CA214 Term Paper

STATEMENT OF NON-PLAGIARISM

I hereby declare that all information in this assignment has been obtained and presented in accordance with academic rules and ethical conduct and the work I am submitting in this document, except where I have indicated, is my own work.

Student Number: 19359231

Student Name: Nicolas Oyeleye

Date:23/11/20

Signature:

Nicolas Oyeleye (Here I signed the document by writing my name)

Word Count : 1591

Title: Cyber Threat Analysis

ABSTRACT

With an increase in the number of cyber threats and cyberattacks happening online, it is essential that we find a method of ensuring that all our information and data are safely stored from outside entities. One such method is Cyber Threat Analysis. The purpose of this paper is to define Cyber Threat Analysis, examine the various threats imposed by Cyber Adversaries, and further dissect the different stages of the Cyber Threat Analysis process. This paper is divided into four main sections in which I will decipher between the points listed above.

Keywords:

Adversary, Threat Analysis, Threat Intelligence, Entity

Cyber Threat Analysis

Introduction

Cyber threat analysis is the method in which knowledge of internal and external information weaknesses of a particular organisation are tested against real-world cyberattacks. This method is threat-oriented and is used for combating cyberattacks, showing a change from reactive cyber security to proactive cyber security. In terms of cyber security, the desired result of cyber threat analysis is to deliver the most effective practises on how to maximise the protective instruments with respect to integrity, confidentiality, and availability, without omitting functionality conditions and usability. Furthermore, the result of cyber intelligence equips organisations with ameliorated practices, ensuring that their information and data are safely stored, denying access from outside entities[1]. Cyber threat intelligence is evidence-based knowledge, including implications and actionable advice, indicators, mechanisms and context, about an existing or emerging hazard or menace to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard. The benefits of cyber threat intelligence include enabling improved detection of threats and informing better judgement regarding decision-making during detection of cyber threats or intrusion. It also empowers organisations to establish a proactive cybersecurity strategy and to aid overall risk management policies.

1. Cyber Threats

Cyber threats should be taken seriously. Many people do not understand the implications of being victims of these threats. A lot more people do not even know how to identify these threats. Successful cyber-attacks can lead to malfunctioning of military equipment, electrical blackouts, and exposure of national security secrets.

A cyber threat is anything that can lead to meddling, interruption or destruction of any valuable service or item existing in an individual or organisation’s repository[2]. It is also defined as the possibility of any malicious attempt to damage or disrupt a computer system or network by accessing unauthorised files and information or stealing valuable data. Whether of “human” or “nonhuman” origin, the threat analysis must scrutinise and eliminate any element that may bring about conceivable security risk.

Threats can potentially lead to loss of revenue, diminished brand reputation, the destabilization of operations, and as mentioned previously, malfunctioning of military equipment, electrical blackouts and exposure of national security secrets. The decision of which one of these options occurring all depends on the intent and motivation of the adversary; the person committing the act.

Cyber threats have many forms. The most common threats include phishing, social engineering, and malware.

Phishing is a type of fraud in which deceitful emails are sent to the public to steal personal data which includes banking information, addresses and login credentials. These emails are disguised to seem to have been sent from reputable sources and are designed to appear legitimate.

Another type of cyber threat is social engineering. This form of threat consists of human interaction that results with a user being deceived into accessing guarded information through inadvertently breaking security procedures.

The Most common and malicious form of cyber threat is Malware. Malware is a piece of software or a program designed to damage a user’s computer or steal information. Examples of malware include trojan worms and horses, spyware, and computer viruses. Ransomware is a subset of malware, in which the adversary locks down the victim’s device through an encryption method, demanding a ransom to decrypt and unlock the victim’s device[3].

2. Cyber Adversaries

A Cyber Adversary is someone or a group of people that intend on performing malicious actions against other cyber resources and services[4]. When investigating threats, it is crucial for analysts to understand how the adversaries work and think. Although their approach and procedure may be similar, what motivates and drives them can be different. Understanding these motivations can provide us with a better perception of why an adversary may strike, when they may strike and what they may be aiming for. The most common adversaries that are pursued during an analysis are cyber terrorists, malicious insiders, hackers, cyber criminals, and hacktivists[5].

Cyber terrorists are the rarest of the five but one of the most ruthless. They are usually motivated by ideological, religious, or political causes. Their main objective is usually to intimidate a section of the public or even a government. They are also capable of interfering with critical infrastructure.

The second type of adversary are malicious insiders. A hint of what they are is given in the name, an insider. These insiders are people that have access to various files and databases in an organisation because of employment. These attacks are malicious in nature, as mentioned in the name and are typically perpetrated by greedy, troubled, or annoyed employees. This attack is targeted at the organisation and is motivated by grievance or just financial gain.

The next type of adversary is called hackers. They are thrill seekers because of their intent and motivation. These people are thrilled by their ability to gain access to secured systems and networks. They are always looking to prove themselves by tackling the hardest tasks. As well as these criminals, hackers can also be professionals. These hackers are referred to as “white hat” hackers, whereas the criminal hackers are referred to as “black hat” hackers. White hat hackers can help organisations ensure that their systems and networks are securely embedded, prohibiting outside entities, such as Black hat hackers, from gaining access.

The fourth type of adversary are called cybercriminals. The motivation of cybercriminals is purely financial gain and greed. The actions of cybercriminals include fraudulently applying for loans and credit cards, filing counterfeit tax returns, the transferral of money illegally and blackmail or extortion. Cybercriminals use people’s Personal Identifiable Information (PII) to acquire what they need. These PII include a person’s name, address, email or even phone number[6].

Finally, the last type of common adversary is called Cyber Hacktivists. Hacktivist’s attacks are targeted and are sometimes perpetrated to promote a social change or political agenda or raise awareness on an issue. These cyber-attacks are often motivated by individuals or groups of people trying to protest. According to an article by Stateline, hacktivism can be described as “digital disobedience”[7]. While some think of it as being a form of protest, it can and often is disruptive. Anonymous is a hacktivist group well known for their work in 2004[8].

3. Cyber Threat Analysis

The first stage of threat analysis is the scope. This involves identifying the assets an organisation wants to safeguard from attacks or that are essential to that organisation.

The second stage of threat analysis is the collection of data. In this stage information about actual cyber-attacks or threat incidents are gathered. Here, analysts separate real potential attacks from threats that are not real but can be considered a potential threat. The scope helps the analyst filter these threats to ensure that their attention and focus is on threats that exist.

The final stage of cyber threat analysis is Mitigation and Anticipation. In this last crucial stage, the analyst uses the data collected in the previous stage to establish the best and most efficient preventive measures to be implemented. The information gathered will be useful in anticipating future cyber threats and attacks[9].

4. Conclusion

In conclusion, cyber threat analysis is the process uncovering cyber threats and defending your systems and networks against them. There are various types of adversaries that we need to watch out for and many ways in which they can deceive people into getting the information they need. All organisations, businesses and individuals must identify what assets they would like to keep safe and then ensure they have the best possible means of keeping it safe.

Link to YouTube presentation video: https://youtu.be/PQe2IMHHiPc

References

[1] What Is Cyber Threat Analysis and its components? | EC-Council Blog. EC-Council Official Blog. (2020). Retrieved 25 November 2020, from https://blog.eccouncil.org/what-is-cyber-threat-analysis-and-its-components/#:~:text=Cyber%20threat%20analysis%20is%20the,reactive%20security%20to%20proactive%20security.

[2] Cyber Threat Analysis [Updated 2019] - Infosec Resources. Infosec Resources. (2020). Retrieved 25 November 2020, from https://resources.infosecinstitute.com/topic/cyber-threat-analysis/.

[3] What are Cyber Threats? Types of Cyber Threats and How To Prevent Cyber Attacks. TransUnion. (2020). Retrieved 25 November 2020, from https://www.iovation.com/topics/what-are-cyber-threats-types-of-cyber-threats-and-how-to-prevent-cyber-attacks.

[4] Cyber Adversary - an overview | ScienceDirect Topics. Sciencedirect.com. (2020). Retrieved 25 November 2020, from https://www.sciencedirect.com/topics/computer-science/cyber-adversary.

[5] Metivier, B. (2020). *Threat Hunting: Six Cyber Adversaries to Pursue*. Tylercybersecurity.com. Retrieved 25 November 2020, from https://www.tylercybersecurity.com/blog/threat-hunting-six-cyber-adversaries-to-pursue.

[6] What do cybercriminals do with the data? Retrieved 25 November 2020, from https://sysnetgs.com/2018/06/what-do-cybercriminals-do-with-the-data-they-steal/.

[7] Hacktivists launch more cyberattacks against local, state governments. PBS NewsHour. (2020). Retrieved 25 November 2020, from https://www.pbs.org/newshour/nation/hacktivists-launch-cyberattacks-local-state-governments.

[8] Anonymous (group). En.wikipedia.org. (2020). Retrieved 25 November 2020, from https://en.wikipedia.org/wiki/Anonymous_(group).

[9] What Is Cyber Threat Analysis and its components? | EC-Council Blog. EC-Council Official Blog. (2020). Retrieved 25 November 2020, from https://blog.eccouncil.org/what-is-cyber-threat-analysis-and-its-components/#:~:text=Cyber%20threat%20analysis%20is%20the,reactive%20security%20to%20proactive%20security.