CISO Data Protection Policy

As the Chief Information Security Officer (CISO) of a publicly traded company, one of the most important parts of my job is to make sure that our systems and services are available to our clients. With the amount that we rely on the internet today, we need to make sure that we do everything we can to avoid downtime. With every minute our systems are down, we lose millions of dollars in revenue and lessen the trust our clients have in us as a company. Because of this, protecting availability is one of the most important aspects when it comes to business operations (Stallings & Brown, 2018).

I would make sure that we implement redundancy for all systems and servers. This would include things like load-balancing, failsafe data centers, and hosting our servers in the most efficient, as well as different, locations. Proper and complete backups of all customer data need to be kept on a regular schedule and encrypted. Even though we will have data centers spread across the country, I will also implement offline backups as well as cloud-based backups. If a hurricane, tornado, or flood took out our infrastructure, we would still have backups available. A thorough Disaster Recovery Plan will be formulated and every employee trained on what to do if such an event were to take place (NIST, 2020). As we are a large company, we are a prime target for threat actors. DDoS (Distributed Denial of Service) attacks as well as other remotely executed attacks are something we must plan for and expect to defend against. By implementing CDN's (Content Delivery Networks) into the availability policy, the risk of those kinds of attacks causing major downtime is less likely (Cloudflare, 2023). Firewalls will also be configured to

mitigate these threats and all internal and external networks will be segmented properly. Regular penetration tests will take place unannounced so we can discover and patch any weaknesses or vulnerabilities as soon as possible. All company machines must be set to auto-update all software to make sure any known vulnerabilities within that software is patched accordingly.

By making sure we stay committed to the uptime and availability of our networks for our clients we can provide the backbone upon which our company operates. If our clients are not able to access our services when they need to, they are much more likely to switch to a different company since in modern times everyone is used to instant gratification. By combining the things listed above - redundancy, defense systems and monitoring, and planning for worst-case scenarios - we will eliminate or at least severely reduce downtime.

References

Cloudflare. (2023). What is a DDoS attack? https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

National Institute of Standards and Technology. (2020). NIST SP 800-34 Rev. 1: Contingency planning guide for federal information systems. https://csrc.nist.gov/publications

Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.