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

日益严峻的网络威胁：星巴克近期事件带来的启示

Source: Pixabay (2018)

背景

在当今的数字化环境中，随着越来越多的企业依赖技术来实现服务数字化，网络攻击的威胁不断升级。因此，这些企业已成为恶意网络活动的主要目标，导致严重的运营中断和数据泄露。近年来，市值数十亿美元的全球咖啡连锁店星巴克，已成为多起网络事件中的众多受害者之一。

2024 年 11 月 21 日，一次勒索软件攻击针对供应链管理公司蓝跃，严重影响了美国星巴克的运营（Hospitality Technology, 2024）。勒索软件是一种网络攻击，它会锁定组织或个人的重要数据，受害者被要求支付赎金以重新获得对其文件的访问权（Trellix，n.d.）。作为美国星巴克的后端解决方案提供商，蓝跃遭受的攻击严重扰乱了星巴克的员工排班和薪资支付（Forbes，2024）。由于此次事件恰逢感恩节前夕，这家咖啡连锁店被迫手动处理支付，以确保员工能按时收到假日薪酬（Forbes，2024）。

在 2022 年的另一起事件中，涉及近 33 万名新加坡星巴克客户的数据泄露事件被曝光，信息在一个在线论坛上被出售（The Straits Times, 2022）。被盗信息包括客户的姓名、家庭住址和电子邮件地址，但客户得到保证，该咖啡店不存储任何客户信用卡信息（The Straits Times，2022）。此次泄露可追溯至该咖啡连锁签约的忠诚度营销机构 Ascentis，该公司自 2014 年以来一直负责开发星巴克新加坡的忠诚度奖励移动应用程序（Channel News Asia，2023）。据报道，此次泄露是由一名前雇员的账户凭证泄露引起的，该雇员此前拥有访问客户数据库的管理权限，而该公司在该雇员离职

后未能停用其权限（Channel News Asia，2023）。这一疏忽使得恶意黑客得以访问、导出并随后在线出售客户数据。

网络攻击以多种方式影响企业。除了失去客户信任和损害声誉外，企业还可能因未能保护敏感的客户信息而面临法律后果和监管机构的罚款。此外，数据丢失和系统崩溃会扰乱日常运营，造成延误并降低生产力。另外，企业还可能面临因数据窃取、支付赎金和恢复工作而产生的直接成本。因此，企业做好准备并建立抵御此类攻击的能力至关重要。

以下是一些企业可以提升其网络安全的方法：

- 制定事件响应计划
- 隔离核心系统以减少攻击蔓延范围
- 定期审查并停用不活跃账户
- 监控员工账户活动
- 启用多因素身份验证
- 集中事件和泄露检测以优化响应能力

讨论问题

1. 从星巴克在网络事件期间手动处理员工薪酬的做法中，可以吸取哪些教训？
2. 像蓝跃这样的供应链合作伙伴遭受网络攻击，可能以哪些方式影响星巴克等公司的运营？
3. 企业可以采取哪些策略来保护自己免受供应链合作伙伴漏洞的影响？
4. 随着恶意网络活动的威胁持续上升，星巴克可以做些什么来更好地保护客户信息免遭泄露？
5. 企业应如何有效建立和实施事件响应计划，以减轻网络攻击的影响？

参考文献

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/

关键词

- 勒索软件
- 网络攻击
- 服务中断
- 数据安全
- 客户信息
- 酒店业/服务业

日益嚴峻的網路威脅：星巴克近期事件帶來的啟示

Source: Pixabay (2018)

背景

在當今的數位化環境中，隨著越來越多的企業依賴技術來實現服務數位化，網路攻擊的威脅不斷升級。因此，這些企業已成為惡意網路活動的主要目標，導致嚴重的營運中斷和數據外洩。近年來，市值數十億美元的全球咖啡連鎖店星巴克，已成為多起網路事件中的眾多受害者之一。

2024 年 11 月 21 日，一次勒索軟體攻擊針對供應鏈管理公司藍躍，嚴重影響了美國星巴克的營運（Hospitality Technology, 2024）。勒索軟體是一種網路攻擊，它會鎖定組織或個人的重要數據，受害者被要求支付贖金以重新獲得對其檔案的存取權（Trellix，n.d.）。作為美國星巴克的後端解決方案供應商，藍躍遭受的攻擊嚴重擾亂了星巴克的員工排班和薪資支付（Forbes，2024）。由於此次事件恰逢感恩節前夕，這家咖啡連鎖店被迫手動處理支付，以確保員工能按時收到假日薪酬（Forbes，2024）。

在 2022 年的另一起事件中，涉及近 33 萬名新加坡星巴克客戶的數據外洩事件被曝光，資訊在一個線上論壇上被出售（The Straits Times, 2022）。被盜資訊包括客戶的姓名、家庭住址和電子郵件地址，但客戶得到保證，該咖啡店不儲存任何客戶信用卡資訊（The Straits Times，2022）。此次外洩可追溯至該咖啡連鎖簽約的忠誠度行銷機構 Ascentis，該公司自 2014 年以來一直負責開發星巴克新加坡的忠誠度獎勵行動應用程式（Channel News Asia，2023）。據報導，此次外洩是由一名前雇員的帳戶憑

證外洩引起的，該雇員此前擁有存取客戶數據庫的管理權限，而該公司在該雇員離職後未能停用其權限（Channel News Asia，2023）。這一疏忽使得惡意駭客得以存取、匯出並隨後在線上出售客戶數據。

網路攻擊以多種方式影響企業。除了失去客戶信任和損害聲譽外，企業還可能因未能保護敏感的客戶資訊而面臨法律後果和監管機構的罰款。此外，數據丟失和系統崩潰會擾亂日常營運，造成延誤並降低生產力。另外，企業還可能面臨因數據竊取、支付贖金和恢復工作而產生的直接成本。因此，企業做好準備並建立抵禦此類攻擊的能力至關重要。

以下是一些企業可以提升其網路安全的方法：

- 制定事件應變計劃
- 隔離核心系統以減少攻擊蔓延範圍
- 定期審查並停用不活躍帳戶
- 監控員工帳戶活動
- 啟用多因素身份驗證
- 集中事件和洩露檢測以優化應變能力

討論問題

1. 從星巴克在網路事件期間手動處理員工薪酬的做法中，可以吸取哪些教訓？
2. 像藍躍這樣的供應鏈合作夥伴遭受網路攻擊，可能以哪些方式影響星巴克等公司的營運？
3. 企業可以採取哪些策略來保護自己免受供應鏈合作夥伴漏洞的影響？
4. 隨著惡意網路活動的威脅持續上升，星巴克可以做些什麼來更好地保護客戶資訊免遭洩露？
5. 企業應如何有效建立和實施事件應變計劃，以減輕網路攻擊的影響？

參考文獻

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/

關鍵詞

- 勒索軟體
- 網路攻擊
- 服務中斷
- 數據安全
- 客戶資訊
- 酒店業 / 服務業