Option #2: Incident Response Plans

Liam Bergerson

CSU - Global

ITS360-1

L. Schneider

1/2/22

Option #2: Incident Response Plans

In this day and age, hackers want nothing more than to find vulnerabilities in a business' network and breach them for their own profit. Simons (2020) discusses that cybercrime has cost businesses over $2 trillion of damage. It is crucial that an incident response plan is developed and implemented to drastically reduce the damage caused by a breach, if one should occur.

Note. Adapted from Tam, M. (2020, August 18). *Elements of an Incident Response Plan*. ISA Cybersecurity Inc. Retrieved December 30, 2021, from https://isacybersecurity.com/elements-of-an-incident-response-plan/

Incident Response Plan

The role of an incident response plan is to reduce the damage caused by a breach. Simons (2020) says that every minute of downtime that passes costs a business $6,000. An incident response plan will highlight crucial steps that should be taken in the event of a breach. This will allow a business to work faster at defusing the threat and minimizing losses.

The major steps of an incident response plan are: Prepare, Identify, Contain, Eradicate, Recover, and Review (Cynet, 2021). Preparation starts with ensuring that the company can respond to an incident when it occurs. Identification involves detecting anomalies from normal operations, understanding if that anomaly represents a security breach, and determining how severe that breach can be. The goal of the containment step is to limit the damage a security breach brings and prevents any further damage. Eradication involves removing any sources of the attack and restoring affected systems. Recovery focuses on bringing systems back to full operation after verifying that it is clean and free from threats. The last step, review, compiles all of the information about the incident and documents how that incident can be prevented in the future.

A successful phishing attack would trigger the incident response plan to take action and try to resolve those issues before devastating damage is done. The malware that has been injected from the phishing link has to be found and eradicated as quickly as possible. Also, an employee that was redirected to a malicious website and has accidentally entered their account credentials into the malicious website would trigger the incident response plan to take action.

Conclusion

An incident response plan is crucial for the resolution of data breaches before devastating damage is inflicted. A business that doesn’t have an incident response plan will suffer more significant damage than a business that has an incident response plan. It allows for an organized approach to eradicating security threats before damage costs become too high.

References

Cynet. (2021, December 14). *Incident Response SANS: The 6 Steps in Depth* Retrieved December 30, 2021, from https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/

Simons, J. (2020, October 28). *Why You Need an Incident Response Plan Now*. ICS. Retrieved December 30, 2021, from https://www.ics-com.net/incident-response-plan/