PROTECTING RETAILERS AND CONSUMERS IN THE MIDST OF CYBERCRIME

As online retail continues to grow in popularity, new risks and vulnerabilities emerge for both the consumer and the retailer. As cybercrime progresses at an incredibly fast pace, criminals are using increasingly sophisticated techniques and technology to expose weaknesses in e-commerce platforms and in user behaviour in ways that are highly effective and damaging.

To secure customer loyalty and maximise convenience for the consumer retailers are storing large amounts of customer data including personal information and payment details. This data is highly valuable and susceptible to exploitation by criminals, either directly through fraudulent transactions, or by monetising this precious information by selling it onwards to other parties to further exploit.

Cybercriminals are becoming more agile, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and cooperating with each other in new ways making this a huge business issue for any organisation.

Retailers need to enhance the protection of their core, and web-facing, infrastructure, which can be subject to large scale and co-ordinated attacks, as well as ensuring their consumers are protected and aware of the risks that online retail can pose.

According to the BRC's 2020 Retail Crime Survey, retailers lost over £1bn to crime and spent a record £1.2bn on crime prevention in the period April 2018 to March 2019. Although a separate report specifically focusing on cyber-crime will be published later this year, the 2019 report found that retailers spent 17% more on cybersecurity than the previous year while almost 80% of the retailers surveyed saw an increase in the number of attacks and/or breaches.

UNDERSTANDING CYBERCRIME IN RETAIL

Cybercrime is a complex problem and no retailer is immune, with the likes of Amazon having admitted being successfully targeted in a recent attack. Retailers have a challenging job to understand, identify and mitigate the multitude of threats that are posed, including:

DATA HACKING – breach digital security defences to access back-end corporate systems and extract key company or consumer data for criminal's own purposes or sell to other criminals

PHISHING – sophisticated emails that appear to originate from a genuine source encouraging recipients to reveal data such as usernames, passwords and payment details

MALWARE – malicious software that can damage corporate systems or enable 'back door' access to an organisation's network. The malware can be installed digitally by encouraging retail staff to click a weblink, or delivered through vulnerable devices connected to the retailer network

RANSOMWARE – malware that disrupts or blocks access to corporate systems until a sum of money is paid. A recent example is the WannaCry attack.

DENIAL OF SERVICE ATTACKS – seeks to disrupt or shut down devices or the network. For retailers, this could be a disruption of the online store causing significant revenue loss

CREDENTIAL STUFFING – attacks that typically use automated bots to attempt to log in to retail sites using lists of compromised user credentials

FRAUDULENT TRANSACTIONS AND IMPERSONATION – criminals steal user credentials, purchase products online via their accounts, and physically obtain the products from the store

WEB SITE OR WEB STORE FRONT ATTACKS – user credentials, payment details and data are captured invisibly from site users using network-based, web scripts and injected code onto the retailer's internet facing web sites.

Computacenter

RESPONDING TO THE CYBERCRIME CHALLENGE

THE IMPACT OF CYBERCRIME IN RETAIL

FINANCIAL

Penalties from fraudulent transactions; loss of revenue from disruption to business services; charges and fines levied due to cybercrime

CUSTOMER SATISFACTION & TRUST

Loss of consumer confidence with regards to data protection; customers switching to competitors or alternatives

COMPLIANCE & REGULATIONS

Additional costs, responsibilities, mitigations resulting from prior cybercrime instances

BRAND AND CONFIDENCE

Damage to reputation and consumer trust following publicity of cyber events and scrutiny on retailer response

Cybercrime is constantly evolving and the range of attacks highly varied and sophisticated making timely detection and prevention a significant challenge. Many attacks play on consumer trust or specifically target more vulnerable consumers in order to maximise success rates. Consumer awareness plays a key role, however there are a range of technology solutions that can be used by retailers to fight back.

1 IDENTITY & ACCESS MANAGEMENT

- Secure accounts managed and governed for both internal users and consumers
- Minimum access to required systems and tools
- Regular processes for changing passwords to keep them secure

2 PRIVILEGED ACCESS MANAGEMENT

- Controlled elevation of security permissions for key (privileged) users in order to undertake specific tasks within the infrastructure
- Privileges can be time or event driven, ensuring that users have no more access than they require

3 ENDPOINT SECURITY

- Anti-virus, anti-malware and firewall products deployed to each individual endpoint
- Continued rigour in the upgrade and security patching of the Operating System and applications mitigate vulnerability threats

4 NETWORK MONITORING

- Deployed inside the network, traffic flows are continually assessed and identification of any rogue traffic or devices appearing on the network
- Deployed outside of the core network to detect potential Denial of Service style attacks

5 PLATFORM HARDENING

- Optimises the configuration of digital systems to remove common vulnerabilities
- Disables unused components and features in order to minimise vulnerabilities

6 PENETRATION TESTING

- Tests the security posture of systems and platforms
- Employs a range of approaches to test devices, systems and networks and assess any weak spots or vulnerabilities

7 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

- Captures, aggregates and correlates security events and logs from systems to aid prevention and detection of security threats by trained analystsapplications mitigate vulnerability threats

8 USER TRAINING AND SUPPORT

- The first line of defence against cyber-crime
- Ensures good practice in using corporate systems or data for retail staff and awareness of cybercrime techniques for consumers

Computacenter

MASTERING BUSINESS SECURITY

DIGITAL Trust.
Mastering business security

COMPUTACENTER'S DIGITAL TRUST

Computacenter offers a comprehensive portfolio of security solutions to mitigate all aspects of the security threat landscape. Our services include:

CYBER DEFENCE CENTER – detects and reacts to cyber security threats. Using trained experts and advanced security solutions we undertake rapid analysis of security threat situations enabling a fast response to mitigate exposure and risk

SIEM CENTRE OF EXCELLENCE – used to enable collection and correlation of security logs and events details in order to provide incident detection and alerting

VULNERABILITY SCANNING – specialist technology scans networks and systems to proactively identify vulnerability and risk areas that may be exposed by criminals. Proactive identification allows these risk areas to be mitigated prior to actual exposure

SECURITY MANAGEMENT – Computacenter provides trained expert security staff to provide management, governance and control of IT security functions to ensure that compliance to the customers security policy is achieved

COMPUTACENTER: WHY WE ARE DIFFERENT

Computacenter has a long and established presence in the retail sector. We work with many leading retail brands to leverage technology to deliver innovative new retail experiences, as well as optimising the management and operation of in-store and digital store technology.

Our credentials include:

- A strong heritage in retail, providing end-to-end solutions to some of the UK and Europe's largest retail organisations
- We are the largest IT reseller in the UK holding strong relationships with the broadest array of vendors to help optimise your commercial engagement
- We are technology independent and able to advise, source, implement and manage technologies from all the market leading vendors
- Expertise across workplace, cloud, data center, underpinned by our networking and security solutions offering retailers an end-to-end solution that is secure and protected by default and design
- We provide opinion and thought leadership on market trends and recommend new innovative solutions
- We offer financial solutions to support technology transformation and deployment, making us a flexible and committed partner

LEADING
pan-European security provider

20+
years' dedicated security practice

4,800+
major incidents managed for our customers annually

200+
highly skilled security experts

7.2m
unique security events handled per year