bb

by Bb Bb

Submission date: 05-Nov-2021 08:09PM (UTC-0500)
Submission ID: 1694438778
File name: CyberSec_FNL.docx (67.37K)
Word count: 1469
Character count: 7880

Cyber Security Company Report

By

Professor

Date

Social Engineering

An attacker either from within or outside may perform a social engineering attack and gain access through a student, teacher, or even admin account. As this security threat is always overlooked, it can easily tarnish the integrity of the product and cause loss of confidential data in the organization. As far as social engineering attacks are concerned, many organizations have faced irreversible challenges experiencing this. If this attack successfully takes place within the company's product, the users may not find the platform useful as they would experience downtimes and account inaccessibility.

Distributed denial-of-service attack

A distributed denial-of-service attack (DDoS) is one of the most dangerous attacks. This attack is of a high threat since the machines holding the product in the cloud can be compromised. The attack involves a flood of network requests to the server rendering it slow and inaccessible. This denies the services provided by the system to the company's users.

Baiting

This type of attack on social engineers depends on using and exploiting false promises to identify the target group. The most commonly used strategy is to arouse the curiosity or greed of potential victims and then steal the victims' personal information or remove malicious software from their system. Unprepared for the computer. An example is where the perpetrator cannot identify a particular company, inserting a flash disk into his parking lot, elevators, etc., where he is easily identified by labels that look legitimate as company payroll. The perpetrator who a legitimate disk has misled will then install it on his system and, in doing so, give the perpetrator access to or launch a malicious computer program. Entice the victim to click on them and lead them to malicious sites. Another example is when criminals use applications that, once downloaded, appear to be infected with malware.

People who take advantage of threats use social engineering methods to hide their true intentions and identity (Mihai, 2015 pp 61). Through these tricks, they present themselves as people the target can trust and use the opportunity to deceive, influence, or deceive them. Fraud, deception, or persuasion result in the people being deprived of access to the organization or information, which is a great privilege. In many cases, the perpetrators of social engineering attackers do not use force but instead rely on the good human condition and a willingness to help others. Although some attacks may take a straightforward step, a few categories are involved in the social engineering attack system. The most common types involved in the program include the investigation phase, where the perpetrator begins to gather background information about the target.

Scareware

This is a tactic used by social media attackers to make a target victim believe that they are facing specific threats (Arapinis *et al.;* 2012 pp 12). They sent several alarms to the target group, warning them of various false threats and telling them to take action. In such a case, the victims are deceived into believing that their system is suffering from malware infection, and therefore they should install specific software to deal with the threat. The software they install is a real threat to the perpetrator in their quest example of scareware. When you browse the internet, you see the ads that constantly appear and inform the browser that his system is infected and provides a solution to the challenge. Any options offered are intended to expose the system to malware by downloading an infected program or visiting a system that infects the system.

Pretexting

This is an attack strategy in which the perpetrator seeks to gain the trust of his victim and collects sensitive, confidential information. In this case, the attackers can obtain information

about the victim through cleverly fabricated lies. To establish trust, perpetrators may disguise themselves as police, coworkers, bank officials, a tax official, or any other organization that the victims know they have in common. The process involves the perpetrator asking the comprehensive victim questions that confirm their identity and gather essential personal information. This type of attack can collect a lot of information from personal addresses to victims, their social security numbers, phone details, bank records, and vacation days as employees and employees of the organization, and they can collect security information. In their various meat plants.

Phishing

Criminal data theft is one of the most common social engineering attacks often presented (Dorr *et al.;* 2020). This is an attack based on the use of text or email messages that seek to arouse fear, curiosity, or a sense of urgency in their victims. These messages also request the victims to identify sensitive information, download or open attachments that contain malware, or use the links provided to gain access to malicious sites. Criminal identity theft scams come in a variety of formats and target victims differently (Cantor *et al.,* 2005 pp 34). An example of this scam is when a person receives an email informing him that he has violated specific policies and asking him to do something immediately, such as changing his password. Since hackers abuse their victims' trust, they use legitimate websites and trick unsuspecting users into using the illegal site, write down their password details and change them. The information is passed on to fraudsters. Consolation to potential victims is that criminal identity theft campaigns use the same or closely related messages as their scams. Email servers are therefore in a position to identify and block these threats.

Spear phishing

The crime of stealing sensitive information is another form of attack on social engineers. This attack is similar to a criminal attack that steals sensitive information that is more targeted . In this attack, the perpetrators act very cautiously and direct certain businesses or individuals. To ensure that these messages can accomplish the job you imagine, tailor it to companies or individuals based on their characteristics, job positions, and contacts that make them invisible. To effectively catch the crime of identity theft, perpetrators must invest a lot of time and effort into it. The beauty of such attackers is that when they use their skills effectively and patiently, it is difficult to detect and achieve high levels of success. An example of a criminal attack on identity theft is when a perpetrator impersonates an organization specialist as an IT consultant. In that role model, they can contact one or more administrative staff via email. After conducting a thorough investigation, the perpetrator may successfully deceive the recipients of their identity by imitating the wrong person and believing that the message is authentic. From their IT adviser, targeted people will go ahead and change their passwords, gaining access to malicious sites through questionable links provided. As the target victims become victims, the perpetrator takes their pieces and exploit them for their benefit.

Security protocols to Integrate

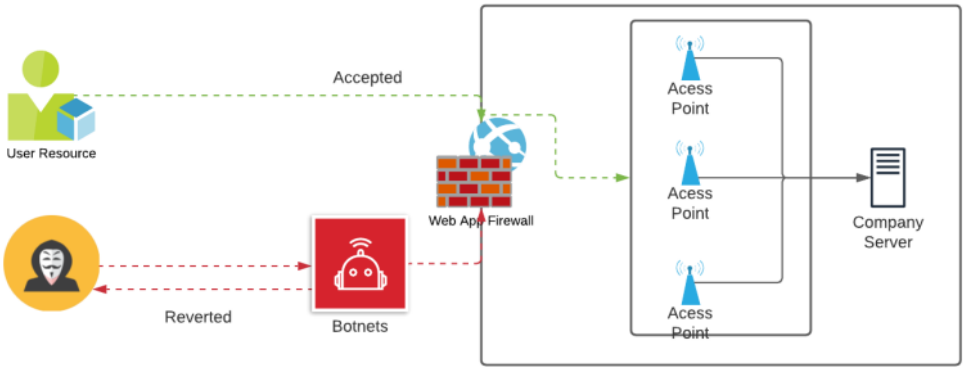
The users can be educated on the types of phishing attacks and how to differentiate clones of web pages (Grolimund *et al.;* 2006 pp 45). Apart from this, they should be encouraged to avoid opening and pressing links on enticing emails. Users should also be warned to avoid free software downloads. This will heavily assist the administrators in avoiding dealing with security threats of inaccessible accounts and ransomware attacks.

DDoS attacks can be hard to counteract and since they block all traffic from reaching the product. Instead of locating the attacker, the cyber security team should focus on bringing the

platform back to its healthy status. However, these attacks should be foreseen beforehand. This can be done through:

- Using technologies that provide a visual representation of the server holding the company's platform. As this may seem to have little effect, administrators who know the normal pattern of the server can detect whether there is a problem if the visual representation of the server changes abruptly.
- Have additional space for heavy CPU loads which will allow the requests from DDoS attacks to have a lesser severe effect.
- Check and regularly update the server to the latest network protocols and configurations.
- Setup steps that should be taken in event of an attack similar to DDoS. This will enable a more fluid way off dealing with the attack as it happens.

Attacker Model



References

Cantor, S., Moreh, J., Philpott, R. and Maler, E., 2005. Metadata for the OASIS security assertion markup language (SAML) V2. 0.

Mihai, G., 2015. Cloud ERP and cloud accounting software in Romania. *Economics and Applied Informatics*, *21*(1), pp.61-66.

Grolimund, D., Meisser, L., Schmid, S. and Wattenhofer, R., 2006, October. Cryptree: A folder tree structure for cryptographic file systems. In *2006 25th IEEE Symposium on Reliable Distributed Systems (SRDS'06)* (pp. 189-198). IEEE.

Arapinis, M., Bursuc, S. and Ryan, M., 2012, March. Privacy supporting cloud computing: Confichair, a case study. In *International Conference on Principles of Security and Trust* (pp. 89-108). Springer, Berlin, Heidelberg.

bb

ORIGINALITY REPORT

2%	1%	1%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Hemalatha S, Vasantha Gowri N, vani A, Sana Qaiyum, vijayakumar P, Sulaima Lebbe Abdul Haleem. "Protection From Distributed Denial of Service Attack Using Fuzzy Logic", Research Square, 2021 Publication	1%
2	topics.libra.titech.ac.jp Internet Source	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		