Diana Y Solorzano

CYSE 425W – Cyber Strategy and Policy

Professor Demirel, Hamza

Policy Analysis Paper 1

January 28, 2024

A similarity that most cybersecurity attacks have in common is that most of time the organizations did not see it coming and were not prepared to respond in a way that would minimize the negative impacts that came with the attacks. While one may not know when or how hackers may try to attack, they can still prepare by implementing a thought-out plan that will help them understand what needs to occur before, during, and after an attack; to minimize the negative impacts from these attacks. For this reason, I have selected the Incident Response Plan / Policy to further research in my Policy Analysis Paper 1.

Cybersecurity attacks, large and small are unpredictable do organizations should implement a policy to better prepare themselves for unexpected attack which is what lead to the development of the IRP. The IRP doesn't provide a list of tasks that need to be implemented, but rather provides an outline of different areas that an organization should analyze and develop a plan that could be modified with time. The IRP was also developed as a response to more sophisticated attacks and the damage they caused outside of the information or assets that were compromised from the attacks. Organizations were also losing a substantial amount of money and resources in attempting to stop the attack from further damage and their reputations were also taking large hits due to the lack of structured organization had during these attacks. The development of the IRP was the perfect solution (Kirvan, 2023).

An Incident Response Plan / Policy is a structured plan that will outline the roles and responsibilities for the required actions that will need to occur before, during, and after an attack. This plan will have a detailed instructions on what activities will need to be performed during an attack, as well as the designated individuals or groups who will need to be notified. This policy mainly focuses on 5 main steps which are: 1. Preparation, 2. Detection and Analysis, 3. Containment, Eradication, and Recovery, 4. Post-Incident Activity, and finally 5. Test Your

Plan. Having clear instructions on what to do at each one of these steps and the designated roles certain individuals will have allows for organization to better protect their assets, know how to respond, and improve their policies and procedures for the future (Schlette et al., 2021).

An organization can apply an IRP to their environment by implementing “a set of instructions to detect, respond to and limit the effects of an information security event” (Kirvan, 2023). They would simply need to determine what actions would need to be taken at each of the 5 steps. In step 1, the organization will focus on creating a simple policy that will dictate how the organization will respond to an incident and which individuals will be in charge. In step 2, the organization will determine which avenues will be used to detect vulnerabilities such as monitoring activity or SIEM tools. In step 3, the organization will determine what tools they will use to indicate that their systems may have been compromised. In this step, the organization will also determine how to contain attacks by possibly shutting down systems or isolating certain devices until it is safe to come back online. In step 4, the organization will have a meeting in order to review the events that have just occurred and understand what procedures or action may need to be improved. In step 5, after the organization has analyzed all the information, they will begin initiating drills and exercises to determine if their plans and policies can withstand an attack or if more changes are still needed (Pagnotta2023).

The Incident Response Plan / Policy can fit within a broader national cybersecurity policy mainly because it can be “described as a national approach to handling significant cyber incidents” (CISA, 2021). Cyberattacks can and will happen to any type of organization. Private, public or government organization would all benefit from implementing a plan in order better navigate cyberattacks to minimize the consequences of the attacks. The flexibility and customization of the IRP makes it easy to implement into any organization.

Resources

Kirvan, P. (2023, February 3). *How to build an incident response plan, with examples, template: TechTarget*. Security. https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan

The National Cyber Incident Response Plan (NCIRP): CISA. Cybersecurity and Infrastructure Security Agency CISA. (2021, October 13). https://www.cisa.gov/resources-tools/resources/national-cyber-incident-response-plan-ncirp

Pagnotta, S. (2023, October 17). *5 steps to creating an incident response plan*. Bitsight. https://www.bitsight.com/blog/5-steps-creating-incident-response-plan

Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on Cyber Threat Intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), 2525–2556. https://doi.org/10.1109/comst.2021.3117338