BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Artificial Intelligence Advances
https://ojs.bilpublishing.com/index.php/aia/index

ARTICLE

Ransomware Attack: Rescue-checklist Cyber Security Awareness Program

Mohammed Daffalla Elradi* **Mohamed Hashim Mohamed** **Mohammed Elradi Ali**

Communication Systems Engineering Department, University of Science and Technology, Khartoum, Sudan

ARTICLE INFO

Article history
Received: 28 April 2021
Accepted: 25 May 2021
Published Online: 5 June 2021

Keywords:
Cyber security
Awareness
Ransomware attack
Phishing email

ABSTRACT

Ransomware attacks have been spreading broadly in the last few years, where attackers deny users' access to their systems and encrypt their files until they pay a ransom, usually in Bitcoin. Of course, that is the worst thing that can happen; especially for organizations having sensitive information. In this paper we proposed a cyber security awareness program intended to provide end-users with a rescue checklist in case of being attacked with a ransomware as well as preventing the attack and ways to recover from it. The program aimed at providing cyber security knowledge to 15 employees in a Sudanese trading and investment company. According to their cyber behaviour before the program, the participants showed a low level cyber security awareness that with 72% they are likely of being attacked by a ransomware from a phishing email, which is well known for spreading ransomware attacks. The results revealed that the cyber security awareness program greatly diminished the probability of being attacked by a ransomware with an average of 28%. This study can be used as a real-life ransomware attack rescue plan.

1. Introduction

Cyber security awareness greatly depends on human-factor psychology, which is a scientific discipline that studies the interaction of people with machines and technology and hence guides the design of systems, products and technologies focusing on both performance and safety as well. Cyber security awareness is also subject to behavioural science and personality psychology, which plays a pivotal role in developing a robust defence strategy and critical defensive decision-making approach for cyber security professionals [1].

Having the adequate knowledge about the psychological traits of an attacker would be very helpful in mitigating the effect of a cyber attack and even formulating some preventive measures to prevent any future attacks. That's why it is crucial to integrate behavioural approaches with cyber security awareness to bridge up the gap [2].

Cyber attacks are rapidly evolving and therefore there must be a defensive attitude to cope up with such a challenging environment, as cyber attacks are conducted on almost a daily-basis. Crypto and ransomware attacks are examples of the most challenging cyber security threats that emerged and growing [3]. A ransomware attack simply denies access to your files and demands payment through Bitcoin, which provides anonymity and the transaction remains untraceable; for the attacker nothing can be better. Figure 1 below shows the ransomware attacks timeline.

**Corresponding Author:*
Mohammed Daffalla Elradi,
Communication Systems Engineering Department, University of Science and Technology, Khartoum, Sudan;
Email: mohd_daf_elradi@hotmail.com

 DOI: https://doi.org/10.30564/aia.v3i1.3162

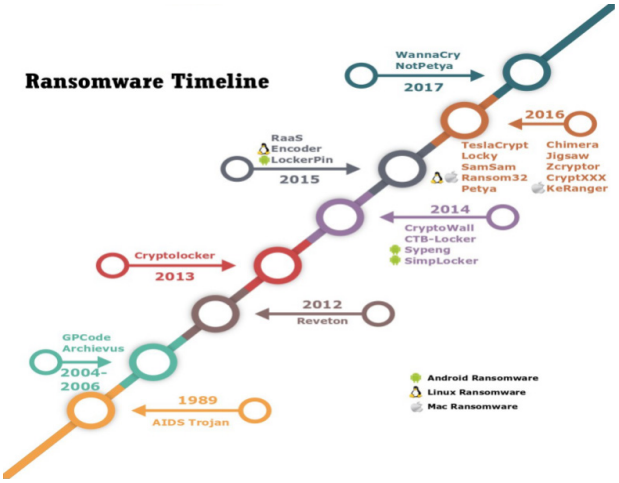

Figure 1. Ransomware attacks timeline

WannaCry as shown in Figure 2 below, the biggest ransomware attack in history used an exploit called EternalBlue, where more than 400,000 devices were globally infected [4]. Ransomware attacks are mostly launched via phishing emails, which are attempting to let victims install malware on their devices via malicious email; that alerts of a definite cyber security awareness weakness.

Figure 2. WannaCry Ransomware attack.

1.1 Ransomware Working Mechanism

As depicted in Figure 3 below, there are six main steps a ransomware attack follows to accomplish its goal which will be discussed briefly below.

1.1.1 Distribution

Ransomware typically uses normal methods of distribution as phishing emails or directing users to compromise websites that hosts a ransomware exploit.

1.1.2 Infection

Arriving on victim's device and starting processes needed to complete the attack. Here, highly escalated activities are performed which include:

- Installing a start-up program to ensure reboot survival.
- Stop major security tools such as Windows Defender, Windows Update services and error reporting tools.
- Compromising explorer.exe and svchost.exe.

1.1.3 Communication

Here the ransomware process will communicate with encryption-key servers in order to retrieve the public key needed for data encryption.

1.1.4 File Search

The ransomware starts to systematically search for files with their various extensions on the system.

1.1.5 Encryption

The core of the ransomware attack starts at this step, where the targeted files are typically moved and renamed, and then encrypted and renamed again.

1.1.6 Ransom Demand

This is the last step; the screen displayed is the ransomware attack and demanding payment via some steps. At this point the victim has no choice but to pay hoping for sending a decryption key or following some recovery strategies such as system image restoration.

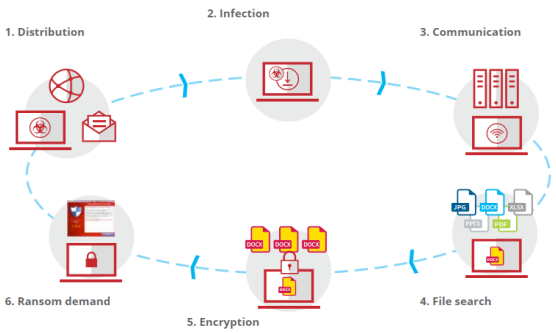

Figure 3. Ransomware working mechanism.

Not forgetting to mention that human beings are the weakest link in the chain of cyber security [5] and their behaviour can easily get compromised if they do not have the sufficient cyber security awareness.

The rest of this paper is organized as follows:

Section II discusses some related work to the levels of users' cyber security awareness and how that contributes to a safer work environment. The methodology followed in conducting the cyber security awareness program is highlighted in section III. Section IV and IIV preview

DOI: https://doi.org/10.30564/aia.v3i1.3162

the results and discussion correspondingly. Eventually, recommendations and conclusion are detailed in section V.

2. Literature Review

Many studies have been carried out in recent years to highlight how cyber security awareness makes a difference in reducing cyber attacks in organizations or even individually. Most of these studies have concluded that the human factor is the most vulnerable part of the process, which leads to catastrophic impacts as a result.

Businesses do not need to invest the security budget in a wrong area i.e. focusing on physical security and appliance, which are considered tangible and ignoring the security issues emerging from the intangible social engineering [6].

In [7], it was clearly stated that before pointing a finger at employees and blaming them for being the weakest link of the cyber security chain, there must have been various security limitations in the business itself which in fact had been reflected on employees and their level of cyber security awareness.

A major contributor to the issue of cyber security breaches is privileges. The more the employee's privileges, the more data that can be accessed, and the more damage that can potentially occur. Simply, the greater the employee has escalated privileges assigned the greater the risk they impose on the business which is likely to be targeted [8].

Internet Security Threat Report Volume 22 [9] concluded that educating the end-user and boosting their cyber security awareness is so crucial, as an uneducated user can cause tremendous damage to an organization. Spam campaigns are the top reason behind malware infestation and ransomwares [10], [14]. Hence, it is mandatory to make users aware of these attacks and other attacks ranging from physical to social engineering attacks, which will greatly be beneficial in mitigating the effects of cyber attacks or even prevent it.

3. Method

Designing a cyber security awareness program might appear to be an easy task, especially for cyber security professionals but in fact it is not. Cyber attacks and the attackers' mentalities are always evolving; as a result, the cyber security awareness program should be capable of covering and coping up with that evolving.

Advancement in technology and especially technologies associated with cyber security has made humans easier to target and exploit [11], as most organizations continue to invest in technical solutions but forget the importance of human factor which exposes them to risks that they are not prepared to face or even protect themselves or the systems they work with [12].

Having users who are fully aware of cyber security approaches will not only reduce cyber security incidents but can extensively increase the organization's aptitude to detect and respond to those security incidents [13].

The success of any proposed cyber security awareness program depends upon some approaches which will be discusses in brief below.

3.1 Identifying the Current Goal of the Program

It is the most essential step in almost any process, which involves analysis and knowing what you have and what you want. Here what the program is intended to achieve is clearly identified and also a metric for measuring the program's success. It is recommended to state the cyber security threats and their impact to let users assess the importance of complying with security regulations and policies by them.

3.2 Defining Success in terms of the Immediate Program Goal

After the program goal is identified, there must be a clear planned metric to measure the rate of success of the cyber security program, which provides a progress indicator and if some security policies have to be amended or adapted to certain emerging circumstances.

3.3 Evolving as the Program Grows

The designed cyber security program must be intended for long-term planning and should even consider the rapid cyber attacks emergence.

The cyber security awareness program targeted 15 users from a company specialized in trading and investment located in Khartoum, Sudan.The participants were surveyed using the survey questions in [15] but some questions had been modified to adapt to organizations' environment instead of educational institutions. This was essential to know where we are and where we want to be after the program.

The results of the cyber security awareness program intended to provide a ransomware attack rescue-checklist for end users will be discussed thoroughly in the next section.

4. Result

This section describes the proposed cyber security awareness program intended to provide a ransomware res-

 DOI: https://doi.org/10.30564/aia.v3i1.3162

cue-checklist and how to prevent such attacks in the future taking the approaches mentioned in the previous section into account.

The ransomware attack response checklist will be highlighted below, taking into consideration its simplicity, so any user with the least technical knowledge can follow it and rescue his files and system.

√ Step 1: Disconnect everything

a. Disconnect the device from the network.

b. Turn off any wireless functionality: Wi-Fi, Bluetooth or hotspot.

√ Step 2: Checking the scope of infection for signs of encryption

a. Shared folders from other computers.

b. Network storage devices.

c. Attached USB devices or external Hard Drives.

d. Cloud-based storage such as OneDrive, Google Drive or DropBox.

√ Step 3: Determine the type of ransomware

For example: Dharma, SamSam, WannaCry.

√ Step 4: Determine the appropriate response

As you have formed a scope about the damage as well as the type of ransomware you are dealing with, you can now be more resilient about the decisions to take in order to mitigate the effect of the attack.

The response can differ according to the severity of the attack and can follow miscellaneous scenarios as follows:

• Response 1

If data or credentials are stolen, the following is expected:

1. It should be determined if ransom will be paid in order to decrypt data or prevent attackers from revealing the data.

2. If ransom will be paid, you can skip steps number 1 and 3 of Response 2.

• Response 2

If you decided not to pay the ransom and recover your files from a backup instead, do the following:

1. Locate your backups, either from a system image or from cloud.

2. Try to remove the ransomware from the infected system.

3. Restore your files from the backup.

• Response 3

Trying to decrypt files, this needs a highly-technical individual

1. Try to find a decryption method. If succeeded, continue to the next steps.

2. Attach any storage media that contains encrypted files.

3. Decrypt files.

• Response 4

Trying to do nothing and lose files but keep the encrypted files for possible future decryption attempts.

• Response 5

Deciding to negotiate and/or pay the ransom by following the steps mentioned in the ransomware attack.

4.1 Preventing Ransomware Attacks in the Future

It is mandatory to have the adequate cyber security awareness to protect yourself from any cyber security attacks, especially ransomware attacks; which have been spreading recently. This is the goal behind this paper which will be covered in the following paragraph.

√ First line of defence: Software

1. Ensure you are using a firewall.

2. Use antispam and/or antiphishing software.

3. Make sure to use a reliable, up-to-date real-time blocking antivirus.

4. Enforce a policy that coerces anyone who logs in remotely must be via VPN.

5. Ensure that all operating systems are up-to-date and patched.

√ Second line of defence: Backups

1. Implement a backup solution, either hardware-based, software-based or both.

2. Ensure the data are safe, accessible and redundant once backed up.

3. Regularly test the recovery functionality of your backups.

√ Third line of defence: Preventing data theft

1. Use network analysis tools to detect any unusual traffic in the system and network.

2. Use least permissions to protect unauthorized access.

3. Use file or drive encryption tools to make it hard to tamper with your data.

DOI: https://doi.org/10.30564/aia.v3i1.3162

√ Fourth line of defence: Enrich your cyber security awareness

Stay away from suspected emails and links as possible, use an up-to-date security software and do not reveal much information when online.

5. Discussion

The ransomware attack rescue checklist in this paper was solely intended to simulate a real-life scenario of a ransomware attack, which is likely to occur especially as it is getting widespread and even evolving regularly. It was designed in a manner that keeps users aware of what they might confront i.e. identify the attack, forming an attitude to deal with it, mitigate its effect and optimally, avoiding the attack and preventing it in the future.

A ransomware attack had been simulated, before exposing the participants to the cyber security awareness program, the results were shocking. Only 13.33% of the participants had the basic security skills that made them to survive been attacked via phishing emails, which is the highest ranking ransomware infestation mechanism. As indicated in Figure 4, there was a probability of 72% being attacked with a ransomware and other cyber security attack, as the level of cyber security awareness was fairly low.

The proposed cyber security awareness program is likely to provide a semi-whole vision of ransomware attacks from various perspectives, which will keep the probability of being exploited with a ransomware attack at its minimal by an average of about 28%.

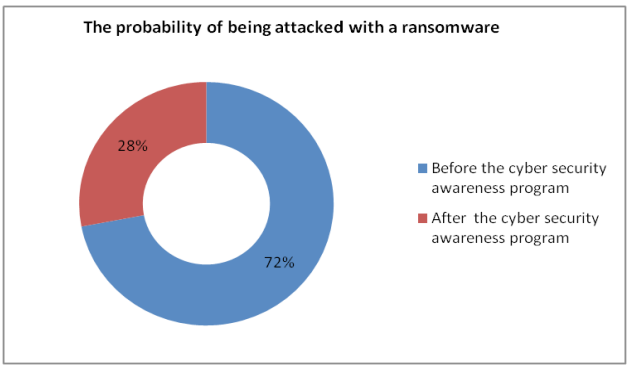

Figure 4. The probability of being attacked with a ransomware before and after the cyber security awareness program.

6. Conclusions

In this paper, a comprehensive ransomware attack rescue checklist cyber security awareness program was conducted, aiming to prevent ransomware attacks, which are immensely launched using phishing emails and spam campaigns; users are likely to fall victims for such attacks if they do not possess the adequate cyber security awareness that guides them on how to deal with such attacks, starting from prevention, identification, mitigating the effect or even recover from that attack.

The results of the proposed program were quite rewarding as the participants showed better performance by about 44% after completing the cyber security awareness program. This definitely counts a lot in real-life scenarios.

It is highly recommended for organizations to invest in educating users and boost their cyber security awareness as well as investing in technology measures to keep their business running in an era of continuous cyber war.

This paper can be considered as a preventive and rescue plan to avoid being attacked by a ransomware and looking forward to having further studies being conducted in this field.

References

[1] Adhikari, D. 2016. Exploring the differences between social and behavioral science. Behavioral Development Bulletin, 21(2), 128-135.

[2] Wayne Patterson, Cynthia E. Winston-Proctor - Behavioral Cybersecurity_ Applications of Personality Psychology and Computer Science (2019, Taylor & Francis_CRC).

[3] Cuthbertson A. (2017): "Ransomware attacks rise 250 percent in 2017, Hitting U.S. Hardest," Newsweek, September 28, 2017. www.newsweek.com/ransomware-attacks-rise-250-2017-us-wanna-cry-614034.

[4] C. Everett, "Ransomware: To pay or not to pay?", Comp. Fraud & Secur., vol. 2016, no. 4, pp. 8{12, 2016.
DOI: 10.1016/S1361-3723(16)30036-7.

[5] Young, H., van Vliet, T., van de Ven, J., Jol, S., Broekman, C.: Understanding human factors in cyber security as a dynamic system. In: International Conference on Applied Human Factors and Ergonomics, pp. 244-254. Springer, Cham (2018).

[6] Gavin Watson, Andrew Mason and Richard Ackroyd (Auth.) - Social Engineering Penetration Testing. Executing Social Engineering Pen Tests, Assessments and Defense (2014, Syngress).

[7] Connolly LY, Lang M, Gathegi J, et al. Organizational culture, procedural countermeasures and employee security behaviour: a qualitative study. Inf Comp Secur 2017;25:118-36.

[8] Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model

 DOI: https://doi.org/10.30564/aia.v3i1.3162

and human responses. Crime Science 2019;8:2-22.

[9] Internet Security Threat Report Volume 22 https://s1.q4cdn.com/585930769/files/doc_downloads/lifelock/ISTR22_Main-FINAL-APR24.pdf.

[10] C. Everett, \Ransomware: To pay or not to pay?", Comp. Fraud & Secur., vol. 2016, no. 4, pp. 8{12, 2016.
DOI: 10.1016/S1361-3723(16)30036-7.

[11] "What you need to know about the WannaCry ransomware", Symantec, Threat Intelligence, Oct. 2017, [Online]. Available: https://www.symantec.com/blogs/threat-intelligence/wannacryransomware-attack.

[12] Wisniewska, M., Wisniewski, Z.: The relationship between knowledge security and the propagation of innovation. Adv. Intell. Syst. Comput. 783, 176-184 (2019).

[13] Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science 2019;8:2-22.

[14] Brewer R. Ransomware attack: detection, prevention and cure. Network Secur 2016;2016:5-9.

[15] Mohammed Daffalla Elradi, Altigani Abd alraheem Altigani,Osman Idriss Abaker. Cyber Security Awareness among Students and Faculty Members in a Sudanese College. Electrical Science &Engineering,Volume 02, Issue 02, October 2020.

DOI: https://doi.org/10.30564/aia.v3i1.3162