Maryville University

Moving WREAL & Co.'s Awareness of Critical Security Controls to implementation: WREAL and Company

Kiauna Newman

Mark Dalle

ISYS 280

March 10, 2018

WREAL and Company

WREAL and Co. is small property management company comprising of ten employees, three mutually equally owners, 5 licensed real estate agents and 2 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 WREAL'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 the one of the owners' of WREAL and Co. realized having some type of critical security controls implemented in the company is needed.

They met up with various Cyber Security companies to determine what controls would be the best fit for them to start with, but they were not satisfied with the recommendations. One of the owner's reached out to me and I provided them with the SANS 2013 white paper. After reviewing the SANS 2013 Critical Control Survey: Moving from Awareness to Action they asked me to provide more information on some controls. (Pescatore)They felt obtaining more information would help them in marketing their company as a secured entity willing and able to protect their customers' privacy, as well as the privacy of the company by investing in critical security controls. Eager to assist them with a plan of action, I identified the following three controls: 1. Inventory of Authorized and Unauthorized Devices, 2. Inventory of Authorized and Unauthorized Software, 8 Malware Defenses. (The Center for Internet Security Ciritcal Security Controls for Effective Cyber Defense)

I provided them with information of each of the controls and a suggestion on how to implement each control. The following information assisted them with their move from awareness to implementation.

CIS Control 1 - Inventory of Authorized and Unauthorized Devices; “Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access”. (CIS Control 1: Inventory of Authorized and Unauthorized Devices)

This control is important because computer hackers make it their daily routine to identify companies who fail to protect their company’s system. Company’s make the mistake of issuing their employees laptops as 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 inventory of the company’s hardware. With this knowledge, the first thing that must be done for WREAL and Co to implement this control is to create an inventory of all 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. ‘This is a

multipurpose scanner that can be used to locate and identify which devices are connected your network.' Once the company has an accurate inventory of their systems they are on the right track to successful implementation for one critical security control. (CIS Controls: Implementation Guide for Small and Medium Sized Enterprises)

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, and 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 from anyone in the world. Some Hackers also distribute fake web pages using their own sites or through third party sites. This instance an 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/or install some type of robotics that allow the hacker unlimited access and control of the system. Lack of knowledge and improper internal controls on the software used in the company allows 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 allows 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 it customers and potentially some of its competitors. (CIS Control 2: Inventory of Authorized and Unauthorized Software)

A suggestion to implement this control WREAL and Co can utilize Microsoft's free tool Microsoft Software Inventory Analyzer (MSIA). This is a cost-effective way to implement 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." (Arwine)

CIS Control 3- Malware Defenses - Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action. (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 attach of 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 defenses 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.

This control can be implemented by installing an anti-virus software on the organizations network. An example of an 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 essential type of protection needed to provide 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.

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.