[Title Here, up to 12 Words, on One to Two Lines]

Name

[Institutional Affiliation(s)]

Advanced Social Engineering

Introduction

Social engineering refers to an art of manipulating people to gain access to their personal and confidential information. The type of information that such criminals seek from a person varies with the need of the information. However, the cyber criminals usually trick potential victims into giving them their passwords, bank information, or gain access to personal computers among other activities (Krombholz, Hobel, Huber, & Weippl, 2015). This paper will, therefore, focus on the issues that are related to social engineering and suggest possible solutions to the current trend of cybercrime.

How the Intruder Gained Access to the System of the Company

There are various ways through which an intruder could have gained access to the information of the company. However, since the attack was through the electronic mail from the criminal. The possible way that the criminal could have used is to develop a password of the email of one of the company's supervisors' through the use of social engineering. Most of the Internet log-in portals require the password that contains approximately eight characters or more. It is not possible to cram all the passwords thanks to various portals that require an online login. Therefore, the supervisor might have been using a similar password to most of his or her portals. The portals include social sites like Facebook, Skype, and Twitter among others.

The intruder could have sent a message to the supervisor through the social media platform. It was in that message that the intruder embedded a link, and since it is from a social media friend, the supervisor just opened the message. Such links usually contain malware that enables cyber criminals to take control of other person's personal computer. All personal information of the supervisor's account to the intruder including the password is then sent to the intruder via the link.

With most of the personal information at hand, the intruder can, therefore, try as many accounts of the supervisor as possible. The intruder then designed a message and posed as the company's customer trying to explain that one of the company's product has been being incorrect. The message required the supervisor to verify the information by clicking ‘reply' button. The supervisor then tried to reply to the mail through the same link. The message that followed was that "No such e-mail address exists." Afterward, the computer speed worsened off and was extremely slow, and it seemed as if someone had gained access to the computer and accessed various confidential pieces of information.

That was the fact; somebody elsewhere had already gained password and other access privileges and obtained various company’s confidential information. Therefore, the information was hacked into as discussed above.

Security Recommendations

To avoid such mistakes in the future organizations and companies should be careful and develop certain protective measures that ensure they do not become an easy prey for the cyber criminals. To avoid becoming a victim, the employees, and the organizations should use all or a combination of the following suggestions.

Slow Action

Cyber criminals usually expect their targets to act extremely fast and think later after falling into their trap. If the supervisor could have waited a little bit longer for similar complaints from other customers the activity could have failed (Tankard, 2011). Therefore, there is a need of being patience when analyzing emails and deciding whether to reply them according to the terms of the sender.

Research the Facts

If the message has some information that can be verified through any means other than that of the sender, then employees and organizations should adopt such method. Suppose the supervisor was curious enough and checked the company's website about the purported faulty about the product. Since there was no problem to be corrected enough research about the reported problem could have helped in avoiding such loss of information (Krombholz et al., 2015). Therefore, companies should invest in research when dealing with issues involving urgency.

Deleting Request for Personal Information

Personal information is composed of passwords and financial information among others. Such messages are usually scams and have some links that will give control of your device to the potential cyber-criminal (Barrett, 2003). It is through the social media that most of the intruders get access to the passwords that they can use to access various portals online. Therefore, employees should avoid accepting any friend requests from strangers. Other recommendations that employees can use are through rejecting requests of financial help or simply ignoring and keeping personal as safe as possible (Tankard, 2011).

How to Test for Vulnerability in an Organization (Mock-up)

Software vulnerability can be seen as a weakness or a loophole in the system that can be taken advantage of by malicious attacker to prevent normal operation of the system or to steal some important information. Certain ways of detecting vulnerabilities have been suggested and therefore, can be applied by the manager to test for vulnerabilities to find lasting solutions. The manager can acquire the services of a white hacker to test for various vulnerabilities. White Hacker is a specialist employed by the company to test for the weaknesses of the information systems of the organization (Barrett, 2003).

The hacker can try to overwrite the data beyond the currently defined capacity. This vulnerability is usually known as buffer overflow. The manager will, therefore, be able to find certain loopholes that can lead to malfunctioning of the system. Suppose it was an intruder hacking, they may add corrupt data to the system leading to the whole data being corrupted.

The manager and the hacker can develop a malicious email with a link and send to one of the senior leaders of the organization. The malicious mail should enable the hacker to read through the information on the device when clicked by the device user. This type of access can be done through XSS or cross-site scripting. It involves an activity by the hacker developing an app that consists of injections of code in the pages that are accessed by the members of the organization (Tankard, 2011). The attacker will, therefore, bypass the access control and perform various malicious activities through the website.

Lastly, the manager together with the white hat hacker can develop an SQL injection that consists of injection code to exploit the content of the database of the company. This type of hacking usually occurs when the database of the company is not properly handled leading to intruders gaining hands on sensitive information and using them for any reason they were looking them for (Krombholz et al., 2015). However, in this case, it is the manager of the organization who gains access to the information.

Legal Conditions of Access to the Organizational Data

However, for an ethical hacker or white hacker, and the manager activities to be considered legal, they must first deal with the legal provisions in order to have an authorized access to the information. When handling a vulnerability check using the organizational data, there is a need to seek for permission or consent from the relevant body. Suppose that the company has contracted another organization to keep their data and limits anyone to the access, then the manager and the ethical hacker must seek the permission to avoid unnecessary liability that may arise. Various violations that usually limit the access to the data are the contractual obligations and confidentiality provisions. Most of the countries only allow access to the organizational data after a valid consent is issued to respective data authority. For example, when dealing with consumer data, the United States data laws permit the access only if the consumer's consent has been obtained.

Conclusion

Ethical hacking into the system of a company is legal since it helps in detecting the flaws in the system of the company. Therefore, it should be encouraged by various managers of different organizations since it may be helpful in detecting and correcting fraud in the system and help in preventing social engineering from hacking into the system.

References

Barrett, N. (2003). Penetration testing and social engineering: hacking the weakest link. *Information Security Technical Report*, *8*(4), 56-64.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network security*, *2011*(8), 16-19.