India Henry

CYSE201 - 7:25

3 April 2024

A later module addresses cybersecurity policy through a social science framework. At this point, attention can be drawn to one type of policy, known as bug bounty policies. These policies pay individuals for identifying vulnerabilities in a company's cyber infrastructure. To identify the vulnerabilities, ethical hackers are invited to try to explore the cyber infrastructure using their penetration testing skills. The policies relate to economics in that they are based on cost/benefits principles. Read this article https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453?login=true and write a summary reaction to the use of the policies in your journal. Focus primarily on the literature review and the discussion of the findings.

The first thing that I made note of was on page two when they mentioned using scanners to help find bugs in code. I think that was kind of a shock because while scanners work, and are low in cost, I don't think they find code that has potential of being exploited very well, especially if that code is a logical error instead of a syntax error. Later on in that paragraph, it states that HackerOne's business success is dependent on the fact that it still operates properly as the "bug bounty" programs age, which I think is especially impressive if these programs aren't frequently updated.

Under the “Industry” subheading, it states that the federal government has problems with hiring IT talent which results in them relying on outdated technology that leaves them vulnerable to attacks. While the reasoning behind why the government has trouble hiring IT professionals makes sense, it seems really weird that the federal government uses outdated technology when out of all entities, they probably have the most to keep confidential. In the following paragraph I found it interesting how it dives into the morality of “white hat” hackers. The paragraph insinuates that hackers of any shape only work money or glory. The example the authors use are how social media companies don’t take valuable information in the same way that financial institutions do, so hackers are more likely to submit their reports to social media companies, because they can’t gain much from the information they collected, meanwhile financial institutions should probably stay on guard, because the information that can be collected from them can be sold on the dark web for more than the company is paying to uncover the bugs in their programs.

The article doubles down on hackers only wanting money or glory under the next subheading, “Brand profile”, where the authors talk about the glory hackers would gain from compromising big companies. The article later suggests that glory is actually the main reason why hackers hack. It is broken down that there is a culture that surrounds hacking, and hackers want to gain experience to move up the hierarchy. Secondly, finding bugs might attract employers. Lastly, there have been cases of bug bounty hackers building lucrative careers and becoming security experts.

Overall, it seems bug bounties are going out of style because they attract more inexperienced hackers that companies don’t really want because of how cost ineffective

they are. More experienced hackers are more cost effective for companies, and like Google, the more valuable you are the more willing companies are to increase your paycheck.

References

Sridhar, K., & Ng, M. (2023, January 6). *Hacking for good: Leveraging HackOne data to develop an economic model of Bug Bounties*. Journal of Cybersecurity. Retrieved April 3, 2024, from https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453?login=true