Week 2 Case Study -

Securing the Network Infrastructure

Anthony Meunier

DeVry University

SEC 280

Week 2 Case Study – Securing the Network Infrastructure

Any respectable business needs a means of securing its network infrastructure. Dealing with important and sensitive client information, as well as company information, requires the system to be secured. Not doing so can lead to potentially catastrophic consequences if there is a breach in (lacking) network security. In a larger-sized business, where employees reach into the hundreds or even thousands, security plays an even more important role in securing the network from/against both the outside, and inside.

Vulnerabilities and shortcomings to a network infrastructure are expansive and ever-evolving. Therefore, having basic means of protection against known vulnerabilities is a requirement when dealing with important client and business-related information and data. Some key concepts of network security in a company of this size includes ideas and practices such as: developing security policies from risk assessment, teaching employees about acceptable use, enabling management to set priorities, empowering administrators, using security policies to enable risk analysis, and formulating an overall security policy. This is, of course, in addition to having “basic” necessities of security in place, such as firewalls and secured physical network components.

In order to properly secure Windows and Unix/Linux servers vital to company operation, a proper security policy needs to be created and implemented company-wide. By following the guidelines listed above, a company can achieve a much more secured network infrastructure and therefore can better protect data integrity. Let’s explore some steps in creating a security policy. Firstly, it is wise to form a security policy committee which jointly determines which tasks are delegated to which members or groups are assigned which individual parts of the policy that is to be set in place. After this is done, the Acceptable Use policy is an important policy to determine and clarify because ultimately it affects the largest number of employees in the company. Guidelines need to be set for and adhered by, all members of the organization. User accounts and their usage helps play into this notion.

In addition to these steps, there are other areas that need to be covered as well. Remote access is important in today’s business-world because often times business needs to be conducted from places outside of the office. Having measures in place that spell out the guidelines for connecting to the organization’s network remotely help in securing the network because through role-based authentication these remote users have limited access to resources based on their role in the company. It may sound redundant, but a Password Protection policy has a useful place in providing network security because it simply serves as another line of defense in accessing the network. An extension of the Acceptable Use policy would be a specific outline of appropriate ways to access and use the Internet; this is important because of how integral Internet access has become in everyday business activities.

As always when discussing and implementing network security, it is much, much better to have an established system in place before an attack occurs. Any type of attack or compromise of security can be catastrophic for a business because not only does the business itself have data that needs to stay private, the company is also responsible for sensitive customer data that has been entrusted to them. Having prevention in place is much easier than performing disaster-recovery. When the latter happens it is often too late in the sense that you will have lost something that is not easily recovered – trust. By studying and practicing some of the methods listed here in creating and implementing a security plan, a company can achieve a lot in securing its network infrastructure, thus helping to secure its livelihood as a business.

References

Avolio, F. (2007, July 1). Producing Your Network Security Policy. Retrieved November 5, 2014, from <http://www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf>

Conklin, W., White, G., Williams, D., & Davis, R. (2009). *Principles of Computer Security, CompTIA Security and Beyond* (2nd ed.). McGraw-Hill Professional