Cybersecurity for Retail

The retail industry consumes a large quantity of valuable, private consumer data, making businesses within this sector a prime target for cyberattacks. No matter the size, brick and mortar or an online retailer, businesses are easily susceptible to hacks and data breaches from cyber criminals looking to steal precious consumer information. **Here are some stats to consider:**

- 72% of retailers have ***experienced cyberattacks*** and 61% experiencing one last year (Ponemon Institute)
- 50% of retailers have ***no response plan*** for a data breach, 11% higher than average across all industries (Ponemon Institute)
- The retail industry is impacted by ***73%*** of point of sale (POS) breaches (IBM)
- Average loss of customer or employee data in a retail breach is ***7,772 records*** (Ponemon Institute)
- More than ***90% of retailers are out of compliance*** with the Payment Card Industry Data Security Standard, or PCI DSS (SecurityScorecard)
- Fines vary from ***$5,000 to $100,000 per month*** for failing to meet Payment Card Industry Data Security Standards, or PCI DSS. (PCI Compliance Guide)

Solutions to Address Common Challenges and Concerns

Endpoint Security with a strong threat hunting tool and real-time change management configuration keeps you informed of any backdoor hacking attempts online

Anti-Malware/Anti-Virus/EDR should be packaged into all POS systems; if using a mobile-based POS app, ensure network connectivity and all communication channels are encrypted

Adversarial Testing (i.e. penetration testing, web application testing, etc.) and other system assessments help uncover vulnerabilities or weaknesses within systems – very important since you are most likely using open-source and third-party APIs and software for an e-commerce site or mobile payment applications

Comprehensive Vulnerability Assessment program evaluates whether an IT system is exposed to any known vulnerabilities, assigns severity levels to identified vulnerabilities, and recommends remediation or mitigation steps, where required

Encryption Key Management protects customer and financial data in the cloud, maintaining compliance with Payment Card Industry Data Security Standards (PCI DSS)

Firewalls/IPS/IDS around customer data ensures proper handling of payment card information in accordance with PCI DSS and performs the latest software patches and upgrades in a timely manner

Two-Factor Authentication provides an additional layer of validation, reducing a threat actor's attack surface and ability to gain unauthorized access to sensitive and POS data

Find the right security solutions for your retail business.
Get a thorough security assessment and a recommended security plan that not only keeps you protected and compliant but meets your business needs and budgetary requirements.
Email info@techguidance.com or call 855.898.0655.

techguidance
Powered by TBI