Rising Cyber Threats: Lessons from Starbucks' Recent Incidents

Source: Pixabay (2018)

Background

In today's digital landscape, the threat of cyber-attacks continues to escalate as more businesses depend on technology to digitalize their service offerings. As a result, these businesses have become primary targets for malicious online activities, leading to significant disruptions and data breaches. In recent years, Starbucks, the multi-billion dollar global coffee chain, has been one of many victims of multiple cyber incidents.

On November 21, 2024, a ransomware attack targeted supply chain management company Blue Yonder, significantly impacting the operations of Starbucks in the U.S. (Hospitality Technology, 2024). Ransomware is a type of cyber-attack that locks an organization's or individual's important data, with the victim being asked to pay a ransom to regain access to their files (Trellix, n.d.). As the back-end solution provider for American Starbucks, the attack on Blue Yonder severely disrupted Starbucks' staff scheduling and salary payments (Forbes, 2024). With the incident occurring just before Thanksgiving, the coffee chain was forced to process payments manually to ensure staff received their holiday pay on time (Forbes, 2024).

In another incident in 2022, a data breach involving almost 330,000 Starbucks Singapore customers was brought to light, with the information being sold on an online forum (The Straits Times, 2022). Stolen information included customers' names, home addresses, and email addresses, but customers were reassured that the coffee shop does not store any customer credit card information (The Straits Times, 2022). The breach was traced back to the coffee chain's contracted loyalty marketing agency, Ascentis, which has been tasked with developing Starbucks Singapore's loyalty reward mobile application since 2014 (Channel News Asia, 2023). The breach was reportedly caused by account credential leakage of a former employee who previously had administrative access to the client database, which the company failed to disable following the employee's departure (Channel News Asia, 2023). This oversight

allowed a malicious hacker to gain access, export, and subsequently sell the customer data online.

Cyber-attacks affect businesses in many ways. Apart from losing customers' trust and damaging their reputation, businesses may also face legal consequences and fines from authorities for failing to protect sensitive customer information. Furthermore, data loss and system breakdowns can disrupt daily operations, causing delays and reducing productivity. In addition, businesses may face direct costs from theft, ransom payments, and recovery efforts. Therefore, it is important for companies to prepare and build resilience against such attacks.

Here are some ways a business can improve its cyber security:

- Establish an incident response plan
- Isolate essential systems to reduce the sprawl of attacks
- Regularly review and disable inactive accounts
- Monitor staff account activities
- Enable Multi-Factor Authentication
- Centralize incident and breach detection to optimize responsiveness

Discussion Questions

1. What lessons can be learned from Starbucks' manual processing of staff payments during the cyber incident?
2. In what ways can a cyber-attack on a supply chain partner, like Blue Yonder, affect the operations of a company such as Starbucks?
3. What strategies can businesses employ to protect themselves from vulnerabilities in their supply chain partners?
4. With the threat of malicious online activities continues to rise, what can Starbucks do to better safeguard customer information from being breached?
5. How can businesses effectively establish and implement an incident response plan to mitigate the impact of cyber-attacks?

References

Channel News Asia. (2023). Loyalty marketing agency fined S$10,000 over data leak of Starbucks Singapore customers. Retrieved https://www.channelnewsasia.com/singapore/starbucks-singapore-330000-customers-data-leak-ascentis-fined-3925281

Forbes. (2024). Wake Up And Smell The Ransomware—Starbucks Impacted By Cyber Attack. Retrieved from https://www.forbes.com/sites/daveywinder/2024/11/27/wake-up-and-smell-the-ransomware-starbucks-impacted-by-ai-cyber-attack/

Hospitality Technology. (2024). Starbucks Affected by Blue Yonder's Ransomware Attack. Retrieved from https://hospitalitytech.com/news-briefs/2024-11-25?article=starbucks-affected-blue-yonders-ransomware-attack

Pixabay. (2018). Cyber, Attack, Encryption. Retrieved from https://pixabay.com/photos/cyber-attack-encryption-smartphone-3327240/

The Straits Times. (2022). 330,000 S'pore Starbucks customers' data leaked, info sold online for $3,500. Retrieved from https://www.straitstimes.com/singapore/330000-starbucks-customers-data-leaked-sold-online-for-3500

Trellix. (n.d.). What is Ransomware?. Retrieved from https://www.trellix.com/security-awareness/ransomware/what-is-ransomware/

Keywords

- Ransomware
- Cyber-attack
- Service disruption
- Data security
- Customer information
- Hospitality