

Watavien Favors

Professor Zehra

CS 462

9 April 2023

Assignment 13

As the leader of the Cybersecurity and Infrastructure Security Agency (CISA) in the US, if the UK government contacts me regarding the increasing ransomware attacks on their retail market, I would take the following steps to help them fight against these attacks. The first thing would be to gather information about the recent attacks, including the type of ransomware, the extent of the damage, and the tactics used by the attackers. This information would help in identifying the vulnerabilities and the patterns in the attacks. After gathering the information, I would assess the situation by analyzing the scope of the problem and the potential risks associated with it. This would help in developing a plan of action that is tailored to the specific needs of the UK retail market. Following assessing the situation, I would develop a strategy to combat the ransomware attacks. The strategy would involve implementing security measures such as firewalls, anti-malware software, and intrusion detection systems, among others. Additionally, I would ensure that the UK retail market has adequate backup and recovery mechanisms in place in case of an attack. It is crucial to train and educate the employees of the UK retail market to recognize potential ransomware attacks and take appropriate actions to prevent them. This would include providing training on basic security practices, such as password management and how to avoid phishing scams. Just because there are security measures in place doesn't mean that the network shouldn't be monitored. After implementing the

security measures, it is crucial to continuously monitor the network and systems for any suspicious activity. This would help in detecting potential attacks before they can cause significant damage.

The scenario for a ransomware attack on the UK retail market would involve a hacker exploiting a vulnerability in the Point of Sale (POS) system to gain access to the network. Once inside the network, the hacker would install ransomware that would encrypt the data and demand a ransom in exchange for the decryption key. The attack could cause significant financial losses and damage to the reputation of the affected retailers.

The main difference between a cyber operation in the retail market sector and other sectors is the nature of the data being targeted. In the retail market sector, the primary focus is on financial data, which can be easily monetized by the attackers. Therefore, attackers may specifically target retail businesses with ransomware attacks to extort money.

To control these ransomware attacks, a proactive approach is required, including continuous monitoring, timely software updates, employee training, and education. Additionally, it is crucial to have a strong well thought-out backup and recovery mechanism in place to ensure that the business can quickly recover from an attack.

In conclusion, ransomware attacks have become a significant cyber threat facing the UK retail market. To combat these attacks, a proactive approach is required that involves gathering information, assessing the situation, developing a strategy, training and educating employees, and continuous monitoring. With the right measures in place, the UK retail market can protect itself against ransomware attacks and ensure the safety of its data.

References

- E&T. (2021, November 19). Ransomware is cyber-criminals' weapon of choice; UK retail facing barrage of attacks. <https://eandt.theiet.org/content/articles/2021/11/ransomware-now-cyber-criminals-weapon-of-choice-as-uk-retailers-face-barrage-of-cyber-attacks/>
- National Institute of Standards and Technology (NIST). (2021). Small Business Information Security: The Fundamentals. <https://www.nist.gov/publications/small-business-information-security-fundamentals>