BIZCOMMUNITY

Retailers must prepare for cybercrime this festive season

Retailers are increasingly coming under attack by cybercriminals, and there is little wonder why. They process payments on oftentimes unprotected Point of Sale (POS) systems, transfer large sums of money, and store and process sensitive customer information, such as banking and card information. They also process more online banking and card transactions. Cybercrime attacks on retail businesses tend to spike over the festive season when transactions spike dramatically.

Retailers are increasingly coming under attack by cybercriminals, and there is little wonder why. They process payments on oftentimes unprotected Point of Sale (POS) systems, transfer large sums of money, and store and process sensitive customer information, such as banking and card information. They also process more online banking and card transactions. Cybercrime attacks on retail businesses tend to spike over the festive season when transactions spike dramatically.

Protecting customers' payment information at every stage of the payment process is vital. Point-to-Point encryption is becoming more critical as it facilitates secure communication channels between devices and company servers, and so protects payment data in transit.

POS systems should be designed to encrypt sensitive data from credit cards the moment information is received and again when it is sent to the payment server, such as passwords, configurations and other critical confidential data.

Get PCI DSS compliant

The Payment Card Industry's Data Security Standard (PCI DSS) increases the governance around cardholder data to reduce credit card fraud. Many banks urge organisations to be PCI DSS compliant to have the right to make credit card payments. Review systems regularly to make sure these standards are followed.

“Most cyber attacks on retail companies happen in the e-commerce space. However, in-store POS systems are not immune to threats.”... “and with the festive season looming, it is a boom time for cybercriminals. Retailers must be aware and implement strategies to guard their businesses, both online and in-store,” says Charl Ueckermann, CEO at AVeS Cyber Security.

According to Ueckermann, AVeS Cyber Security has encountered numerous organisations that have limited to no protection on POS devices. This has a direct impact on cybersecurity for organisations because most times, the POS and corporate systems run on the same infrastructure and network. What this means is that when a POS system is compromised, a network breach can occur for the corporate network as well, leading to confidential client information breaches.

“Protecting POS systems, therefore, requires a multi-faceted and multi-layered approach. You want a highly-effective detection and protection tool to identify and remedy vulnerabilities proactively. The solution should have anti-virus capabilities specifically designed for POS systems. You also want to ensure that the POS software itself is up to date to the latest version, at all times. This is especially important for high transaction times...”

Keep you software updated

POS systems are vulnerable to attack when they are old or outdated because the software would not have been designed with today’s modern-day hackers in mind, making them vulnerable and susceptible to malicious code. Attacks on POS systems are becoming quite sophisticated, and cybercriminals are known to use both hardware and software to hijack payment card information and steal business data. Malware targeting POS systems is common and is one of the many ways to steal payment card details. Malware is used to obtain sensitive information, and in some cases, to even steal money directly from bank accounts.

“Your security technology should be able to detect malware, tampering, rooted/jailbroken POS devices, and more. The security stack should include a feature that proactively alerts retailers and POS providers when it is not safe to use the POS devices for making payments or performing other electronic transactions. If not, your system and your business will be vulnerable,” stresses Ueckermann.

Attackers also exploit mobile POS applications to steal personal and sensitive information that is used to make fraudulent purchases. This can result in big financial losses and damage to credit reputations for unsuspecting customers, and worse still, identity theft.

The backend of mobile applications can also be used by cybercriminals to compromise POS systems as well as the majority of business transactions that are processed on the server’s side. This gives them a way into internal business systems. Once the attacker gets inside the network or central system of POS vendors or retailers, they are able to access the compromised POS application as well as other POS applications used by the retailer in other locations.

Attacking the entry point at the backend is a common attacking method, and Ueckermann says countless large-scale security breaches have been caused by this method.

He concludes, “The onus is on retailers to do the due diligence to protect their customers and data against cyber-attacks over the holiday shopping season and beyond. Strategies and measures should be in place to provide a safe and secure experience for customers online and in-store.

“Card and online payment processes should be secured and encrypted, controls should be in place to check and ensure the integrity of handheld POS devices, and mobile payment systems should be subjected to regular patches, updates, and equipment upgrades to protect against continually evolving threats.”