Security domain and strategies

Technology, Internet

The Richman Company is a successful and prosperous firm with branches in eight locations throughout the country and Canada. To support its growth, the company uses both an intranet and an extranet network. These networks are essential to the successful operation of the company because they provide the means of communicating with all employees, who use the intranet to enroll in company benefit programs. These networks also allow all of the company’s business partners, vendors and privileged customers to gain information about the company. In recent years, the company has been expanding rapidly.

As one of the company’s interns, I have been asked to analyze the company’s vulnerabilities and make a plan to protect company assets and to utilize available technology most effectively. Before making the final proposal, I examined Richman’s use of the intranet and the extranet networks and found problems that require immediate attention. One problem that results in a grievous vulnerability regards the use of the intranet which Richman hosts for employees. I found that many of the computers were using Internet Explorer with the default setting “ Websites in less privileged web control zone can navigate into this zone” enabled.

According to Cesar Cerrudo, founder and CEO of Argeniss, a Internet website is able to reference an Intranet website by including a HTML FRAME or IFRAME from the Intranet website. Internet Explorer automatically requests and displays the content without user interaction. IE just displays “ Unknown Zone (Mixed)” in the status bar without raising any alerts nor prompting the user for authentication. This security setting allows an internet web page to view/refer to content in Richman’s intranet website. In order to preserve the company’s privacy, this default setting must never be used.

For example, all computers must be set to eliminate this window of opportunity for trespass into the company’s protected assets. Leaving this entry open would allow an intruder to enter the company’s intranet network and explore its contents. Another area of vulnerability is in Richman’s hosting of the extranet. The extranet is used by its business partners. In order to allow extranet servers access to its internal database, the company has to make openings in its firewall.

As stated by Karen A. Korow Diks, in “ Security Considerations for Extranets,” the more openings in the firewall, he greater the possibility for unauthorized people to get in and do damage. Since an extranet increases the number of network connections, it increases the risk of network penetration. Once a network is compromised, this provides an entry point for compromise of systems and data that exist for all other networks connected to it. In order to protect Richman and eliminate these glaring vulnerabilities and to strengthen its security policies, I have two recommendations: the formulation of a detailed security policy and the acquisition of the Cisco system ASA 5580 Series Adaptive Security Platform.

First, I would recommend that Richman take steps to make certain that all employees are knowledgeable of and in compliance with the Richman company security policy. According to David Kim and Michael G. Solomon, authors of the course textbook, the company policy statement should include the following:

•an explanation of how the company’s security will comply with laws, regulations and standards of due care and due diligence.

•detailed examples of the company’s direction for security in such areas as email, remote access and internet surfing. standards that mandate requirements for hardware and software solution used to address security risks throughout the organization.

•procedures that discuss the systematic action to accomplish a security requirement, process, or objective and covering such things as changing passwords, responding to incidents, and creating backups.

•baseline workstation requirements that list the components and configuration settings which will make it easy to ensure all new workstations are the same.

•baseline settings for each of the different operating system used by Richman such as Windows Vista, Windows 7, Windows XP, Windows 2000, and Mac OSX. a defined plan for auditing to include how security controls will be verified. Also, as a means of non-repudiation, once an employee participates in training to ensure knowledge of the company’s policy, the employee must sign a statement verifying agreement with and acceptance of the company policy.

Finally, after investigating several systems on the market and in order to best protect Richman from the vulnerabilities discussed above, I propose that the company contract with the Cisco Corporation for the acquisition of the Cisco 5580. According to the Cisco 5580 Data Sheet, this system has market-proven security capabilities.

The Cisco ASA 5500 Series integrates multiple full-featured, high-performance security services, including application-aware firewall, SSL and IPsec VPN, IPS with Global Correlation and guaranteed coverage, antivirus, antispam, antiphishing, and web filtering services. Combined with real-time reputation technology, these technologies deliver highly effective network- and application-layer security, user-based access control, worm mitigation, malware protection, improved employee productivity, instant messaging and peer-to-peer control, and secure remote user and site connectivity.

The only IPS with market leading reputation technology, Cisco IPS with Global Correlation provides twice the efficacy of legacy IPS and includes guaranteed coverage for enhanced peace of mind. Offering seamless client and clientless access for a broad spectrum of desktop and mobile platforms, the Cisco ASA 5585-X delivers always-on secure mobility with integrated web security and IPS for policy enforcement and threat protection. As stated in www. verisign. com/ssl, an important part of the above system is the SSL (Secure Sockets Layer), a cryptographic protocol.

SSL encrypts the segment of network connection above the transport layer using asymmetric cryptography for key exchange symmetric encryption for privacy and an authentication code for message integrity, thus addressing transmission methods and techniques as well as transport formats. Another aspect of the system that is necessary for Richman’s security is the IPsec VPN (Internet Protocol Security). According to the NIST guide to IPsec VPNs there must be a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP Packet of communication session.

IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. This will further add to the prevention of unauthorized access to the network via its intranet/extranet services. Also, according to Cisco, its SSL VPN has some unique features. Most noticeably SSL VPN uses SSL protocol and its successor TLS (Transport Layer Security) to provide a secure connection between remote users and internal network resources.

Unlike traditional IPsec remote-access VPN technology, which requires installation of IPsec client software on a client machine before a connection can be established, users do not need to install software in order to use SSSL VPN. As a result, SSL VPN is also known as “ clientless VPN” or “ web VPN. ” In conclusion, if Richman adopts these recommendations, it will be able to continue its growth without hindrance. It will prosper and remain in the forefront with the latest, cutting-edge technology.