Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 124 (2017) 656–663

Procedia Computer Science

www.elsevier.com/locate/procedia

4th Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia

Security Strategies for Hindering Watering Hole Cyber Crime Attack

Khairun Ashikin Ismail, Manmeet Mahinderjit Singh*, Norlia Mustaffa, Pantea Keikhosrokiani, Zakiah Zulkefli

School of Computer Science, Universiti Sains Malaysia,11800 Penang, Malaysia

Abstract

The significant increase of Advanced Persistent Threat (APT) attacks, especially via watering hole leads to a huge loss to the company as they enable Bring Your Own Devices (BYOD) in the workplace. Higher education institutions also faced the same threat since BYOD has been adopted into their institution. In this paper, a simulation on watering hole attack and spear phishing; comparison between these two APT variants, as well as the survey design based on the Protection Motivation Theory (PMT) are presented. The result of the survey is analyzed using PLS-SEM. The result demonstrated that severity factor and vulnerability factor moderately explained the Protection Behaviour factor; and Protection Behaviour factor is a moderately strong predictor to self-efficacy, but avoidance behavior does not predict self-efficacy directly. Based on this result, a set of security policy for hindering watering hole and spear phishing attack is designed and implemented. The new policy will then be adapted to the university e-learning portal.

Peer-review under responsibility of the scientific committee of the 4th Information Systems International Conference 2017.

Keywords: Bring Your Own Devices (BYOD); Advanced Persistent Threat (APT); Watering Hole; Cyber Crime; Smartphone

1. Introduction

Bring Your Own Device (BYOD) policy at the educational institution have allowed the students and staffs to use their own device to access the institution's network and perform various tasks through the network and e-learning portal thus resulting in usage of personal devices in education environment by the university students. According to the 2014 Educare report [1] on the usage of mobile devices in educational institution from various countries, laptops and smartphones is a must have device among the undergraduate students, where 90% of them owns a laptop and 86% owns a smartphone.

While the policy, ensuring the high reachability and availability to various kinds of knowledge, it may also

* Corresponding author. Tel.: +604-6535346.
E-mail address: manmeet@usm.my

1877-0509
Peer-review under responsibility of the scientific committee of the 4th Information Systems International Conference 2017
10.1016/j.procs.2017.12.202

increase the chance of having cyber-attacks on the institutional network. One of the cyber-attacks is the Advanced Persistent Threat (APT) in which combines both social engineering and information gathering in order to have a high success rate. The APT attacks are most likely to target the organization that employs BYOD due to lack of user's awareness and and their knowledge of an APT variant and adverse effect of the attack on higher education institution are still on minimal point [2,3]. As a result, it is hard for security experts to propose an avoidance technique in order to prevent the attacks. As this research focused more on the fear factor or known as the threat appraisal, Protection Motivation Theory(PMT) is used. Previously, same method has been used by [4, 5, 6] which tested on the effects of PMT factors to comply the security policy and the protection behaviour across context. Hence, in this research, PMT will also be used as a theory to analyze the behaviour of the users.

This research aimed to simulate the watering hole attack for demonstrating the watering hole attack in BYOD Higher Education and comparing watering hole attack with spear phishing. Next, this paper presents user-awareness exercise and retrieves feedbacks from users by adopting the outcome from the simulation and further determines watering hole avoidance factors and analysis by using SEM tool. Lastly, this research also aimed to design a set of security policies for hindering watering hole attack in BYOD Higher education. Thus, this paper is structured as follows: Section 2 cover the related literature of BYOD in Higher Education, APT and PMT. Section 3 and 4 are the methodology and implementation section. Section 5 presents the survey conducted and results obtained. Section 6 will be on proposed security policy followed by conclusion as a final chapter.

2. Literature Review

In this era, lecturers and researchers have been encouraged to put all learning materials and sensitive data online to ensure ease of reachability and availability. However, cyber-attack such as APT attack may cause these assets to be compromised. Thus, in this section we will discuss about 1) how APT can occur in the BYOD, 2) how APT can occur in the educational institution by learning the user's behaviour on the device through the PMT. Next, the author will start the discussion with the usage of BYOD in higher education institution and its effects.

2.1 Byod Higher Education and it's Security Issues

BYOD is a management policy that enables the users to access the work-related resources and application through their own personal device(s) [5]. The device is allowed to access various kind of information including the sensitive one such checking email and students' grade, educational resource, research data and grants. However, as much as BYOD in higher education benefits the students, educators and management of the institution, there are also lots of security issues emerging along with the trends. Issues such as SQL injection, man-in-the-middle and reverse engineering that occur in desktop computer also can occur in BYOD. The smartphones and tablets architecture which operated on low processing power and memory space, aggravate the situation as the chances of having the cyber-attack in BYOD environment are much higher.

Besides that, malicious user behaviours due to lack of awareness such as downloading unauthorized applications and accessing sensitive data using unsecure network can lead further attacks to happen [3,7]. As a result, they might accidently download malware into their device, that later will gain full access to the victim's device and perform attack to the institution. According to report from Jupiter Networks [8], the amount of Android malware has increase to 400% since summer 2010. However, as compared to a laptop or desktop, APT attack on the devices will have a higher success rate because of the architecture. Besides that, lack of research related to APT attack in educational institution also worsen the situation. Therefore, in order to gain more information about how APT attack can happen and how to protect the educational institution, analyzing the behaviour when using the device would be able to help in addressing this issue. One of the ways is by using Protection Motivation Theory (PMT). Next, the paper will provide more details about PMT.

2.2 Protection Motivation Theory (PMT) in Determining the Avoidance Technique

PMT was proposed in 1975 and used Health Belief Model's emphasis on the cognitive processes mediating attitudinal and behavioural change to provide conceptual clarity to the understanding of fear appeals [12]. According