Maryville University

WRIEL & Co.’s Critical Security Controls and Ethical Hacking

Kiauna Newman

ISYS 470

October 21, 2018

WRIEL and Company

WRIEL and Co. is small property management company comprising of ten employees, three mutually equally owners, five licensed real estate agents and two administrative assistants. The company has been running for over ten years, and the recent interest in critical security controls came from the widespread news coverage of a recent security breach at a local property management company. The company was one of WRIEL’s top competitors; the company was hacked by a local hacker currently in police custody for his actions. Reporters’ stated the hacker was able to get into the company’s system with the unbeknown assistance of a former employee, recently fired from the company. Reading this article in the newspaper made one of the owners’ of WRIEL and Co. realize having some critical security controls implemented in the company was needed and they also needed to know what vulnerabilities existed within their system.

They met up with our Cyber Security company to determine what policies and controls they should have in place. After reviewing the Three Different Shades of Ethical Hacking: Black, White and Gray, they felt obtaining more details would help them in marketing their company as a secured entity willing and able to protect their customers’ privacy, as well as protect the confidentiality of the company, by investing in critical security controls. Eager to assist them with a plan of action, myself and upper management decided to use the gray box approach because we all felt it would be best suited to find out their company’s vulnerabilities. While performing the penetration testing, I provided them with information of each of the controls and a suggestion on how to implement each control.

The first phase was the reconnaissance and foot printing. To perform foot printing and reconnaissance on WRIEL, we used WHOIS to determine the contact information for the company. We also looked on job boards to determine the type of software and operating system the company uses. A conclusion of the foot printing and reconnaissance stage led us to suggest the company, Wriel alter its job descriptions and implement screening policies for potential clients as well as more security protocols.

During the scanning and enumeration phase, we used Nmap and other enumeration tools. Our suggestion to Wriel is to implement CSI Controls 1 and 2. CIS Control 1 - Inventory of Authorized and Unauthorized Devices, is an important control because computer hackers make it their daily routine to identify companies who fail to protect their company’s system. Companies make the mistake of issuing their employees’ laptops as a way to get more work done. If the work cannot be done in the office, it can be done at home; so they issue laptops or allow employees to download company information and access it from their home computers. All laptops and external devices used to access, or store company information should be inventoried and ensured it contains the proper type of security to prevent unwanted access to company information. (CIS Control 1: Inventory of Authorized and Unauthorized Devices)

A company should have a thorough overview of their network and what hardware needs to be defended. The only way a company new to security control can know what is on their network is by having an inventory of the company’s hardware. With this knowledge, the first thing that must be done for WRIEL and Co is to create an inventory of all the hardware used to access the company’s network. A suggestion to achieve critical security control 1 is to “use a network scanner (commercial or open source) to identify all the devices on your network.” An open source network scanner that is used by many is NMap.

CIS Control 2 - Inventory of Authorized and Unauthorized Software - Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute. Also ensure that unauthorized and unmanaged software is found and prevented from installation or execution. (CIS Control 2: Inventory of Authorized and Unauthorized Software)

Hackers routinely look for companies with susceptible versions of software that can be easily accessed by anyone in the world. Some Hackers also distribute fake web pages using their sites or through third-party websites. This instance unsuspecting individual access the site the computer being used becomes vulnerable thereby making the company’s information an easy target. The hackers are now able to compromise their machines, often installing programs to access the company’s system via a backdoor and install some type of robotics that allows the hacker unlimited access and control of the system. Lack of knowledge and improper internal restrictions on the software used in the company provides to way for the company to protect their assets or their customers. (CIS Control 2: Inventory of Authorized and Unauthorized Software)

Lack of proper controls allows users to run software for personal use and makes the company available for outside attacks. The unwanted access on just one machine enables a hacker the ability to access all company information and thereby compromise the entire company. This type of compromise can not only impact the company but also its customers and potentially some of its competitors. (CIS Control 2: Inventory of Authorized and Unauthorized Software)

A suggestion to implement this control WRIEL and Co can utilize Microsoft’s free tool Microsoft Software Inventory Analyzer (MSIA). This is a cost-effective way to achieve critical security control 2. The Microsoft Software Inventory Analyzer (MSIA) is a free tool that can help with your software inventory. Using this tool, “you can generate an inventory of core Microsoft products that are installed on your local computer or throughout a network.” (Microsoft Software Inventory Analyzer Documents)

After performing the system hacking phase. Our team suggested WRIEL company implement CIS Control 3- Malware Defenses . (CIS Control 8: Malware Defenses) Vindictive also known as “malicious” software is a dangerous and vital part of Web-based threats, and is most likely designed to attack your computers, mobile devices, or any other device used to store your company’s data. The software can be quick to move, easily adaptable, and enter through any way possible via any desktop computer, laptop, mobile phone, tablet, personal/company email, websites, clouds, user installed apps and removable storage devices. Steps can be taken to disable this type of vindictive software by installing modern malware created as a defense. (CIS Control 8: Malware Defenses)

Malware defenses need to operate with all the changes coming on a constant basis. The guards must be implemented at multiple access points to detect, cease the movement of, or control the execution of the vindictive type of software. “Company endpoint security suites provide administrative features to verify that all defenses are active and current.” (The Center for Internet Security Ciritcal Security Controls for Effective Cyber Defense)

This control can be implemented by installing anti-virus software on the organization's network. An example of anti-virus software to use is McAfee Endpoint Protection. It has core endpoint protection. McAfee Complete Endpoint Threat Protection includes anti-malware, firewall, device control, and email and web security. This will provide the company with the necessary type of protection needed to offer a high-quality malware defense. (SANS Critical Security Controls Poster)

Works Cited

Arwine, Troy. “E-GOV Security (Part 2–Twenty Critical Cyber Defense Controls to Secure Citizen Data & Maintain Public Trust).” *"Stay Safe" Cyber Security Blog*, 22 Dec. 2010, blogs.technet.microsoft.com/staysafe/2010/12/22/e-gov-security-part-2twenty-critical-cyber-defense-controls-to-secure-citizen-data-maintain-public-trust/.

*The Center for Internet Security Critical Security Controls for Effective Cyber Defense*. Version 6.1 ed., The Center for Internet Security, 2016, www.cisecurity.org/controls/.

*CIS Control 1: Inventory of Authorized and Unauthorized Devices*, www.cisecurity.org/controls/inventory-of-authorized-and-unauthorized-devices/.

*CIS Control 2: Inventory of Authorized and Unauthorized Software*, www.cisecurity.org/controls/inventory-of-authorized-and-unauthorized-software/.

*CIS Control 8: Malware Defenses*, www.cisecurity.org/controls/malware-defenses/.

“CIS Controls: Implementation Guide for Small- and Medium-Sized Enterprises (SMEs).” *CIS Controls*, www.cisecurity.org/wp-content/uploads/2017/09/CIS\_Controls\_Guide\_for\_SMEs\_2017-1.pdf.

“McAfee Complete Endpoint Threat Protection.” *McAfee Complete Endpoint Threat Protection – Endpoint Protection | McAfee Products*, Mcafee, www.mcafee.com/us/products/complete-endpoint-threat-protection.aspx.

“Microsoft Software Inventory Analyzer Documents.” *Microsoft - Official Home Page*, www.microsoft.com/en-us/download/details.aspx?id=20934.

Pescatore, John, and Tony Sager. “SANS 2013 Critical Security Controls Survey: Moving From Awareness to Action.” *SANS Institute Reading Room*, SANS Institute, Jan. 2013, www.sans.org/reading-room/whitepapers/analyst/2013-critical-security-controls-survey-moving-awareness-action-35065.

“SANS Critical Security Controls Poster.” *SANS*, Council on Cyber Security, 2014, www.sans.org/media/critical-security-controls/Poster\_Fall\_2014\_CSCs\_WEB.PDF.