Updates
November 22, 2024
‘Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers

As the holiday shopping season kicks into high gear, it also becomes a prime opportunity for cybercriminals to target retailers, their suppliers, and their customers.

As The Hacker News reports, criminal use of artificial intelligence (AI) tools is expected to enhance the established pattern of increased malicious activity against retailers. This time of year presents a perfect storm of risks, making it crucial for retailers to stay vigilant. Here are just a few of the ways bad actors exploit the season:

1. **Targeted cyberattacks.** Retailers face an increased risk of ransomware and denial-of-service attacks. During the holidays, when downtime is most costly, many businesses feel pressured to pay ransoms to avoid disruptions.
2. **Reduced IT and security staffing.** End-of-year vacations often leave security and IT teams understaffed, making it harder to detect and respond to attacks promptly.
3. **Supply chain vulnerabilities.** Cyberattacks on supply chains can have amplified consequences during this busy shopping period, potentially halting deliveries and damaging trust.
4. **Online scams.** With consumers making more online purchases, fraudsters have more opportunities to impersonate retailers and defraud unsuspecting shoppers.
5. **Strain on resources.** The surge in traffic to retail websites consumes bandwidth and resources, creating more room to hide and leaving less capacity to detect and mitigate attacks effectively.
6. **Technical attacks.** “Grinch bots,” exploitation of application programming interface (API) vulnerabilities, and other attack techniques are amplified by the use of AI at a time when retailers’ detection and defense resources may be strained.
7. **Financial fraud.** Holiday shopping sees a sharp rise in payment card fraud, gift card abuse, and fraudulent refund claims.

The threats don’t stop at direct attacks on retailers. Cybercriminals also impersonate trusted brands, luring customers to fraudulent e-commerce sites that steal personal information or payment details. Security Magazine

reported that recent domain-registration activity shows a surge in registration of website names designed to target retailers and their targets, and ICS similarly warns of e-commerce site impersonations. These fake sites not only harm consumers but also damage the reputation and trust retailers rely on. Retailers must remain proactive by requesting takedowns of fraudulent sites and staying informed of these trends.

To counteract these risks, now is the time for retailers to leverage comprehensive cybersecurity strategies. Proactive and reactive measures are essential, including:

- **Preparedness assessments.** Evaluating and enhancing cybersecurity protocols before an incident occurs.
- **Incident response planning.** Assessing current threats and reviewing and practicing response strategies to ensure swift action during an attack.
- **Real-time incident management.** Coordinating with the right enterprise-wide team, including technical and legal experts, to respond effectively to incidents as they unfold.
- **Collaboration with law enforcement.** Facilitating communication and reporting to authorities.
- **Post-incident support.** Managing follow-up actions with customers, regulators, insurers, and other stakeholders.

Perkins Coie partners with top technical and forensic experts to bolster resilience, conduct readiness reviews, and provide incident support. By addressing vulnerabilities and strengthening defenses, retailers can minimize risks while ensuring a secure and successful holiday season.

This holiday season, don’t let cybercriminals take advantage. Stay prepared, stay vigilant, and stay protected.

Authors

Explore more in

Privacy & Security Data Security Counseling and Breach Response Retail & Consumer Products

Related insights

Update

Wrapping Paper Series: Issues and Trends Facing the Retail Industry During the Holiday Season