Cyber Criminology

Cybercrime Definition and the types

Cybercrime are crimes that are carried out on a computer and computer network. Cyber criminals normally target the victim's security or finances to gain data or sabotage the victim. Types of cybercrime includes stealing data, sabotaging systems, or spying.

The impact of Cybercrime

Many companies or individuals have suffered damages like losing money or brand identity. According to the FBI's Internet Crime Complaint Center, cybercrime has costed the US 7 billion in 2021 .A good example would be the major cyberattack on SolarWinds. In which the attackers gain accessed to all the networks connected to SolarWinds, and started stealing the information on all the networks.

Application of criminological theory

Using rational choice theory it can be said that Cybercriminals go through perceptions of how much they could lose if they commit a crime. Along with their own self interest, like gaining money or stealing private information. Although it seems like many still choose to commit crimes like stealing data because they think they are safe behind their screens.

Criminal Justice

In response to the SolarWinds incident. Federal agencies coordinated a response forming Cyber Unified Coordination Groups. These groups consisted of the Cybersecurity, Infrastructure Security and the Federal Bureau of Investigation. They would integrate private sectors for greater efficiency in incident response.

References

Clough, J. (2015). *Principles of cybercrime*. Cambridge University Press.

McQuade, S. C. (2006). *Understanding and managing cybercrime*. Boston: Pearson/Allyn and Bacon.

Schram, P.J., & Tibbetts, S.G. (2017). Introduction to Criminology: Why Do They Do It? (3rd ed.). Thousand Oaks, CA: Sage.

Office, U. S. G. A. (2022, February 8). Cybersecurity: Federal response to SolarWinds and Microsoft Exchange incidents. Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents | U.S. GAO.

Cybersecurity

DDOS

Distributed Denial of Service is a very brute force and aggressive attack threat that mainly targets integrity and availability. A DDOS attack targets a network and floods it with traffic to overload the network to the point where it shuts down. Countermeasures to protect against DDOS attacks include increasing bandwidth to make it harder to overload the network, or use a CDN to filter out malicious traffic.

Phishing

Phishing is a very dangerous attack and targets all confidentiality, integrity, and availability. Phishing is referred to as a social engineering attack, where it's soul purpose is to trick the victim into either giving the attacker sensitive information or to download malicious software. Countermeasures to protect against phishing is using anti virus software to block malicious software, and also double checking for trick emails

SQL Injection

A Structured Query Language attack is a threat to confidentiality, integrity. SQL injection attacks occur when a malicious code is sent into a website that is using an SQL search box. Countermeasures to protect your website include keeping all software components up to date with the latest security patches, and configuring proper error reporting

Malware

There are a lot of types of malware, that are all treated as threats to confidentiality, integrity, and availability. The most common being viruses, worms, and trojans. These files or codes that infect or steal information but are done in different ways. Worms spread and duplicate to more hosts, trojans hide to perform actions but carry out malicious intents. Countermeasures to protect against malware include using antivirus software to block out viruses, and practicing safe browsing to prevent suspicious links or emails

References

Geerts, T. (2021, June 24). 7 tactics to protect against ddos attacks in 2021: CSA. 7 tactics to protect against DDoS attacks in 2021 | CSA.

Cybersecurity Jobs

Cybersecurity Skills

Networking - Knowledge of networking is key to start a career in cybersecurity, this helps you understand data transmission and how to secure data.
Coding - Knowledge of programming languages like python and java let you identify and fix vulnerabilities, and can prevent scripting attacks as well

Junior Cybersecurity Engineer

Requirements:

- Knowledge of network based, system level, and application layer attacks and mitigation methods
- Scripting and automation skills wither either Bash, Python, Pearl, etc

Cyber Security Manager

Requirements:

- 5 years of combined experience in the Information Security / Cybersecurity domain with a focus on conducting Threat Hunting and/or experience conducting Cyber Incident Response
- Foundational skills in Windows PowerShell and WMI

Threat and Vulnerability Manager

Requirements:

- In depth knowledge in networking, phishing, and endpoint security
- Windows / Linux System Administration

References

Jena, B. K. (2022, October 21). Top 8 cybersecurity skills you must have: Simplilearn. Simplilearn.com. Retrieved from https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-skills