Unit 1 Research Project

Eddie S. Jackson

Kaplan University

IT540: Management of Information Security

Kenneth L. Flick, Ph.D.

09/23/2014

Table of Contents

Abstract

The unit one research project presents a two-part assignment that deals with information security concepts. In part one of the assignment, a list of ten technology-based objects are to be listed, relative security threats acknowledged, and then a security policy drafted to reduce or moderate such threats. In part two of the assignment, a mock security policy is to be reviewed for missing, incomplete, inaccurate, and ill-advised aspects in the given policy. The main components of the policy include email, encryption, shared folders, backups, portable devices storage devices, and passwords. Due to the many elements of the security policy, further research was in order to perform a proper security policy analysis.

Keywords: POP, SMTP, PGP, SSL, passwords, portable storage

Unit 1 Research Project

Part I

The main objective of Part I of the assignment is to list ten company devices or systems that need to be protected by information security. These technology-based items must be linked to a potential threat, as well as a proposed security-related policy given to mitigate the possible threat. The ten items that have be selected for a security policy analysis are: laptop hardware, desktop hardware, the email system, sensitive data being stored on hard drives, end-user passwords, operating system integrity, mobile phones, company backup tapes, walk-up access to employee desktops, and company servers.

Laptops. Laptop computers offer the mobility of moving around inside and outside of the company, and permit the employee to work in an online and offline fashion. The associated threat of using laptop computers is the hardware being lost or stolen. To reduce the loss of equipment, and ultimately loss of company revenue, it is the company's policy to install Computrace on all laptops. Computrace is part of the MCLA Laptop Initiative and is known as persistent software (MCLA, n.d., para. 1). Computrace works by embedding itself in the BIOS and on hard drive of the computer, which acts an Internet beacon. And, in the event that a laptop is lost or stolen, a company can work directly with the local authorities to recover the laptop.

Desktops. Desktop computers usually sit on end-user's desks, inside the company itself. Even though the computer is within the walls of the organization, the actual hardware could be carried out the front door; this would result in loss of inventory, as well as a breach in security. To mitigate the direct theft of the equipment, most computers are outfitted with security-based slots, where a security cable can be attached to the device itself. Once the security cable is in place, the cable can be looped around a portion of the desk, a pole, or even mounted to the floor. The desktop security policy will state that the high-carbon steel Kensington Desktop and Peripherals Locking Kit be purchased and attached to each desktop (Kensington, n.d.).

Email. The Email system is essential to many of the daily business processes at a company. One particular area of concern is Email messages being hijacked or read during transmission. To protect messages in transit, the SSL (Secure Sockets Layer) security protocol has been selected. SSL encrypts the communication stream between the sender and recipient of the Email message (SSL, n.d., para. 1). At its core, SSL operates by utilizing a certificate. A SSL certificate contains all the necessary details that allows point A to send secure messages to point B, and vice versa. It is important to note, that without implementing SSL, the Email message would be sent in plaintext, which any level of electronic eavesdropping could exploit. Thus, the Email security policy mandates that all email transmissions, POP (receiving email) and SMTP (sending email) must have the SSL option selected in whichever email client is being used (Microsoft, n.d., para. 1).

Sensitive data on hard drives. It is common practice at many organizations to access sensitive data stored on server hard drives, as well as laptop and desktop hard drives. There is a genuine threat that this sensitive data (perhaps client financial or healthcare information) could somehow end up in the wrong hands or outside the company. In the case where hard drives that have sensitive data are lost or stolen, the data on the drives must remain secure. To guarantee the highest level of hard drive security, a full hard drive encryption strategy is recommended, specifically Microsoft's Bitlocker Drive Encryption. Bitlocker protects the entire hard drive by encrypting the hard drive and storing cryptographic information in a TPM chip, or Trusted Platform Chip (Microsoft, para. 1). The TPM is a special chip on the motherboard that works to secure the hard drive by using a tamper-resistant technology. By implementing Bitlocker on all company hard drives, the stored data is protected against outside or offline attacks.

Consequently, the hard drives policy states that all company hard drives will have the Bitlocker software installed.

Passwords. Maintaining end-user password security is critical to granting the right person to the right network resources. The primary weakness in passwords is the cracking of simple or commonly used passwords. Once a hacker has cracked a password, computer systems and company data have been compromised. To reduce the probability that a password can be cracked, password complexity and expiration rules are in order. The task of password complexity and password resets could become the responsibility of the end-user; however, this may lead to compromised security due to human error or negligence. The best practice method for enforcing password complexity and expiration rules is to use software policy, specifically group policy (Microsoft, n.d.). Group policy allows several password complexity requirements to be enforced; these would include: enforce password history; maximum password; minimum password age; minimum password length; and passwords must meet complexity requirements (Microsoft, n.d., para. 1). Implementing this kind policy allows the system administrator to require an end-user's password to contain alphanumeric characters, upper and lower case letters, special characters, and Unicode characters. Thus, the password security policy dictates that all passwords must adhere to the group policy.

Operating system integrity. Companies run on laptops, desktops, and servers–and these devices run on operating systems. Operating systems, which manage tasks, memory, software, and hardware, are constantly under attack by the hacker community through viruses, worms, malware, etc. (GFC Learn Free, n.d., para. 1). These attacks constitute a serious threat to the daily workflow and operations within the business. To mitigate such a wide range of possible threats, it is critical that the operating systems be patched. This can be accomplished using software such as Microsoft's Windows Server Update Services (WSUS). WSUS, which is a free add-on from Microsoft, permits a company to schedule and deploy critical updates, security patches, and application updates to a fleet of computers (Tech Target, n.d., para. 1). By keeping machines up-to-date, the operating systems maintain the highest levels of integrity, and reduce the chances of known exploits having an impact on work processes. And, due to this increased operating system integrity, the operating system policy states all machines must receive updates at least once a month.

Mobile phones. Mobile phones, or the more common term of smartphones, offer the functionality of many computer-based services and features at the touch of a user's fingertips; this can be great for multi-tasking, checking Email messages, and working on the go. However, with this increased mobility and functionality also come new security threats. A lost or stolen mobile phone can compromise security by allowing private company Email messages, client data, and contact lists to be wide-open to the public. To protect this data on mobile devices, passwords could be placed on phones; however, a clever hacker can get around a password. A better solution would be to remotely erase the data on the phone upon notification that the device is missing (the device can also be disabled at the same time). Different mobile vendors have various software solutions to perform this wipe functionality; for example, Apple uses the iCloud; Google Android uses Android Lost; and the Windows phone can be erased and disabled by accessing the website http://www.windowsphone.com/en-us (Lendino, 2012). Consequently, the mobile phone security policy will state that all company mobile phones must be erased and disabled as soon as the phone has been established as missing.

Backups. Company backups are the data backups done to tape and hard drives. The relative threat associated with backups is when they are stored offsite; the backups could possibly be lost, stolen, or damaged. Backups are vital in the case of a disaster recovery or the loss of data onsite; backups are required to restore business continuity. The offsite storage could be handled by the company, but this increases the chances of a breech in security. A best practice solution would be to use a reputable offsite data management and backup service, such as Iron Mountain. Iron Mountain specializes is data backup, storage, and disaster recovery, while at the same time offering highly secure pickup and delivery of data backups (Iron Mountain, n.d.). Thus, due to the importance of offsite backups, the backup policy mandates the use of Iron Mountain as the primary servicer for data management, daily pickups, and facilitation of data restorations.

Unlocked computers. No matter how complex a password is, if an end-user walks away from their desk with their computer unlocked, security can be compromised. The main threat of unlocked workstations, while end-users are away, is that anyone could just walk up to the computer and gain unauthorized access to network resources. Moreover, sensitive company and client information could be stolen. To protect against unauthorized access to network resources, the desktop usage policy states that screensavers must be activated ten minutes after the computer is idle, as well as all personnel being required to lock their machines while away from their desks; this will be strictly enforced via warnings and write-ups (Microsoft, n.d., para. 1).

Company servers. Another area of major concern is protecting physical access to company servers. Company servers contain the core applications, databases, and shared files of the organization. The theft or damage to any one of the servers could prove catastrophic to business operations. Thus, all company servers will remain behind locked doors, with limited access. Specifically, the servers will be contained within a data center with built-in perimeter security. The data center security solution is from ASSA ABLOY, which offers blast, wind, and fire protection, as well as digital locks, identity management, and key systems (ASSA ABLOY, n.d.). Because maintaining tight security around and into the data center is critical to business operations security, the company server policy will mandate all servers be protected in a data center designed by ASSA ABLOY.

Part II

The second part of the assignment segues into reviewing the Acme security policy, and identifying the missing, incomplete, inaccurate, and ill-advised portions of the policy. The main objectives of Part II of the assignment is to create an awareness towards weak security policy, and to research best practices as it relates to the design and implementation of information security policies.

Four major areas of concern. The four major areas of concern are end-user passwords (User Account Security Vulnerability), company backups (Physical Access Vulnerability), email security (Mail System Vulnerability), and provisioning proper access to company resources (Internal Vulnerability) (T&M, n.d.).

Incomplete aspects of the security policy. When considering laptop computers and screensavers with enabled passwords, what is missing from the original policy statement is exactly how long the computer idles before the workstation will automatically lock; a recommended idle time limit would be ten minutes, which can be enforced through local or domain group policy (Microsoft, 2009, para. 2). The second incomplete policy has to do with the Acme company backups, which are being stored offsite in a secured location. What is missing from the policy is how often the backups are done, who they are done by, and who has access to the backups. A suggested backup strategy would include the backup operator performing a full backup on Monday, and incremental backups throughout the rest of the week; and using Iron Mountain to store backups offsite (Comodo, n.d., para. 1).

Inaccurate sections of the security policy. When considering portable storage devices, such as USB flash drives and Firewire disk drives, it is important to recognize that the use of such devices pose a considerable threat to security. The original Acme policy stated that using portable devices with encryption would be acceptable, however this is inaccurate. Portable storage devices are still prone to theft, hardware failure, and being infected with malware (Schwartz, 2011). There is also the scenario where a drive may not be encrypted, sensitive client was stored on the device, and the device was lost or stolen. Thus, the portable device security policy should state portable devices should never be used to store client or company information. The second inaccurate security policy has to do with screensavers. The Acme policy stated that laptops were to have password enabled screensavers and that users were to switch on their screensaver to lock the workstation while away; screensavers are not usually initialized by the end-user, thus cannot be used by the user to lock a computer. A better security policy would enforce the screensaver to auto-lock after ten minutes, as well as include a clause that states the end-user must manually lock their computers [while away] by using the menu driven options or hotkeys such as pressing the Windows + L buttons on the keyboard (Microsoft, n.d.).

Inaccurate sections of the security policy. The Acme password security policy suggests that choosing an uncommon word as a password is acceptable; this is incorrect. Password selection is more than just not choosing a common dictionary word. Passwords *should* be chosen wisely, however the user password compliance must be enforced using policy, such as group policy. For example, a best practice password policy would mandate that a user password be a mixture of letters and numbers, one special character, and one upper case letter (Microsoft, n.d., para. 1). The second inaccurate section of the security policy deals with security sensitivity levels. The Acme policy states suggested security sensitivity levels should be unrestricted and client sensitive; these do not support a wide enough sensitivity range and are not considered industry standard. More adequate, commercially-based sensitivity levels would be public disclosure, internal, confidential, and strictly confidential (Brother, n.d.). There are also private sector security levels of unrestricted, confidential, secret, and top secret; however, these security levels are not recommended in this security policy (Oracle, n.d., para. 4).

Ill-advised aspects of security policy. Acme is to perform periodic backups, which are to be stored offsite with shared access; the ill-advised aspect of the security policy is the shared access portion. Company backups should only be available to backup operators and disaster recovery personnel; otherwise there is a risk of stolen or damaged backups. The second ill-advised policy deals with the administrator account being given out to consultants. The administrator account should never be given out, other than to system administrators and those directly responsible for the daily maintenance and administration of company equipment (such as technical support analysts that work for the company). All other personnel should have an account created, which is then added as a member to the suggested group name Consultants_Group; this group will delineate administrative access to its respective members. Using this strategy, the consultants have the ability to do their job, while the local administrator account remains secure.

References

ASSA ABLOY. (n.d.). Data Center Security Solutions from ASSA ABLOY. Retrieved from http://www.assaabloydss.com/en/local/dss/Solutions/Data-Center-Solutions/

Brother. (n.d.). To properly manage and protect information. Retrieved from http://technet.microsoft.com/en-us/library/cc875814.aspx

Comodo. (n.d.). Selecting the backup type. Retrieved from http://help.comodo.com/topic-9-1-455-4993-.html

GFC Learn Free. (n.d.). What is an operating system? Retrieved from http://www.gcflearn free.org/computerbasics/2

Iron Mountain. (n.d.). Services. Retrieved from http://www.ironmountain.com/Services.aspx

Kensington. (n.d.). Desktop and peripherals locking kit. Retrieved from http://www.kensington.com/us/us/v/4482/1664/ desktop-and-peripherals-locking-kit#.VCDb8MZ0x3A

Lendino, Jamie. (2012/4/12). How to remotely disable your lost or stolen phone. Retrieved from http://www.pcmag.com/article2/0,2817,2352755,00.asp

Microsoft. (n.d.). Best practices for enforcing password policies. Retrieved from http://technet.microsoft.com/en-us/magazine/ff741764.aspx

Microsoft. (n.d.). BitLocker Drive Encryption overview. Retrieved from http://windows.microsoft.com/en-US/windows-vista/BitLocker-Drive-Encryption-Overview

Microsoft. (n.d.). Enforcing strong password usage throughout your organization. Retrieved from http://technet.microsoft.com/en-us/library/cc875814.aspx

Microsoft. (2009/10/30). Group policy settings for personalization. Retrieved from http://technet.microsoft.com/en-us/library/ee617164(v=ws.10).aspx

Microsoft. (n.d.). How to quickly lock your computer and use other Windows logo shortcut keys. Retrieved from http://support.microsoft.com/kb/294317

Microsoft. (n.d.). POP3, SMTP, and other e‑mail server types. Retrieved from http://windows.microsoft.com/en-us/windows-vista/pop3-smtp-and-other-e-mail-server-types

Microsoft. (n.d.). Use your Windows password for your screen saver password. Retrieved from http://windows.microsoft.com/en-us/windows/windows-password-for-screensaver-password#1TC=windows-7

MLCA. (n.d.). Computrace. Retrieved from http://techhelp.mcla.edu/index.php/ Computrace_Software

Oracle. (n.d.). 6.1.1.1 Classification Levels. Retrieved from http://docs.oracle.com/cd/E23943_01/doc.1111/e10640/c06_classifications.htm

Schwartz, Matthew. (2011/8/8). How USB sticks cause data breach, malware woes. Retrieved from http://www.darkreading.com/risk-management/how-usb-sticks-cause-data-breach-malware-woes/d/d-id/1099437

SSL. (n.d.). What is SSL? Retrieved from http://info.ssl.com/article.aspx?id=10241

T & M. (n.d.). Information Systems Security Audit. Retrieved from http://www.tmprotection. com/InformationSystemsSecurityAudit.php

Tech Target. (n.d.). Windows Server Update Services (WSUS). Retrieved from http://searchwindowsserver.techtarget.com/definition/Windows-Server-Update-Services-WSUS