can-help-women-from-being-unfairly-punished-for-challenges-they-face/?sh=7a460d8b6d50 abgerufen

Ruiz, M. (21. April 2021). Covid-19 And Gender Equality: Employers Can Help Women From Being Unfairly Punished For Challenges They Face. Von Forbes: https://www.forbes.com/sites/allbusiness/2021/04/17/covid-19-and-gender-equality-employers-can-help-women-from-being-unfairly-punished-for-challenges-they-face/?sh=7a460d8b6d50 abgerufen

West, K. (7. August 2020). IN A WORLD IMPACTED BY COVID-19, WOMEN LEADERS CAN MAKE THE DIFFERENCE. Von Graduate School of Business University of Cape Town: https://www.gsb.uct.ac.za/ideas-exchange/leadership-and-ethics/in-a-world-impacted-by-covid-19-women-leaders-can-make-the-difference abgerufen

World Health Organization. (9. March 2021). Devastatingly pervasive: 1 in 3 women globally experience violence. Von World Health Organization: https://www.who.int/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence abgerufen

Zetlin, M. (March/April 2018). 54 Percent of Women Report Workplace Harassment. How Is Your Company Responding? Von Inc.com: https://www.inc.com/magazine/201804/minda-zetlin/sexual-harassment-workplace-policy-metoo.html abgerufen

Ethics in Ethical Hacking

Rishi RAJU

Computer Science for Business Management, Romanian-American University, Romania

Abstract

This article explores the ethics in Ethical hacking, the problems faced by ethical hackers, companies, and network systems and a general guideline followed by ethical hackers.

Keywords – Ethical hacking, Ethical hackers, hacking process, White hats, Black hats, network systems.

Introduction

Ethical hacking and ethical hackers (white hat) are terms used to describe hacking that is done under a legal guideline by a company or individual to help identify potential threats on a computer or a network. These methods are used to search for any weak points of a security system that can be exploited by malicious hackers. The information that is gathered through ethical hacking is then used to improve system security, and to minimize any potential attacks. Ethical hacking is a challenging area of study that requires a vast knowledge and mastery of everything that makes up a network or system. Ethical hacking is also called as penetration testing (Wikipedia, the free encyclopedia, 2021).

Background & History

Hacking was first used as a constant way of learning new methods of improving and optimizing systems to run more effectively, hacking was not always displayed under a bad spotlight. It was a term used by engineers who consistently worked to build their systems. Throughout the years

hacking has been used to manipulate and attack networks and systems illegally. In the 1970s with the growing popularity of computer systems people started learning about the capabilities of these systems. People soon began to exploit these capabilities of systems and networks for selfish purposes, which led to the term hacking be an exclusive representation of criminals.

Hacking gained a bad profile in the media. The term "hacker" was used to represent people who were indulged in these malicious activities for personal gains, these group of people today are known as black hats. And then there were people who would try to prevent such malicious attacks on systems and networks, these group of people tested the weaknesses and flaws in a network or system. The people that prevent such malicious activities are known today as white hats or ethical hackers. Ethical hacking started gaining its precedence over the years due to the increase in cybercriminals, it has become a part of a legal system in cybersecurity.

The Ethical Hacking Process

White hat hackers (ethical hackers) honor the boundaries and confidentialities of a business or company they are hired by. They process through the systems same as the Black hat hackers. After the security has been breached through the mentioned process, they work to improve and prevent any malicious access to private details or control over any system (Jaskolj, 2009).

Educational challenges

An ethical hacker needs to possess a bigger understanding of computer skills. It is not feasible for each ethical hacker to be an expert in every field and thus ethical hacking whose members have skills that contribute to one another are created to provide an organization with a team that have the complete skill set required of an ethical hacker.

Organizations may have a large sort of computer systems and it's essential for any ethical hacker to be knowledgeable in operating systems, as well as network hardware platforms. It's also a baseline that an ethical hacker holds a solid foundation of the principles of information security.

I believe with the ever-rising need of cybersecurity; ethical hacking being certified for a good cause is a necessity. Ethical hacking has been a controversial and socially immoral topic but having the

knowledge and ability to control systems and networks that are a huge part of everyone's lives in this generation has become a key in privacy, confidentiality and security.

However, ethical hacking requires a lot of system and network-based knowledge, and to be able to think and predict possibilities. Some forms of knowledge that impact an ethical hacker's skills would be:

a) Programming

b) Scripting Knowledge

c) Networking skills

d) Understanding database

e) Knowledge of platforms and operating systems

f) Knowledge of search engines and servers.

Code of Ethics

Before performing any form of ethical hacking, one must know and understand the state of an organization's system and network. This will provide a guideline for handling information and the sensitivity of the information of that organization.

Deciding the sensitivity of information should be done before and while proceeding with ethical hacking. This is so that one does not violate any company principles or legal laws.

Keeping all the information transparent to the one that has hired him/her always and letting them know of the flaws while ethical hacking is a given. This makes sure that the client knows how to proceed with their confidential data and how to act upon it.

Ethical hacking should always be done within the limits of the client. There is always a way to access beyond the targeted area of a network system but staying within the targeted area and respecting the client's wishes is a huge part of an ethical hacker's morality. This increases the trustworthiness and reliability of the ethical hacker.

After the penetration testing has been conducted, any information gained from it should be held within the company and not disclose any information to other parties (Johansen, 2017).

Social concerns

The field of IT relies on the society's reaction to everything performed by them. As per the ethical principles a firm should communicate with its society. If information systems or schools were to be hacked there will be a huge uprise in the current society. Therefore, with the involvement of ethical hackers in such areas there needs to be a basis of trustworthiness and reliability on any actions performed by them (UKessays, 2018). In the current generation, society plays a major role in how something is perceived and allowing even people who are certified for ethical hacking might be a harder pill to swallow. "The roots of the fabrication of hacking as a social problem lie ultimately in the complex relations of humans to the technologies they create" (Alleyne, n.d.).

Conclusion

Ethical hacking primarily consists of teaching and developing the younger generation's mind-set to only work within the legal boundaries, to report any system vulnerabilities and respect the data sensitivity of the organizations. Companies face a lot of variables and need to consider these variables while hiring white hats or ethical hackers. Building a relationship based on trust is a huge of part being an ethical hacker. The term "Ethical hacker" is a misappropriation of the term "Ethical" (Olivier, 2020), even so in our current society we need to keep security as a primary source of trust for companies that are looking to build themselves within the society. And Ethical hacking to be a part of a bigger picture, rather than to be looked down on due to the history society has delt with hackers.

With the rising popularity of social media, gadgets, military defenses that rely on system and networks that contain confidential information, ethical hacking should be a variable that adds to the security and safety of our society.

References

Alleyne, B. (n.d.). Retrieved from gold.ac.uk: https://research.gold.ac.uk/id/eprint/22394/1/Alleyne%20Hacking_Cambridge%20Encycl%20%20ACCEPTED.pdf

Jaskolj. (2009, april 7). McMaster. Retrieved from wiki.cas.mcmaster.ca: http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking

Johansen, R. (2017, march 24). ethical-hacking-code-of-ethics-security-risk-issues. Retrieved from panmore.com: http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues

Olivier, D. (2020, February 11). Springer. Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-29053-5_9

UKessays. (2018, november). Ukessays. Retrieved from https://www.ukessays.com/essays/information-technology/issues-in-ethical-hacking-and-penetration-testing-information-technology-essay.php?vref=1

Wikipedia, the free encyclopedia. (2021, march 23). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/White_hat_(computer_security)

https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ethical-hacking

http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking

https://en.wikipedia.org/wiki/White_hat_(computer_security)

https://www.eccouncil.org/ethical-hacking/

http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues

UKEssays. (November 2018). Issues In Ethical Hacking And Penetration Testing Information Technology Essay. Retrieved from https://www.ukessays.com/essays/information-technology/issues-in-ethical-hacking-and-penetration-testing-information-technology-essay.php?vref=1

https://research.gold.ac.uk/id/eprint/22394/1/Alleyne%20Hacking_Cambridge%20Encycl%20%20ACCEPTED.pdf