Lucas Esquivel

CS 462

Module 13: Assignment

Ransomware is a serious cybersecurity threat to retailers and consumers alike. They pose serious privacy and safety issues as well as making the likelihood of you recovering your data very slim, or you could bend your knee to the attackers and pay them a sum of money they request and even then, they might not give you back your data, or not all of it. Like the article states, over half the employees working in retail don’t understand the cyber-security implications like having poor password hygiene. If I oversaw the CISA and overlooking the UK’s retail market, I would first make sure to emphasize how important the pre-phase 0 is. Planning is the most important step in my opinion. I am a believer of rather being safe than sorry so I will need to make sure I have established the right public-private partnerships that weigh safety and prevention of cyber-attacks before anything else. In this phase it is also important to properly train retail employees, so they at least have knowledge to conduct safe Internet etiquette whenever they are using the company’s network. This phase is also important to make sure systems are running as should and that everyone knows the steps of operation if an attack like ransomware were to occur. It is better to be prepared than to face very costly damages, like this scenario that happened to a British pharmaceutical company that the NotPetya ransomware cost roughly 107 million in disrupted production, goods it couldn’t deliver to its customers, and clean-up and recovery costs (Acronis, 13 January 2020). It is better to spend time and money on preparation so when you get attacked you are better prepared to handle the situation fast and take care of the threat easily.

Another step I would focus on is force deployment because it is a necessity to have a strategic plan that includes Cyber Ops operations in order to handle these attacks. In the UK a National Health Service suffered a ransomware attack back in August that caused major outages to NHS services across the UK. The company Advanced called in both Microsoft and Mandiant to help with investigations (Patrick O’Connor, 26 September 2022). This attack shows why it’s important to focus on both the preparation phase and force deployment phase. This company Advanced who was the service provider for the UK National Health Service was able to have backup help them in dealing with this issue. They were able to contact their buddies from Microsoft and Mandiant to handle the attack which is part of the force deployment phase because in this phase there is systems under attack and operation needs to be implemented. The difference with this and the retail market is that the health sector remains a major attack target to threat groups because of the amount of damage that can be caused and the amount of vulnerabilities that medical equipment can provide for attackers to get into systems. Retailers on the other hand don’t suffer as big ransom payments as other sectors.

Works Cited

Patrick O’Connor, CISSP. “The Biggest Cyber Attacks of 2022.” *BCS*, 8 Nov. 2022, https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2022/.

“The Top 5 Ransomware Attacks in the UK and Their Hidden Costs.” *Acronis*, https://www.acronis.com/en-gb/blog/posts/ransomware-attacks/.