Infoblox
NEXT LEVEL NETWORKING

REPORT

Retail Risks Revealed: Cybersecurity Threats at All Time High During the Holidays

An International Survey of Retail IT Professionals and Consumers

Foreword

by Victor Danevich, CTO Systems Engineering at Infoblox

The level of online shopping activity increases significantly during the holiday season and can provide rich pickings for the opportunistic cyber-criminal intent on theft or fraudulent behaviour.

With the latest advancements in retail technology creating a larger, more complex attack surface with more potential vulnerabilities open to exploitation, it's never been more important for retailers to have full network visibility so that they can respond quickly to cyber incidents which could result in lost revenue and reputational damage.

Consumers too must be more mindful of threats to their personal data and take appropriate security measures. More education is required on the risks consumers face when shopping online and how they can best avoid them.

Through additional security measures and greater consumer awareness, retailers and their customers can enjoy a happy and secure holiday season, safe in the knowledge that they're doing what they can to keep the criminals at bay.

Overview

This report has been commissioned to gain a better understanding of the threats posed to the personal data of online shoppers, particularly during the holiday season, and whether retailers and consumers are taking sufficient steps to mitigate these threats.

With extensive insights from retail IT professionals in the UK, US, Germany and the Netherlands, as well as feedback from consumers in these regions on their attitudes regarding security when shopping online, we explore seasonal trends in cyber-attacks, the security implications of new technology, and consumer concerns and levels of awareness to these issues.

The report provides practical recommendations on how online retailers can best manage threats to their customers' privacy, during the holidays and throughout the year.

A rise in cyber attacks

The holidays are a time for giving, especially when it comes to retail shopping. Seasonal sales accounted for around a fifth of all retail sales in 2017[1], and it looks as though the volume is only set to increase. US consumers spent more than $108 billion online during the holiday season, 14.7 percent more than during the same period the previous year[2], while overall online sales in the UK rose by 7.6 percent in December 2016[3].

As the number of sales continues to increase, so do the number of attacks on online retailers and their customers. Indeed, the threat of cyber-attack is such that a separate study found the retail industry to be the most at risk[4].

For example, in early 2018, the credit card details of thousands of Macy's customers were compromised when hackers used logins and passwords obtained from third-party sources to access online accounts[5]. Around the same time, malicious software on an external support product enabled the theft of personal and payment details of 40,000 Ticketmaster customers[6]. These are just two of dozens of examples from 2018 alone.

The Infoblox survey revealed that 31 percent of retail IT professionals had witnessed a rise in social engineering attacks over the holiday period, and with good reason. At this time of year, circumstances can often make it easier to catch potential victims off guard. Fake promotional websites are a classic phishing technique, luring people in with an unbeatable deal on that 'must have' present. In these cases, it's worth considering the old maxim; if it seems too good to be true, it probably is.

With an increase in social media scams (15%), DDoS attacks (14%), and ransomware (11%) also being reported, it's little surprise to learn that almost two thirds (65%) of online retailers will increase security measures around network monitoring and visibility during the holidays. However, while bolstering security provisions is vital to tackling threats such as those faced by online retailers, it's also important to recognize

[1] National Retail Federation – Winter Holiday FAQs - https://nrf.com/winter-holiday-faqs
[2] Adobe Digital Insights Holiday Recap 2017 - http://adobeenterprise.lookbookhq.com/adi2018/adi-holiday-2017-rec
[3] British Retail Consortium – Some glitter but no gold for Christmas - https://brc.org.uk/news/2017/some-glitter-but-no-gold-for-christmas
[4] 2018 Trustwave Global Security Report - https://www2.trustwave.com/GlobalSecurityReport.html
[5] Pymnts.com - Macy's Online Customers Warned Of Data Breach - https://www.pymnts.com/news/retail/2018/macys-customers-data-breach-cybersecurity-hack/
[6] BBC News - Ticketmaster admits personal data stolen in hack attack - https://www.bbc.co.uk/news/technology-44628874

the flaws within a network that can be exploited, allowing these threats to disrupt systems, exfiltrate data and cause wider harm.

Unpatched vulnerabilities and customer/end-user errors were jointly cited as the main weaknesses that could result in the occurrence of a network attack (25%), closely followed by vulnerabilities in the supply chain and unprotected IoT devices (23%). Without action however, this awareness has little value. It's crucial therefore that retailers take the necessary steps to ensure that their network is as watertight as possible, whether that's by implementing a solid patch management process, or by educating employees, customers and partners on the potential pitfalls of poor cyber hygiene.

Embracing new technology

Far more than a buzzword, digital transformation is essential for the survival of retailers in an environment dominated by online shopping. Improved customer experience is typically cited as the key driver for any digital transformation program, the importance of which is illustrated by PwC's finding that only four percent of consumers will continue to interact with a brand that provides an unsatisfactory experience[7]. What's more, PwC reports that customers are willing to pay more for greater convenience, speed, efficiency, and a friendly and welcoming service, each of which can be enabled through the application of technology. Technology is developing at an unprecedented pace, however, presenting retailers with a wide range of options for ways in which to enhance their online offering.

Connected smart speakers, for example, such as Amazon Echo and Google Home, are currently enjoying a huge surge in popularity, with sales for 2018 forecast to reach 75 million units[8]. As a result of this widespread adoption, a quarter of consumers already prefer to use a voice assistant rather than a retailer's website or mobile app to make a purchase, and this is expected to rise to 40 percent by 2021[9]. It's unsurprising then that 40 percent of forward-thinking retailers intend to invest in smart speaker technology over the next 12 months.

Whether powering automated sales assistants, or salesbots, or enabling more targeted, personalized offerings based on historical user data, artificial intelligence (AI) is increasingly popular with retailers too. Implementing AI has been found to boost growth by up to 30 percent[10], a factor which is bound to have been a consideration for the 40 percent of respondents planning to invest in the technology during the coming year.

Omnichannel technologies, allowing customers to enjoy a frictionless shopping experience whether online, on a mobile phone or in store, and fourth screen technology, delivering personalized video content, were also cited as targets for future investment by retailers.

However, despite the potential benefits that these and other technological innovations can offer, almost half of the survey respondents (47%) expressed concerns around the complexity and security implications of their implementation.

[7] PwC – Digital transformation in the retail and consumer industry - https://www.pwc.co.uk/services/consulting/accelerate-digital/retail-digital-transformation.html
[8] Canalys – Amazon reclaims top spot in smart speaker market in Q3 2018 - https://www.canalys.com/newsroom/amazon-reclaims-top-spot-in-smart-speaker-market-in-q3-2018
[9] Business Insider Intelligence – Voice in Retail - https://www.businessinsider.com/intelligence/research-store?r=US&IR=T#!/Voice-in-Retail/p/114202737/
[10] Peak – UK retail: The state of the nation - https://blog.peak.ai/uk-retail-the-state-of-the-nation

The opportunities offered by digital transformation are clearly not without risk, and consideration must therefore be given to the potential vulnerabilities in any new technology. As we've seen, around a quarter of retailers see unprotected IoT devices as a risk. In this instance, IT professionals may want to ensure that the manufacturers of such devices build security in from the start, including the ability to change passwords and maintain a regular patching schedule. Investing in enterprise-grade DDI (secure DNS, DHCP and IPAM) would also be recommended to monitor and manage the increasing number of endpoints introduced by each new technology.

Consumer concerns

The majority of global consumers shop online to some extent[11]. According to the survey, over a quarter (26%) said they would shop exclusively online over the holiday season, while 37 percent would also visit brick and mortar stores to make their purchases.

Despite the proliferation of data breaches affecting high profile retailers, the security of personal data is of concern to only 13 percent of online shoppers, even though eight in ten are aware to some degree of the data that is collected through the use of loyalty cards as an example.

For most consumers (60%), the main cause of anxiety is around the delivery time of their online shopping orders. There seems to be either a significant lack of awareness or a general refusal to acknowledge the risk to personal and financial information when shopping online, particularly during the holiday season. The survey data shows retailers experience an increase in social engineering attacks over the holiday period. But the risk of ID fraud, a serious consequence of such an attack, hardly registers with customers, with only 13 percent regarding it as a concern. It's interesting that while appearing to be largely unaware of potential threats to the privacy and security of their personal data, more than a third of consumers (35%) expressed a lack of trust in how their data is held by retailers.

It's perhaps this apparent lack of trust that encourages many consumers to take matters into their own hands. Almost half (47%) of consumers ensure that they are using a secure Wi-Fi network when shopping online, while 29 percent encrypt their passwords. Eighteen percent report taking no steps whatsoever to protect their data.

It's clear from these findings and the mixed signals they send, that more education is required regarding the risks that consumers face when shopping online, especially during the holidays, and the steps that they can take to better protect their own data and identity from those intent on theft and fraud.

[11] Periscope by McKinsey – CPG Goes Omnichannel: Shoppers Grasp the Digital Opportunity - https://www.periscope-solutions.com/download.aspx?fileID=3456

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com