITY RISK ASSESSMENT

The process of managing the risk is accomplished by developing a risk management and mitigation strategy, whereby assets, threats, and vulnerabilities are identified and the commensurate risk is quantified. Controls can then be selected to avoid, transfer, or reduce risk to an acceptable level. Security risk assessment is a method to maximize use of finite organizational assets based on measurable risk and organizational risk tolerance. Risk assessment steps are as follows:

- *Identify assets within the security perimeter*
  *A*n asset can be a tangible item, such as hardware, or intangible, such as an organizational database. By definition, an asset has value to the organization, hence requires protection. Assets must be identified, and ownership must be established. A relative value must also be established for each asset so importance can be established when risks are quantified.
- *Identify threats to the assets*
  Threats exploit or take advantage of asset vulnerabilities to create risks. Threats to each asset must be identified. There can be multiple threats for each asset. Identification of threats must be realistic. Only those threats that have a significant probability, or extreme harm should be considered. For example, a threat to the organizational database may be theft or alteration.
- *Identify vulnerabilities to the assets*
  *V*ulnerabilities are recognized deficiencies in assets that can be exploited by threats to create risk. An asset may have multiple vulnerabilities. For example, the vulnerability to an organization's database may be a poor access control or insufficient backup.
- *Determine realistic probability*

*P*robabilities for each threat/vulnerability combination should be determined. Combinations with statistically insignificant probability may be ignored.

- *Calculate harm*
  Harm (sometimes referred to as impact) may be quantified numerically to reflect damage from a successful exploit. This value allows the rating on a relative scale of the seriousness of a given risk independent of its probability. Harm is not related to probability.
- *Calculate risk*
  Mathematically, risk can be expressed as: **Probability x Harm = Risk.** This calculation results in a numeric rating of asset-based risk for a given set of threats and vulnerabilities. This numerical interpretation allows prioritization of finite risk-mitigating resources.

VI. CONCLUSION

This study has demonstrated how differing the viewpoints of the organization and the individual are when it comes to network security management. Organization's needs are often more directly connected with their financial mission or goal. This often means that they look for network security management to lower costs arising from network security breaches or for enabling new business opportunities. Today network security has to do with protecting your sensitive information from both outsiders and insiders. You need a security policy that covers all risks. Security tools such as firewalls, antivirus software, and encryption will help your company deter access to unauthorized users. Believing that your environment is secured is not enough. You have to take a proactive approach to security, making sure that newer technologies are implemented to keep up with sophisticated hacker tools. A safe and secure computer environment will protect your investments for the coming years.

REFERENCES

[1] Blum, Magedanz, Schreiner, Wahle, "From IMS Management to SOA based Management", Journal of Network and Systems Management (2009) 17, pp. 33-52

[2] L. Bernstein: "Network management isn't dying, it's just fading away", Journal of Network and Systems Management 15, pp. 419-424, DOI 10.1007/s10922-007-9080-y (2007)

[3] Gupta: "Network Management: Current Trends and Future Perspectives", Journal of Network and Systems Management 14, pp. 483-491, DOI 10.1007/s10922-006-9044-7 (2006)

[4] Angelos D. Keromytis, Sotiris Ioannidis, Michael B. Greenwald, and Jonathan M. Smith. The STRONGMAN architecture. In *Proceedings of the 3rd DARPA Information Survivability Conference and Exposition (DISCEX III)*, pages 178 – 188, Washington, DC, April 2003.

[5] Sushil Jajodia, Steven Noel, and Brian O'Berry. *Topological Analysis of Network Attack Vulnerabiity*, chapter 5. Kluwer Academic Publisher, 2003.

[6] Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M. Wing. Automated generation and analysis of attack graphs. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, pages 254– 265, 2002.

[7] Paul Ammann, Duminda Wijesekera, and Saket Kaushik. Scalable, graph-based network vulnerability analysis. In *Proceedings of 9th ACM Conference on Computer and Communications Security*, Washington, DC, November 2002.

[8] N. Damianou, N. Dulay, and M Sloman E. Lupu. The ponder policy specification language. In *Workshop on Policies for Distributed Systems and Networks (Policy2001)*, HP Labs Bristol, Jan 2001.

[9] Ronald W. Ritchey and Paul Ammann. Using model checking to analyze network vulnerabilities. In *2000 IEEE Symposium on Security and Privacy*, pages 156–165, 2000.