**Cyber security in the retail sector**

Retailers, whether they are small local stores, online sellers, or global brands, are now dealing with a larger volume of data than ever before. This data encompasses customer information, both online and in-store, as well as supply chain and asset tracking data. The way customers shop has fundamentally changed, thanks to online shopping and in-store apps that offer the latest deals and savings. This shift has allowed retailers to create unique customer profiles, enabling them to deliver personalised experiences.

However, every data transfer point presents an opportunity for malicious actors to gain unauthorised access to corporate and personal data. They can also introduce harmful software into the underlying infrastructure, posing a significant threat to businesses and their reputation. While retailers may already have physical and digital security measures in place, the evolving landscape of cybercrime demands a proactive approach. The retail sector must closely examine the latest threats and develop a new model of cybersecurity to counteract them.

**The Changing Face of Cybercrime**

The projected cost of cybercrime is set to reach $10.5 trillion by 2025, highlighting the increasing range of threats retailers face. These threats include account takeover, credit card fraud, phishing, web scraping, API abuses, and distributed denial of service (DDoS) attacks. Although some of these strategies have existed for years, the accessibility and sophistication of artificial intelligence have made them more automated, leading to larger and faster attacks. State-sponsored cybercrime has also added to the constant risk faced by the entire retail sector, impacting sales, customer satisfaction, and brand reputation.

Additionally, due to stringent data protection regulations like GDPR, retailers have a legal obligation to ensure data is collected, transferred, and stored with the utmost care. They are expected to demonstrate a proactive approach to cybersecurity at their corporate headquarters, store locations, warehouses, supply chains, and across their online presence.

**The Ongoing Threat of Ransomware Attacks**

Ransomware attacks remain a significant threat to retailers. Recent examples include an attack on KP Snacks in 2022, which disrupted its IT infrastructure and caused supply issues. In March 2023, WH Smith experienced an attack compromising personal data of its staff. When cybercriminals seise control of IT infrastructure, retailers are unable to conduct business, and paying the ransom does not guarantee data restoration. GDPR regulations also require affected companies to inform customers about compromised data, which can lead to further cybercrimes. Retailers need a comprehensive plan to protect against ransomware attacks, restore critical infrastructure quickly, and secure it to minimise trading losses and reputational damage.

**DDoS Attacks Impact In-Person Sales**

DDoS attacks have long been recognised as disruptive to online businesses, but they can now affect face-to-face sales as well. In the era of contactless payments, if the EPOS system becomes inoperable, sales cannot be completed, impacting retailers' profits, reputation, and customer experience. With the frequency and intensity of DDoS attacks increasing, effective DDoS protection should be an integral part of any robust retail security system.

**Balancing Customer Experiences and Data Security**

The cyber threat landscape is continuously evolving, with new threats emerging regularly. This evolution will only accelerate as the retail sector adopts smart technology, while cybercriminals utilise bots and automation to intensify attacks. Retailers must prioritise cybersecurity on par with physical security systems and collaborate closely with technology partners to develop fully integrated systems that provide customers with peace of mind while shopping.

If you would like to delve deeper into any of the topics discussed here, feel free to reach out to us.