


CMPG 215

Information security attacks and threats

Antonet Zwane 41509056

INDEX

Table of Contents

Introduction to information security attacks and threats.....	2
What are information security attacks and threats.....	2....
Types and examples of information security attacks and threats.....	3....
Digital Agriculture.....	3
APT (Advanced Persistence Threat)	6
 Lazarus Attacks.....	6
.....	3
Phishing attacks.....	7
Lessons and possible solutions.....	8
Conclusion.....	8
REFERENCE LIST.....	9

Introduction

Technology is an application that is constantly growing and evolving every time of our lives, huge concerns about information security arise at the same rate as the evolution of technology. Information security is used to protect organizations and systems against unethical users of data and attackers. Although different security attacks and threats occur each time to oppose the growth of this application, the need for solutions should also arise at the same concern. The noticeable increase of these issues in recent years is causing a huge concern in the technology world, threats like the malicious software also known as malware, Advanced Persistent Threat (APT), the ransomware and the phishing attacks also the possible solutions are what will be discussed in this analysis.

Firstly, the difference between an information security attack and an information security threat is that an attack includes trying to remove, destroy, obtain or reveal information without authorized permission or access. A threat is taking advantage of the system's vulnerability to breach the information security and harm or alter it. The attackers usually study the system of an organization and look out for its weaknesses or weak spots to use it at their own advantage normally with specific motives, commonly in hopes of receiving remuneration from an organization or spying on competitors in a business setting. The weak spots or weaknesses in the system are called system vulnerability, which as mentioned can be used by cybercriminals to their advantage. When vulnerability in the system is detected a threat agent is often used to penetrate the system. Research indicates that 70% of security threats are conducted by employees or insiders of that organization in an instance where a threat is opposed in an organization.

Types of information security attackers

There are two types of information security attackers also known as information security source, the insiders and the outsiders. Usually, the attackers have what is called a threat agent, which refers to the environment, the technology and humans that can help them gain access to the system. Insiders refer to anyone and everyone who has remote or physical access to the system or organizational entity in business that can lead and open opportunities of information security risk or internal information security threat. Examples of the insiders are mostly employees because they are the ones who normally have access to the organization's

3

information, former employees who usually want to make the organization suffer, malicious insiders, partners, clients or people remarkably close to you. On the other hand, outsiders are cybercriminals who cause external threats. Examples of outsiders are hackers, either ethical or unethical, criminal groups and huge establishments, that simply want to gain unauthorized access to the user's system.

Malicious Software (Malware)

Malware shortened for malicious software is an intrusive software developed by cybercriminals commonly known as hackers, to penetrate or get into a system without permission from the user, usually designed with an intention to disrupt, steal, leak or obtain unauthorized access to confidential information of the user. Sensitive information like passwords, bank details, emails, the IT infrastructure, IT services and more are what cybercriminals are mostly seeking from the user. Malware gets into the system through different and unnoticeable ways. There are a few ways that cybercriminals use for malware to get into and penetrate the system of the user, things like pop up ads are used and are generated to make changes in the system settings once access is gained. Links, normally suspicious free links of websites or webpages are also a way that malware can gain access to a system. Thirdly emails are also an easy way that can be used to inject malware into the user system.

Once malware has successfully entered the device, it locks up the device and makes the device unusable so that the cybercriminal can be the only person that can have access to it. The malware can ultimately destroy the computer's system to damage network infrastructure, use the computer power to send spam emails, run botnets or crypto jacking or rather an auction on the dark web will be held for your intellectual property. Common examples of malware are viruses, worms and ransomware, in this case you have to pay to get access to the system back.

Recent attack of malware (Digital Agriculture)

In the year 2022 research in Australia was conducted regarding malware attack on digital agriculture as many cases were reported. Digital agriculture is the use of smart digital devices to

assess, monitor and manage environmental parameters that could easily affect food production. Digital agriculture varies, there can be one where there must be a technical model or machinery that can control the drone for spraying crops or for heating the system of a vertical farm, so it varies. Digital devices like drones, smartphones and sensors can be used to access valuable data about production without the need for human intervention. There are also several applications regarding digital agriculture, applications like automation, crop management and precision. As digital agricultural farming is introduced to farmers and is becoming more of a usage than before, information security attacks and threats also rise.

Reasons behind these attacks are that cybercriminals just want to temper with the production of the agricultural business and eliminate competition in cases where there are many farms and agricultural spaces that make use of commercial farming. The other thing is that farmers use low-cost security systems because they want to save but do not know that the system is prone to security attacks. Lastly for financial gain, especially if the agricultural space is making a lot of money or has a good business relationship with other businesses in terms of supplying. The use of intelligent machinery and smart irrigation are some of the things that can be maliciously attacked and exploited. Typically, cybercriminals will find a weak spot in the system, vulnerability like employees, software, technology or devices. So, the vulnerabilities in these can cause huge and disastrous effects in terms of supply, cost and labour.

When it comes to what has been studied is that digital agriculture stakeholders put less effort into the security of the technical devices and the focus is mainly on production, security must also be prioritized and adding security in the design phase of the system should be considered. New detection and prevention systems should be implemented to prevent attacks on the system. Some of the datasets in the systems are old and sometimes they are traditional home datasets so AI algorithms can come in handy to develop systems that can mitigate existing attacks in the dataset of the system. Frameworks should also be implemented to guide farmers and businesses about security at different levels of devices, like specific security for data, devices and applications used in production. Lastly the attacks and threats are inventible so it is advisable for the farmers or stakeholders to be prepared for any future incidents and must have all their security and detective devices in check or simply try to report the crime when it happens.

Advanced Persistence Threat (APT)

Advanced persistence threat or APT is a state sponsored group that gains unauthorized access to the system or network and establishes a long-term presence without being detected, in order to gain sensitive information. Normally the APT is used to target big establishments or governmental organizations. As APT is normally used to attack big entities, the cybercriminals there are ultimately a team of experts or experienced cybercriminals with more resources and a substantial financial backup. While some are funded by the state or government using cyber warfare weapons. APT are different because they are complex significantly so, once the targeted system is infiltrated the cybercriminal must remain in order to attain and access as much information as possible, launched against a big pool of targets, so they are manually executed, and they usually aim to attack and penetrate the whole system or network and not just one specific part of the system.

Common examples of APT are cross-site scripting, remote file inclusion, SQL injection and many more used to establish hold (foothold) in the targeted system.

Lazarus attacks (APT)

In 2021 Kaspersky which is a campaign to help detect and solve security crimes, came across a group called the Lazarus Group, which attacked industries, mostly the defense industry using APT and other malicious software. Mostly with the intention of stealing the industry's database and spreading the malware attack. The APT used often undergoes three stages after a successful attack on a system. The first stage is infiltration which compromises the web assets, network resources or authorized human users of that system. This infiltration is achieved either by phishing, social engineering attacks and malicious uploads by the targeted entity. A simultaneous execution of the DDoS attack against the targeted entity occurs, to distract system personnel and to weaken the security perimeter of the system, making it an easy advantage to breach. So, this requires the attackers to be quick because right after gaining access to the targeted system a backdoor shell must be installed for it to grant them access and run the operations of the system.

The second one is expansion, which after infiltration allows the cybercriminals to broaden their presence within the system. This often include compromising the staff of the entity because of the now illegal access to sensitive information and causing a movement in the entity's hierarchy, those above-mentioned reasons allow them to gather information like the financial records of the organization, data and more. So, the danger is that the accumulated information can be sold or exposed to the wrong people in public, like the competitors of the organization or simply delete the data. The third one is extraction, after successful expansion the information is stored in a very secure location inside the victim system, then finally the data can be extracted without being detected. Things like white noise tactics are what is normally used to cause distraction and distract the security team so that information can be successfully extracted from the victim system.

5

Phishing Attacks (Garmin)

In 2020, Garmin was a victim of a phishing attack, even though the attack was reported as an outage by the company, it later revealed that the company was a victim of this attack, and it forced their services to be offline. A huge disruption of customer support, website function and communication occurred. Luckily no trace of customer data was stolen but a ransom was paid of \$10 million to the attackers.

Phishing attacks are when cybercriminals convince or deceive people into revealing sensitive information. According to the FBI's Internet Crime Complaint Centre, as of 2020 more phishing attacks incidents have been reported more than any other computer crime. Phishing has become more advanced and mirrors the system to allow the user to navigate sites and implement security boundaries while the cybercriminal is observing everything. The term "Phishing" was first implemented in the 90s but it refers to the lures of fishing for sensitive information.

There are different types of phishing, there is spear phishing, email phishing, Whaling and CEO phishing, clone phishing, voice phishing, SMS phishing and many more, but the one that will be discussed is email phishing. Email phishing is often delivered through spam emails, attempts to trick people into revealing sensitive information and login credentials. Phishing is a bulk attack unlike APT where a specific victim is targeted, phishing is sent in bulk to a huge number of emails or people in hopes to get a victim, meaning targets or victims may vary, financial institutions may be targeted, streaming services, email and cloud productivity providers. So, the stolen information may be used to install malware, steal money or phish other targets within the victim system and in streaming services accounts may be stolen and sold to dark markets.

Lesson and Possible solutions

Information security crimes (threats and attacks) can cause a serious disruption in a business or the user system. In business commercial loss and reputation can be compromised, so attackers can expose your business to negligence claims or regulatory actions, loss of customers and clients/suppliers and inability to meet contractual obligations. Other things that are learnt is that the information security threats are not necessarily new, similar attacks happen to other victims and that organizations usually do not have knowledge about these attacks hence they are more vulnerable and prone to these cyber-attacks and threats. As much as these are problems in the technological space, possible solutions may be recommended. The first thing is

always to update or encrypt devices so that threats and attacks may be detected early. Backing up data also can serve as a solution to the situation, backing up data in more than device. Paying the ransom in case of ransomware does not guarantee return of files or data stolen so reporting the crime is what can be done. Registering your device to services like McAfee, NCSC and many cybercrimes detecting services can come in handy and prevent attacks. Investing in email specific security tools to protect yourself from unnecessary spam emails and avoid clicking on suspicious links from questionable sources.

Conclusion

Taking all the information into consideration, information security attacks and threats are a huge problem not only for organizations but for individual users also. Cybercriminals are mostly after money; data of the user and they study the system before attacking. There will be a growth in these attacks and threats at the same rate as technology is growing but how a user protects themselves from them is what is important. Also, with the growing knowledge of these attacks and threats people can easily expose and avoid being victims of cybercriminals. Also, not prioritizing security of your system is going to cause security problems for you. It is better to prevent this before happening than trying to fix it after it has happened.

REFERENCE LIST

Techopedia

www.techopedia.com/definition/6060/attack

Malwares - Malicious Software - GeeksforGeeks

<https://www.geeksforgeeks.org/malwares-malicious-software//>

Imperva

[Cyber Security Leader | Imperva, Inc.](#)

Datamation

<https://www.datamation.com/security/cyber-attack-prevention>

Jouini M et al. Computer Science 32: 2014.489 – 496.

<https://scholar.google.com>

Google Scholar

<https://doi.org/10.3390/s22093520>

[Google Scholar](#)

Kaspersky

[APT attacks on industrial companies in H2 2021 | Kaspersky ICS CERT](#)

Tech Target

[10 of the biggest cyber attacks of 2020 | TechTarget](#)