International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217653

Increasing Awareness for Cyber Security in the Corporate Sector

Rishikesh Rao*
Masters in Computer Science, Somaiya University, Mumbai, Maharashtra, India

Article Info
Volume 7, Issue 6
Page Number : 171-177

Publication Issue :
November-December-2021

Article History
Accepted : 01 Dec 2021
Published : 07 Dec 2021

ABSTRACT

The age of computer advancement has caused a revolutionary change in the corporate sector. From on-campus working hours to remote work from home scenarios, from meetings in a conference room to meeting online in a virtual environment, things are changing continuously in the corporate environment. This paper tries to educate and generate awareness about cyber security in the non-technical human resource and try to make them understand the potential risks to their organization which can be caused because of not giving much attention to smaller details. This paper concentrates on those attacks which can be mitigated by any non-technical employee and which are easy to understand and give preventive measures for the same.

Keywords: Corporate, Cyber Security, Phishing, Insider Attacks, Weak Passwords, Cyber Security Awareness

I. INTRODUCTION

In this age of digitalization, the corporate sector has modified itself in a very big way. From moving an entire enterprise to a cloud platform to creating work- from-home opportunities for people, the corporate sector is drastically changing and is constantly shifting towards rapid digitalization. Due to this rapid shift, there is an ever-growing concern towards maintaining a secure digital space which will attract more people towards this change. The current scenario in the corporate field is that many are not aware of the risks of not having adequate cyber security and the loss which can happen if they have a system breach in their organization. Technical aspects of these cyber-attacks are known to professionals who have a career in the field of security, but the majority of the people working in the corporate field may or may not have sufficient knowledge on trying to prevent/mitigate risks which can allow criminals to bypass the organizational security boundaries and perform a crime. The human resource which works in the organization should be made aware of the attacks which are simple to execute but once executed will cause great damage to the organization. This paper aims to create awareness towards such types of attacks which have a big human factor in them and has some methods which will help them to mitigate such attacks to keep their organization safe from such attacks.

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

II. METHODS AND MATERIAL

As this paper focuses on security risks and attacks which have a simple plan of execution and has a more human-centric approach in their execution, we will be looking at some attacks which affect the corporate space more often and which can be mitigated at the employee level if the necessary precautions are taken at the right time.

A. Phishing:

Phishing is a very well-known security attack that has a very human-centric approach. It is a sub-category of social engineering attacks. Social engineering attacks are security attacks that are more human-centric and which try to entrap the victim by giving false promises or by intimidation.

Phishing is a security attack where the suspect/hacker will try to try to act as a sender of a legitimate E-mail and will try to persuade the victim to do some tasks which will benefit the suspect. Usually, phishing is done to gain entry into an organization via a weak human link by making the end-user(victim) share their user credentials with the suspected attackers. Some of the reasons why an employee of an organization falls into the trap of a phishing email are:

1. the email appears to be sent from a legitimate source.
2. the email which has been received by the employee contains a link which when clicked takes the employee to a site that asks for the employee's login credentials and guarantees the employee that if the employee does enter his credentials, they will get an appraisal or some sort of benefit from the organization.
3. the email demands the recipient to take some urgent action, disobeying the mail would result in some penalty.

The above reasons may be too realistic and genuine, but they may be a setup for a possible cyber-attack on the whole organization. To minimize these risks, employees of a particular organization should be made aware to look for these things in an email:

1. Are there words that imply a sense of urgency in the email?
2. Is the email address from where the email has been sent valid?
3. Does the received mail contain any links to some websites which belong to some organization?

In case a suspicious email has been reported for phishing, the technical/security team should look for these signs in a phishing email:

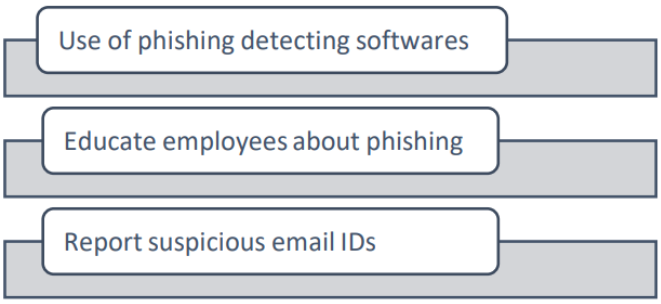

Fig 1.1 Preventive measures against phishing attacks

consideration. A password is used as a means of authentication and is considered as one of the most important areas in information/cyber security [2]. It is a method to validate authentic users. Passwords are used in various authentication processes like log-on or any organization gives a default user id and password to its employees from which they can use the organizational resources.

The main issue is on how to create a password that is a strong password and how to keep it in our memory. Organizations should follow the password guidelines which are provided by NIST. A weak password is a password that has only alphabets, alphabets that are recurring in the password, the password is related to the user, for example, his name, date of birth, etc.

Whereas a strong password may be completely unrelated for the user, will be containing more than 15-20 alphanumeric characters, it would not store in written or on the internet. [3]

Human memory plays a major part in the creation of a password. Everybody wants to create a password that can be easily remembered but also wants it to be strong and secure. These things don't go hand in hand. Due to this, most people create passwords in such a way that they will remember them for a longer period. For that purpose, people create short passwords which are related to them and if they don't change their passwords from time to time, they fall victim to a cyber-attack.

The cyber-criminal takes advantage of this laziness/carelessness and tries to get access to an organization through the weak link of a weak password. A weak password of a trainee employee can put the entire organization at the risk of an attack. If an attacker gets access to the organizational network, he can damage the organization in as many ways as possible.

Important things to be remembered by an organization while creating passwords:

1. Remind employees to change their passwords periodically.
2. While creating a password use NIST guidelines for secure password creation.
3. Use strength meters to guide employees on the strength of their passwords.

Fig 1.2 Important measures regarding password security.

1) Case Study:

An organization named BMX Pvt Ltd. is an organization that deals with logistics and other related services. BMX Pvt Ltd. has a very weak password policy for its employees. Bob is recruited in this company as an Operations Executive and is given a set of user IDs and passwords. Bob is a very lethargic and careless man. Bob does not change the default password which is given to him by the company and neither does the company remind him to change his password. One day, while on his usual workday, he feels that something is weird with his system because his workstation blacks out every half hour. On the next day, Bob is surprised to find that all his confidential files were missing. He reports it to the technical team and the technical team starts its inspection. The team infers that the entire organizational network has been compromised and a ransom has been demanded from the company otherwise all the trade secrets of the company may get published in the public space. The cyber cell puts the company's infrastructure understudy and puts a hefty fine on the company for not following standardized regulations.

C. Insider Attacks:

Many security attacks are carried unintentionally and without the knowledge of the end-user and have no malicious intent, but some of the attacks like insider attacks are carried with an intention and a direct purpose to compromise the security of an organization. Insider threat is an umbrella term that is used for classifying many attacks which are done intentionally by any employee who is working in an organization. Some of the attacks which come under the term 'Insider attacks' are sabotage, data theft, fraud, workplace violence, etc. These terms are usually used for stealing and conning people to gain some vital information or to damage the reputation of a particular organization. [4]

There may be many reasons which may be causing an employee to commit such a crime. Many may be motivated with money, a better position in other

organizations, revenge, and many other motives as well. The main difficulty does not lie on the technical side, it lies in the human resource selection process and in the attitude the company/organization has towards its employees.

There are many aspects that an organization has to take care of while considering insider threats. The main area of concern is human behavior and the organization's depth of knowledge regarding the mental health of its employees. It is observed that a person with good mental health is less likely to commit crimes. The organization has to keep tabs on their employee's physical as well as mental health in a periodic fashion. An organization can keep tabs on its employees by the means of polls, surveys, seminars, etc. Employees can also be asked to submit their concerns regarding some suspicious employees if required.

1) Behavior Analysis:

Behaviour Analysis is a very important aspect that should be done in any organization to get insights into the behaviour of its employees. There are many systems built to analyse the behaviour of people such as Fault Tree Analysis and Finite-State Verification. These systems use a vote-based approach to identify possibilities of insider sabotage and are also used to get mitigation suggestions for the same. [5] Another aspect of behaviour analysis is the appointment of a corporate counsellor who can solve the problems faced by the employees in the organization. It is to be highlighted and emphasized to the employees the results of their intentional and unintentional actions and the potential damage they may cause to the organization.

Apart from behaviour analysis, organizations should arrange events and seminars which will emphasize the importance and impact of professional behaviour on the growth of an employee in the organization. An insider attack can be also motivated by the competition in the market. So, organizations are advised to keep a check on the level of information which is passed on to various levels in the organizational hierarchy.

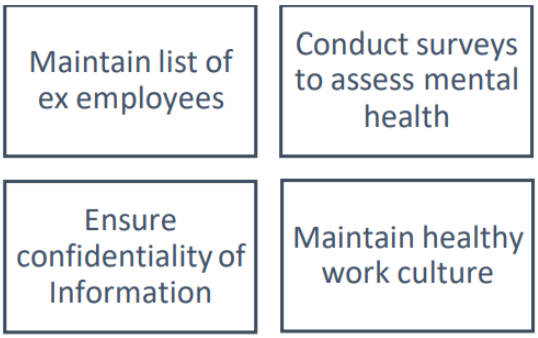

Fig 1.3 Tips to mitigate insider attacks.

Although the above points are important and compulsory to follow, there can be many other reasons for anybody to initiate an insider attack on an organization since the threat actors are the human mind and the human factor is extremely large in these types of attacks. However, employees can try to maintain professional behaviour and should try not to indulge in sharing information outside the organizational boundaries.

2) Case Study:

Mr. A was recently hired by an organization for a Technical Officer Role. He worked in that organization for 3 years and was removed from that organization on the allegation of committing fraud with a client in the name of the organization. After a couple of years, Mr. A was approached by another organization that offered him the same job profile which was offered to him by his previous organization. But he was asked to share some confidential details which were related to his previous organization and he was manipulated by saying that it is time to take revenge for the insults which were levelled on him by his previous company. Mr. A agreed and shared the details which helped his current organization to some extent. One day, Mr. A came to know that a recruit was hired by his previous company and was given the same credentials which were given to him. So, he used those credentials to steal some private data of the company. The company

got to know about what has happened and launched a complaint against Mr. A.

From this, we come to learn about many things that organizations should consider. Organizations should always have a proper and regularly updated list of the people on their campus and must always give new credentials to new employees. Organizations should also do background checks on the human resource which they hire.

III. RESULTS AND DISCUSSION

After exploring some of the important attacks which can affect any corporate venture, there is a major point of concern in the area of spreading awareness about these attacks and methods to mitigate the damage caused by these cyber-attacks. Awareness has been spread through various means such as government notices, declaring a whole month as 'Cyber Awareness Month', and so on. But these methods often don't have a major impact on spreading awareness in the general public as well as in the corporate sector.

There may be various reasons for the failure in delivering awareness for cyber-attacks, one of the major reasons being the lack of sufficient information about the same. It may also be the environment of the country or the country's digital culture which may be a hindrance in spreading awareness. The above-mentioned factors are the 2 major factors by which we can determine whether the awareness campaigns launched in various places across the globe may be effective or not. [6] If we take the case of India, India is just in its growing stages in the area of a strong digital culture that is aware of what cyber security is or what can happen if someone breaches a computer system. The general public is not that aware of what is the potential of a computer in terms of attacking as well as defending when it comes to a cyber-attack. The primary reason is the lack of knowledge of the sector of security.

Another problem that is faced by any awareness campaign is which delivery method should be chosen so that laymen could understand the technical message simply and easily. Many delivery models such as game-based, instructor-led, video audio-based, simulation-based, etc. [7] can be used to spread awareness amongst the masses. But these methods will only be useful if the digital culture of the region is known. A better way of spreading awareness for anything in the general masses would be the introduction of the topics in their education.

A proper solution to at least lessen the risks of getting attacked by a cyber-criminal would be the inclusion of cyber security in the training phase of any employee to make sure that they are ready and aware. Through this paper, we want to propose a training method which can help in creating the needful awareness in the employees.

This method can be called CST (Corporate Security Training). By this method, organizations can efficiently train their employees. There are 3 main parts in this method which every organization should remember:

1. This method is a continuous process.
2. This method works on the principle of zero trust which presumes that the trainees/employees have no prior information.
3. This method should not be discontinued even after the training of the employees is completed.

For this method, the organization should create a team of 4-5 professionals who are experts in the domain of cybersecurity. These professionals should select the type of attacks that are most likely to be done on their organization. (Like a top-five or a top ten list). Then they should create a curriculum for the organization which focuses on mitigating the chosen attacks.

The curriculum should follow these three principles:

1) Inform: The team should continuously inform the employees on the recent trends and latest news related to the chosen attacks and arrange seminars and meetings to address mitigation techniques and

risk reduction methods to the trainees/employees. The team should also conduct surveys to understand the knowledge level of the trainees/employees and should incorporate these findings into the revised curriculum after every audit.

2) Test: This is the main part of CST. This phase tests the level of understanding a trainee/employee has gained after attending any informative session. But the team has to remember that tests should not be taken immediately after a conducted session. Tests should be taken in the form of Multiple-Choice Questions (MCQ) or the form of a survey. The surveys should contain questions that should put the trainee/employee in a real-time situation. If the team wants to take a real-time test, then they are free to do so. But they should ensure that the real-time test should be a simulation and ensure that any real cyber- attack is not taking place at that instance of time.

3) Audit: This is the last phase of CST. In this phase, the coaching team should audit the performance of the trainees/employees and should compare the test results with their previous results to understand how much the employee/trainee has learned from the test/inform phase. These insights should be taken into consideration along with employee/trainee suggestions and feedbacks to improve the teaching as well as the learning experience of the team and the trainee/employee.

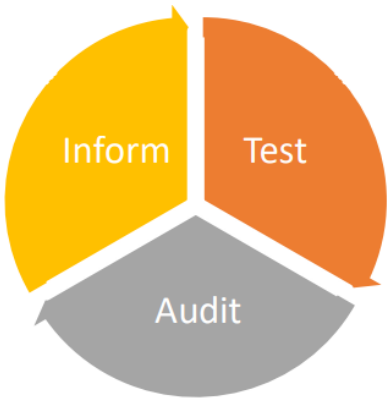

Fig 1.4 Phases of Corporate Security Training

IV. CONCLUSION

In this paper, we have tried to highlight some security risks which have a big human factor by specifying their attack methods, some case studies, and prevention/mitigation methods as well. We also tried to highlight the importance of spreading awareness regarding information security and have discussed reasons why security awareness campaigns tend to fail and explained things that can be done to make awareness campaigns a successful venture.

The above method can be used by both organizations as well as security training facilities to train their employees or clients. As mentioned before this method is a continuous process, so it will work best if an organization creates a team of security consultants and experts to carry out this method. The organizations which give cyber security training to corporates are contract bound and therefore will execute this method till the time which is mentioned in their contract. This will not help the organization which is undergoing training under the proposed method to gain full benefits of this method.

As advancements in the digital sector increase, more vigilance and importance are given to increasing and maintaining digital security. Since advancements in the digital space had led to innovations and advancements in the corporate sector, it has become the need of the hour to educate professionals on the need to maintain proper security ethics in their respective fields. The specialty of cyber-crime is that it is not bound by geographical boundaries and it can be done in a fraction of seconds as well. It is very difficult to catch a cyber-criminal since it is easy to delete digital activity.

V. REFERENCES

[1]. R. M. Schuetzler, “Trends in Phishing Attacks: Suggestions for Future Research,” p. 10, 2011.

[2]. M. Yıldırım and I. Mackie, “Encouraging users to improve password security and memorability,” Int. J. Inf. Secur., vol. 18, Dec. 2019, doi: 10.1007/s10207-019- 00429-y.

[3]. D. Charoen and D. Charoen, “Password Security.”

[4]. F. L. Greitzer, “Insider Threats: It’s the HUMAN, Stupid!,” in Proceedings of the Northwest Cybersecurity Symposium, Richland WA USA, Apr. 2019, pp. 1–8. doi: 10.1145/3332448.3332458.

[5]. M. Bishop et al., “Insider Threat Identification by Process Analysis,” in 2014 IEEE Security and Privacy Workshops, San Jose, CA, May 2014, pp. 251–264. doi: 10.1109/SPW.2014.40.

[6]. M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber Security Awareness Campaigns: Why do they fail to change behavior?,” p. 11.

[7]. J. Abawajy, “User preference of cyber security awareness delivery methods,” Behav. Inf. Technol., vol. 33, no. 3, pp. 237–248, Mar. 2014, doi: 10.1080/0144929X.2012.708787.

Cite this article as :

Rishikesh Rao, "Increasing Awareness for Cyber Security in the Corporate Sector", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 171-177, November-December 2021. Available at doi : https://doi.org/10.32628/CSEIT217653
Journal URL : https://ijsrcseit.com/CSEIT217653