WHITEPAPER

2024

EMERGING CYBER THREATS IN THE MIDDLE EAST RETAIL SECTOR

MAY
24

rewterz

Retail establishments offering both online and physical services are appealing targets for cybercriminals, who employ diverse tactics to breach their security. The Middle East's burgeoning online and brick-and-mortar retail sector is no exception. While cyberattacks of the past have been focused on the lucrative oil and gas sectors in the region, the economic boom of the Gulf Cooperative Council (GCC) and the digitization of retail makes it an increasingly attractive target. Some attacks leverage sophisticated technology to catch vulnerabilities in the IT infrastructure, while others involve insiders simply copying data onto portable media and exiting the facilities.

A study conducted by IBM in 2023 reveals an upsurge in the number of cybersecurity breaches in the Middle East, reaching an unprecedented average cost of $8.07 million per breach. This is a significant increase from 2022, when the average cost per breach was $7.46 million, and notably surpasses the global average of $4.45 million per incident. In fact, the Middle East now ranks second only to the USA in terms of regions with the highest average cost per data breach.

A new report by payments platform Adyen focuses on UAE's retail sector, and the information is troubling. According to Adyen, 44% of UAE retailers experienced cyberattacks in 2023, an increase of 15% from 2022. The report estimates that, on average, UAE businesses fell victim to losses of approximately $2.9 million each due to fraudulent activity.

Cyber attacks and breaches are not limited to retail outlets. Fast Company observes that consumers are increasingly affected by retail sector attackers, with over a third (35%) of UAE shoppers reporting payment fraud in 2023, with Eid being a notable time for cybercrime increases, with cyber criminals poised to take advantage of the surge in consumer spending twice per year at predictable times. A prominent newspaper recently reported that customers can be lured into malicious cyber attacks through phishing scams that promise holiday season benefits and discounts.

BELOW WE DISCUSS SOME OF THE MOST COMMON CYBER ATTACKS AND IT INFRASTRUCTURE VULNERABILITIES EXPLOITED TO HARM RETAILERS:

Network and System Compromise:

Cyber adversaries can compromise the network and systems of shopping centers and retailers by exploiting software and hardware vulnerabilities, pilfering login credentials, or utilizing malware for unauthorized data access. In a notable instance concerning a major apparel and home furnishings retailer, attackers exploited inadequate security measures on the Company's wireless network. This enabled them to intercept card transactions and infiltrate the organization's central database, which lacked encryption and housed sensitive personal and credit card information. The attackers then easily downloaded this database and proceeded to sell the pilfered data across multiple platforms. Multiple techniques targeting wireless networks were employed to breach the system, allowing the perpetrators to monitor and intercept network traffic. This eventually led to the extraction of confidential information.

Third-Party Vendor Compromise:

Presents an escalating threat to shopping centers, with criminals targeting third-party vendor systems to pilfer sensitive information. In August 2022, hackers injected malware into several extensions, including Fishpig, a widely-used vendor providing Magento-WordPress integrations, which are utilized by approximately 200,000 retail eCommerce websites. Retailers may have their internal security on lockdown, but by targeting their service providers, cybercriminals can exploit a forgotten vector into a retailer's data.

Denial-of-service (DoS):

(DoS) attacks are one of the most prevalent cyber threats to shopping centers. These attacks aim to incapacitate the target's systems, disrupting operations and rendering them unavailable for use. Typically, DoS attacks involve crowding the target's systems with an overwhelming volume of traffic, either through an influx of requests to the server or by exploiting weaknesses in the network infrastructure. The retailer is then forced to give in to extortion demands to gain back control of their services. Given their reliance on technology for daily operations, shopping centers are open to such attacks, presenting lucrative targets for cybercriminals. DoS attacks are uniquely troubling for retail operations who need their systems to be online and functional daily for smooth and quick transactions.

In Ransomware attacks criminals infect computer systems with malicious software, encrypting vital data and demanding payment for decryption. Shopping centers are particularly vulnerable to such attacks as they possess large volumes of sensitive customer and financial data. Retailers also have increased reliance on operational systems for daily functions. The repercussions of a ransomware assault on a shopping center can be severe, often including disruptions to routine operations, loss of access to crucial data and systems, financial setbacks stemming from ransom payments, data recovery endeavors, and revenue loss, as well as damage to reputation, erosion of customer trust, and potential complications with insurance claims and legal matters.

Phishing and Social Engineering:

Cybercriminals frequently employ phishing attacks and social engineering tactics to illegaly obtain sensitive information from retailers. This often involves fraudulent emails, text messages, or phone calls, prompting individuals to divulge login credentials or other confidential data. Illustrating this threat, the 2018 Marriot International breach, allegedly initiated through a legacy system adopted after a merger, is speculated to have involved a Remote Access Trojan introduced via a phishing email.

In the Middle East and North Africa region, even human rights defenders must be wary. Human Rights watchdog Amnesty International points to an increase in phishing scams targeting human rights groups, highlighting the third-party provider scam in 2019 in Egypt that targeted civil society groups. Given the increased frequency of such attacks, it is imperative for shopping centers to educate their staff about these risks and implement robust security measures.

Advanced Persistent Threats (APTs):

(APTs) are sophisticated attacks engineered to dodge detection and persist over extended durations. The previously mentioned breach at Marriot International was thought to be inserted through an older system integrated to the Marriot network post-merger.

Ransomware:

Ransomware is a well-known and pervasive threat to the retail sector in 2022, perpetrated by gangs. Some of the more notable groups, such as Hive and ALPHV/BlackCat craft ransomware in a variety of programming languages such as Rust, Python, and Golang. In doing this, that can effectively attack operating systems using diverse combinations. Despite the retail sector's resilience, ransomware attacks posed financial and operational threats due to the handling of extensive customer data, including personally identifiable information and credit card details. A report that examined data from July 2021 to June 2022 revealed that 42 companies in the GCC were targeted, with the majority in the UAE, Saudi Arabia and Kuwait.

Notably in February 2022, an extortion group known as Lockbit reportedly targeted UAE Telecoms giant Etisalat, demanding USD 100,000 for releasing the Company's sensitive data. The proliferation of Ransomware-as-a-Service (RaaS) operations, coupled with the availability of affordable malware kits and phishing tools, has empowered smaller or less-skilled cybercriminals to initiate attacks and breach networks. Often the malware utilized in these attacks operate even in 'Safe Mode', circumventing standard security measures.

Point-of-Sale (POS) and card skimming:

(POS) and card skimming are methods utilized by criminals to illicitly acquire customer credit card details during transactions. These assaults pose significant risks to shopping centers and retailers, potentially leading to substantial breaches of sensitive data. POS systems have increasingly become targets for cybercriminals seeking immediate access to valuable transaction data, including card numbers and PINs. A notable instance involves a major food and beverage retailer. In this case, attackers implanted malware into the retailer's POS systems, enabling the collection of card data, including PINs, from every swiped card. This malware proliferated across the organization, infecting millions of POS systems and harvesting vast quantities of credit card data for resale on illicit markets. It is important to note that the malware used in this attack was commercially available, revealing the accessibility of such tools on the criminal underground.

ADDITIONAL EMERGING THREATS IN THE RETAIL SECTOR:

Insider threats within the retail sector demand attention, particularly as employee turnover rates remain high. Seasonal and short-term employees, possessing system access but lacking strong allegiance to the company, pose significant security risks. Moreover, many retailers outsource business operations to third-party entities, which may not undergo the same rigorous screening as traditional employees. An illustrative example involves a major retailer specializing in communication-related products and services. Over several years, an employee of this retailer illicitly acquired over 8 million pieces of sensitive data, including personal information and classified documents, illegally selling them to bidders.

With increasing instances of cyber attacks, retailers will be well-advised to ensure their IT infrastructure's security is robust and proactive. In addition, enhanced physical internal security measures, screening of third-party vendors and training of employees will all be necessary to ensure that retailers are prepared for any offensives that will come their way.

LEARN ABOUT OUR CUTTING-EDGE SECURITY SOLUTIONS TO KEEP YOUR RETAIL OPERATIONS SAFE.

Contact a Rewterz expert