Texila International Journal of Academic Research
Volume 4, Issue 2, Dec 2017

End Users Security Awareness Campaign from Information Security Threats, Vulnerabilities and Concurrent Cyber-Attacks

Article by Francis Kwesi Aidoo
Master of Science in Information Technology, Texila American University
E-mail: itfrancis4u@gmail.com

Abstract

The intent study of this article is to fortify the protection of sensitive data and information from breach any means necessary from attack either an insider or an outsider in the organizations. In every firm, the core achievement of its information security is to entrust the CIA-Trid; Confidentiality, Integrity and Availability of all of their resources and the liable personnel to disclose confidential information from breach is the end users of the system, having them in their respective field of assignment accordingly. This year 2017, research and analysis information gathered on the incident which took event on May/June ransomware cyber-attacks "WannaCry and Petya" affected many organizations such as companies and government agencies in different countries around the world demanding a ransomware bitcoin $300 method of payment, failure to comply will be subject to accumulate in double every day repeatedly. The breadth of study is to introduce the End User Security Awareness Campaign in the Organizations as a routine practice to stay awake from numerous information security threats, vulnerabilities and concurrent cyber-attacks circulating in different organizations around the global countries. To achieve the objectives, end users will partake in continuous awareness training and assessment through social engineering practices and procedures on how to stay vigilant to prevent every user from such attacks. The organizational IT function will also partake the involvement of hardware and software firewall applications, regular windows updates and patches, consistent antivirus updates, which will restrain the vulnerabilities to risk and any associate attacks to that effect.

Keywords: *End user security awareness from information security threats, vulnerabilities and cyber-attacks.*

Introduction

Systems and security devices are installed to check the rampant attacks on an organization's information system and reduce the its impacts, end users on the other hand, tend to have the weakest links to the system by exposing classified information knowingly or unknowingly, this could be as a source to the attacker causing a breach in the security. Information security and cyber security as defined to be the strategic process, policies and tools for ensuring and preventing unauthorized access to vital data and information from modification, disruption and disclosure. It has been partaking an acute role in our day to day business processes in different organizations and individual lives. Computers were designed to make work easier in the field of information system that also partakes the advantages and disadvantages of its usage in the information technology field. In this paper, we are going to scrutinize and disseminate the "pros and cons" why the need for the study topic end user's information security awareness campaign from numerous threats, vulnerabilities and consistent cyber-attacks in everyday usage of the network and internet. Only this year, research and analysis captured depict the numerous ransomware attack through Server Message Blog Port, under the environment of the Microsoft operating product. This attack affected over 150 countries around the Globe, and 230 victims of computers and beyond. One important objective of this paper is to review the source of the rampant security threats, vulnerabilities and cyber-attacks, circulating in various organizations respectively, and then how can we partake in its resolution, introduce the end user's security awareness training campaign to educate every user of the system from such risk by enforcing the

DOI: 10.21522/TIJAR.2014.04.02.Art020
ISSN: 2520-3088

(CIA-Triad), Confidentiality, Integrity and Availability to protect sensitive data and information from breach by any hacktivist.

The below figure is an overview of the scope of study, end user security awareness campaign and its achievement from information security threats, vulnerabilities and cyber-attacks, associated to hacktivism;

An overview of end user security awareness campaign – achievement.

Figure 1.0. An overview

Problem statement: "ransomware cyber attacks"

Maintaining the integrity of information has become crucial to individual and business organizations of today. In the figures shown below, depict the consistent ransomware threats and attacks captured within the middle of the year 2017 and yet to be experienced more if inadequate policies and procedures are not met to be adhered, in order to mitigate the frequent occurrences. This type of ransom attacks; "WannaCry & Petya" uses the exploitation of Server Message Block, (SMB) Port "Eternal Blue" phishing mechanism to propagate into the operating systems. It has affected over 230 victims and more than 300.000 computer devices around the globe, subject to increase in accordance to research. The role of this "External Blue" exploitation vulnerability in the Microsoft Operating System environment is encrypted the user's information and then demand a ransom payment "Bitcoin Crypto-Currency" $300 to be remitted by the victim, subject to increase in every three days $600 if delayed. This has affected the following organizations; Post office, Airport, Health Centers, Banks, Power Grid, Maersk Line, all of the global countries such as; Ukraine, Russia, Germany, Netherland, India, Brazil, Spain, China, Hong Kong, Italy etc.

Any existing solution for the problem

Most organizations involve the implementations of intelligent hardware devices" firewall" as a plus and the entry point to the internal resources, intent to protect their network resources from breach by any attacker. The best thing to do is to find the best palpable solution to secure your network from being invaded. The primary objective of an intelligent firewall device will be to scrutinize, limit and protect a network from any attack, this attack could be generated from within or from an external source to cause harm. When we look at the genesis of cyber-attacks, they are not limited to, firewalls protection why because, hackers are smart to invade into every system provided there's a vulnerability, which can be possible through manipulation practices "social engineering" to iron out the loopholes on the network typical practice e.g.:

phishing, pretexting, quid pro quo, etc. Other measures that organizations also consider to ensure the integrity of their information is to have antivirus on their servers and client workstations, account login password, automatic windows or operating systems update, etc. All this solution has been in provision but still, there's a deficiency in their information systems which is vulnerable to risk.

Which one is the best one

Well, preferably, with all of the above stated measures should be adequate to ensure the maximum required protection of every organizational data and information except, when the end users of the system do not familiar themselves with the internet for their day to day organizational business activities are neither accept any removal or hot swappable device but still, the system will be prone to risk why because in every information security, there's nothing like hundred percent assurance of security. To maximize and mitigate the flaws in every organizational information security system, the best option and top priority in every information system is to safeguard the **CIA – Triad,** acronym Confidentiality, Integrity and Availability and this can be achieved through the end user security awareness campaign program mandated to be adhered by every user of the system to become familiar with the petrified threats, vulnerabilities and consistent cyber-attacks. One significant use of having a concurrent end user security awareness campaign is that, it abreast the user's knowledge for understanding how they can be manipulated in the field of social engineering characteristic typical, phishing, quid pro quo, pretexting and so forth. With all this practice been factored in every organizational information system, controlled and monitored periodically, the possibility of a consistent cyber outbreak will be deduced to the least minimal percent, which will guarantee the integrity of sensitive information from breaches in returns to have access to your own data, you need to remit a ransom bitcoin payment to the attacker **"hacker"** not limited, possible to apply the principles of social engineering to impersonate someone for identity theft or credit card fraud etc. So in all, when this measures are restored in the organization as a mandated policy and procedures, monitored and controlled, periodic antivirus updates, server updates and patches, clients work stations scheduled updates, enforced CIA-Triad practice, end user security awareness campaign program mandated periodically inclusive on the topic, social engineering practice, then the maximum assurance of security can be achieved to protect the company vital and sensitive information and also to save money from such consistent ransom cyber-attacks.

Limitations

There are laid rules and policies governing how an organization's information system, disseminated, these set the roadmap to what practices are generally accepted or rejected the regardless status or positon, in order to create an error for an attack. This article is not centered to only individuals, but rather, it is applicable to every organizational information system that partakes the use of computer systems as part of their daily business function in order to create awareness to every user of the system to stay vigilant from the consistent threats, vulnerability and cyber-attacks. As mentioned, this awareness practice will not be a nine-day wonder of implementation but a continuous practice to solidify the trust of the organizational information system. The end users will also be abreast to feel more secured from "social engineering" of their personal information such as, identity theft, credit card fraud, password compromised etc.

Achievement: Aim

The primary achievement of this article end user security awareness campaign on their respective influence about security threats, vulnerabilities and cyber-attacks, against social engineering practices, is to ensure the CIA-Triad Confidentiality, Integrity and Availability in the field of information systems in the organizations, to protect data and information from the breach by any attacks.

Specific objectives

- Mitigate the consistent cyber attacks
- Protect sensitive information from breach
- Maintaining the integrity of the information

DOI: 10.21522/TIJAR.2014.04.02.Art020
ISSN: 2520-3088

- Securing the users of the system, which is at least as important as securing systems
- To establish a knowledge baseline for each user in the organizations
- Add the user's component to defend in depth etc.

Methodology: approach

The research, analytical literature and methodology examined, reviewed within the year 2017 authenticate the source of this consistent ransom attack are through the manipulation and exploitation of Server Message Block, (SMB) Port, under the Microsoft Windows Operating Systems environments which affected many organizational computers, around the globe. This occurrence has become rampant in the field of information security why because, in accordance with the analysis examined in the literature on the subject topic, most people in the organization are prone to the following errors when policies and adequate procedures are not regulated to be adhered on the below;

- E-mail attachment which contains malicious files
- Uncontrolled PC's, and Servers
- Week encryption, password management
- Unauthorized attached and unattended workstations
- Inefficient antivirus software's
- Unreported security threat, vulnerability and violations
- No updates, Patches and hot fix
- Poor perimeter protection that includes physical and electronic etc.

Online methodological surveys and theoretical analysis approach considered outlined that, fraudsters does acquire the required knowledge to invade into the system, through manipulation process and the way to entrust the safety aspect of this situation is to be very careful on what to click on their inbox when connected to the internet, applying the verification and authentication principles to be sure of first, not to download nor open untrusted software's and applications, checking for ambiguous messages and grammar that dictates for payment of jackpot or lottery wins etc.

Graph results: WannaCry – Ransomware Cyber-Attack

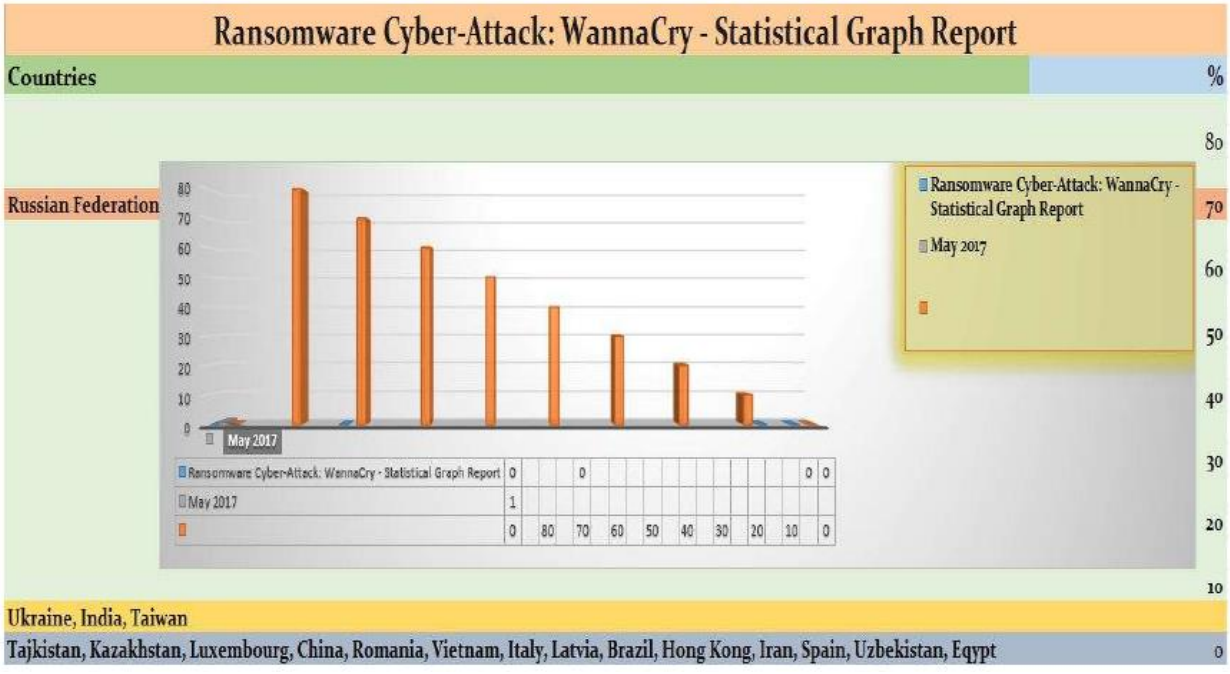

Figure: 1.1. WannaCry – statistical graph

Graph Results: Petya – Ransomware Cyber-Attack

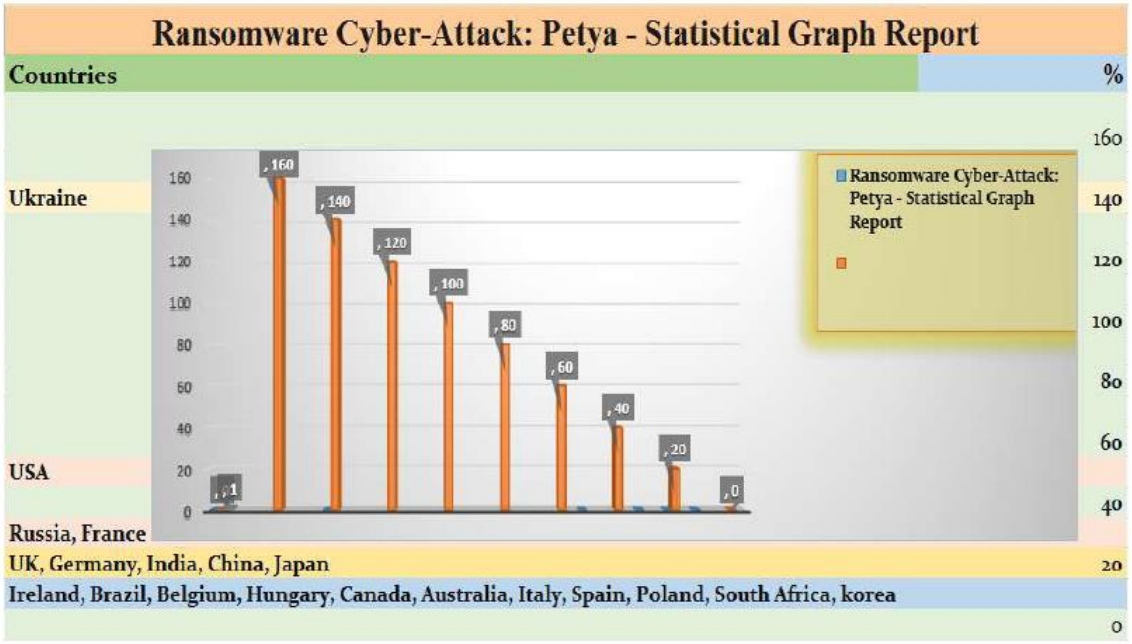

Figure: 1.2. Petya – statistical graph

Results: Petya

Why do people practice hacktivism?

Hacktivism; is considered as having someone practicing hacking, or invading into a computer system, for a personal or socially intent which is not a legal practice. Such people who do performs the act of hacktivism is said to be a hacktivist. Hackers are always hungry, developing a technique to intercept people information for their own intent shown in the figure below

An overview of a hacker

Figure: 1.3. An overview of hacking partitioning

DOI: 10.21522/TIJAR.2014.04.02.Art020
ISSN: 2520-3088

Discussion

The issue of at hand poses serious security challenge us and thus need has come to the realization of security awareness in all fields we must therefore endeavor to heighten its impacts. As we know of that, in every information system, users are liable to share with confidential information to any social engineering practitioner, depending on the level of intelligent in the field of information system security for that manner.

It is a very good practice to every organizational information system to achieve the CIA-Triad in the organization which is not limited why because, users of the system factor most and they can be manipulated through the social engineering process by any attacker, if the below steps is examined to ascertain the vulnerabilities of the system;

- Quid pro quo
- Phishing
- Baiting
- Pretexting
- Tailgating

On the subject, these are some of the major social engineering practice that a hacker can formulate on one or beyond, to invade into the computer system on the network, when discovered the vulnerability and weakness to a certain adaptable level of risk. There are many questions that arises, why in spite of the many security checks and implementations of high-end devices and software's to forestall the breach of system's security; yet they are still vulnerable to attacks. Hypothetically, this should be the ideal solution, but in the midst of information security, ensuring the safety of information has to be a day-to-day practice and process.

Conclusion

With the consistent ransom cyber-attacks and its panacea, noted in this paper will not guarantee the hundred percent of assurance in the information security of the organizations, but rather, it will ensure the maximum protection of data and information from breach, that can be controlled and mitigate to the minimal, if "ONLY" the end user awareness campaign is adhered to as a routine experience, controlled, monitored and become a subject of the company learning and development safety and security policy.

Figures/ Image/Table

Ransomware cyber-attack – WannaCry.

Figure 2.0. WannaCry – attack display overview

Ransomware cyber-attack – Petya.

Figure 2.1. Petya – attack display overview

References

[1].Adam L. Young, M. Y. (27 June 2017.). The Birth, Neglect, and Explosion of Ransomware. Communications of the ACM, Vol. 60 No. 7, Pages 24-26.
[2].Anderson, J. M. (2003). Why we need a new definition of information security: Computers & Security. ISBN.
[3].B., M. E. (2001). Information security is information risk management. ACM.
[4].Evans, M. (2 July 2017.). Business News: Hospital Is Forced To Scrap Computers. The Wall Street Journal.
[5].Henley, J., & Solon, O. (27 June 2017). Petya ransomware attack strikes companies across Europe and US. The Guardian.
[6].Jannsen, C. (9 October 2014). "Security Architecture". Janalta Interactive Inc.
[7].Kiountouzis, E., & Kokolakis, S. (n.d.). Information systems security facing the information society of the 21st century. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4.
[8].Perrin, C. (31 May 2012.). "The CIA Triad". ISDN.
[9].Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company.
[10]. Schofield, J. (28 March 2016). How can I remove a ransomware infection. The Guardian.
[11]. Uchill, J. (28 June 2017). Overnight Cybersecurity: New questions about 'ransomware' attack – Tensions between NSA chief, Trump over Russia – Senate panel asks states to publicize election hacks. The hill.
[12]. Young, A. (2006). Cryptoviral Extortion Using Microsoft's Crypto API. International Journal of Information Security. Springer-Verlag.
[13]. Young, A. M. (1996). Threats and Countermeasures. ISBN.
[14]. https://en.wikipedia.org/wiki/Information_security.
[15]. https://en.wikipedia.org/wiki/Computer_security.
[16]. https://en.wikipedia.org/wiki/Network_security.
[17]. https://en.wikipedia.org/wiki/Ransomware.
[18]. https://en.wikipedia.org/wiki/Social_engineering_ (security).