Defense in Depth Solution for EZTechMovie

- Tyler Chotikamars
- University of Arizona Global Campus
- CYB 499 Capstone for Cyber & Data Security Technology
- Bipin Bhatt
- August 22nd, 2022

Purpose:

- This Power Point is meant to be shown to the board of directors and to those whom security it may concern on the behalf of EZTechMovie. Here, an outline for a defense in depth solution for critical business function will be presented. With this being presented, a solution arises that will help EZTechMovie maintain their business and longevity.

CBF

The Critical Business Function that is being covered within this Power Point presentation includes compliance with the Credit Card Payment Industry. Some other Critical Business Functions that EZTechMovie can work on could include upgrading their network security and data security.

Implementing Policies as a control

The reason policies serve as good controls is because they are cheap to implement. Policies can delegate responsibilities, procedures, and provide instructions. Policies can help set the curve for what is expected from employee’s, this helps protect the company and its customers as it can provide consistency. One thing to keep in mind when creating/implementing policies is that they must be able to stand up in court. Ensuring this will allow the company to operate with less liability.

Implementing Network Security

Implementing network security will ensure that DDoS/Dos attacks, Man in the Middle, Phishing, and other types of attacks are at the very least being monitored.

Information Security Gap Analysis

A major gap exists within the current information security infrastructure. A noticeable problem that exists is non-compliance with the credit card payment industry. Other gaps within security include personal identifiable information exposed to an open network. Network security is also lacking as the company is easily exposed to DDoS/DoS attacks. There is nothing protecting the systems that EZTechMovie operates, this includes attacks from ransomware and other types of viruses.

Security Assessment

The way the EZTechMovie is set up makes the company fit the description of a honey pot without any actual contingency in place to capture intruder data. The current state of EZTechMovie leaves them without a security framework to follow. There also are not any policies that exist to help protect the company. Following the security assessment, it is clear to see that a beginner hacker could easily carry out a multitude of attacks on EZTechMovie. This security assessment could highlight why it is important to do assessments and show how security can affect companies on a large scale. Many companies today have a weak security infrastructure.

Information System Contingency Plan

Contingency plans consist of understanding the system in place, setting procedures in the event of an outage/activation, recovery sequences, and reconstitution. With the case of EZTechMovie, it is clear to see that they need to develop a plan of action for what happens when data goes corrupt, server outages happen, employee’s abuse elevated permissions, and when the credit card payment industry removes them as an authorized dealer. Backing up data and documenting events are a big step in this plan.

Defense in Depth Conclusion

Defense in Depth considers having multiple controls that work together in an effort to provide total security on all fronts of an oncoming attack. In this case this includes protecting everything such as, network switches, firewalls, routers, servers, data center, people, and infrastructure software (Site Report Card, 2018). This defensive strategy has an emphasis on composing strong defenses, as having one vulnerability can allow for others to fester. Implementing a layered security is key in this sense as it will force attackers to target multiple things in order to be successful.

References

- Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning
- Industrial Control Systems Cyber Emergency Response Team. (2016, September). *Recommended practice: Improving industrial control system cybersecurity with defense-in-depth strategies* (Links to an external site.) [Report]. U.S. Department of Homeland Security. https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- Joint Task Force Transformation Initiative Interagency Working Group. (2012, September). *Guide for conducting risk assessments* (Links to an external site.) (Special Publication No. 800-30: Revision 1). National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- Swanson, M., Bowen, P., Wohl A. W., Gallup, D., & Lynes, D. (2010, May). *Contingency planning guide for federal information systems* (Links to an external site.) (Special Publication No. 800-34: Revision 1). National Institute of Standards of Technology. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
- Site Report Card. (2018, Sept). What are the 7 Major IT Infrastructure Components?. What Are the 7 Major IT Infrastructure Components? (sitereportcard.com)