COMP7330 Assignment 2

Topic: " implementation of the anti-ransomware on campus network systems "

Student Number: ____ 15451682_____

Student Name: _____CHEUNG Saiho_____

Program: _____MSc AIS_____

Abstract: Ransomware is a type of malware, and denial-of-access attack, the infection mechanism is kidnapping some different types of files in the victims' computers for payment request through the network when most of anti-virus software cannot kill it. Therefore, the system administrator needs to implement a coherent of security countermeasures in which kind of sensitive data should be protected in the campus network system.

Background:

In the 21th century, most of academic institutes and schools have implemented the computer network systems which are providing the variety of systems to communicate and share information with everyone, such as e-mail system, document management system, etc. there have contained the amount of sensitive data in the document files, including student personal data and grading report.

Briefly introduction of the ransomware:

As the hackers want to steal this sensitive data on these kind of systems, they have sent the fake e-mail about the promotion of teaching products to the staff which embeds the harmful program code. It is a typical case in network attack, such as ransomware. It is found in 2012 and a later type of malware, the symptom is kidnapping the victim data in all IT devices, instead of computer only. The infection file types have included document, executable program and image. (Hampton &Baig, 2015)

The threat mechanism of ransomware:

The ransomware is belonging to a denial-of-access attack and prevented access to these files for using asymmetric key encryption mechanism. The threat mechanism has separated in the four steps, the first step is that the ransomware has installed itself in victim computer and set keys in the boot table of the operating system during running automatically every time. The second step is synchronized to secret channel between the criminal's server and victim computers and generate one pair of cryptographic key, the public key is stored in victim computer, the private key is stored in criminal's server securely. The third step is that the ransomware has encrypted the common types of files on victim computers. The fourth step sends the payment request of the victim. (Zimerman, 2010)

A scourge of the ''Locky'' ransomware

According to the news report has claimed that many teacher's computers have infected the 'Locker'

malware via junk email, the teacher has opened this email and triggered the trap of hyperlink, all document and program files must be locked in their computer and network drive which is prompted windows for payment request. (“Locky 勒索病毒肆虐 數十校中招 - Yahoo 新聞香港,” n.d.) They must need to pay the few hundred dollars or a piece of bitcoin when a hacker has provided the private key to decrypt the locked files. Otherwise, these files cannot open again without payment.

A set of security countermeasures against ransomware

In this case, the system administrator should have proposed a coherent set of security countermeasures to prevent the ransomware attack. It is mainly focused on the logical control which is including the file backup strategy, update system patch program frequently, password and system policy control and e-mail system protection. (Endres, 2010)

For the file backup strategy, the administrator must need to do a full backup in weekly, incremental backup in daily and restrict all common files storing on the file server, including document and media files. The system backup image files should be stored in some external hard disks or the mirror backup site in different locations.

For the update system patch program frequently, the anti-virus software and operating system must need to update patch program and latest version frequently. It should have enabled the windows update service when all computers have installed the update files in central and reduce the network traffic.

For the password and system policy control, all user’s password has expired within three months and simple password is not acceptable enforcement. On the other hand, the system security policy must need to restrict some access right for the group of users, such as no allowed install any software in the computer, disable the Macro function in Microsoft office and the network drive is only allowed to access the specify users when they need.

For the e-mail system protection, the security setting has ignored all incoming e-mails when they come from the interested destinations. Some email systems can block the email which contains the keywords or attachments in the defined checklist for input by administrator. (Posey, Alabama, Box, Posey, &Garrison, n.d.)

Conclusion:

In conclusion, the most important things are concerned that the users should not access the untrusted

e-mails or websites, the IT officer should update and review the security assessment potential threats in campus network from time to time.

Bibliography:

Endres, G. C. (2010). Back to School. *Nation*, *291*(12), 2.

Hampton, N., &Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace. *Australian Information Security Management Conference*, *2015*, 47–56. http://doi.org/10.4225/75/57b69aa9d938b

Locky勒索病毒肆虐 數十校中招 - Yahoo 新聞香港. (n.d.). Retrieved March11, 2017, from https://hk.news.yahoo.com/locky勒索病毒肆虐-數十校中招-225526550.html

Posey, O. G., Alabama, A., Box, P. O., Posey, R. B., &Garrison, C. P. (n.d.). PHISHING : ONE HOOK , MULTIPLE CATCHES : EXAMINING THE VULNERABILITY OF ACCOUNTING STUDENTS TO USER-NAME AND PASSWORD COMPROMISE, 47–54.

Zimerman, M. (2010). Protect your library's computers. *New Library World*, *111*(5/6), 203–212. http://doi.org/10.1108/03074801011044070