Check Point®
SOFTWARE TECHNOLOGIES LTD

SECURE YOUR EVERYTHING™

RETAIL:
IS DIGITAL EXPANSION OUTPACING SECURITY?

Introduction

A recent news story from Krebs on Security reported, "'BriansClub', one of the largest underground stores for buying stolen credit card data, has itself been hacked. The data stolen from BriansClub encompasses more than 26 million credit and debit card records taken from hacked online and brick-and-mortar retailers over the past four years, including almost eight million records uploaded to the shop in 2019 alone."[1]

One has to ask, why retail organizations are so easily breached. How is it possible to lose vast quantities of sensitive customer data to the likes of global criminal enterprises like BriansClub? The answer: Retail networks are one of—if not the—most complex IT environments of any industry. In this paper, we'll explore the key cyber security issues within the retail environment and suggest ways security professionals can better protect their retail operations.

Retail environment: Complexity everywhere

On the front end, online and brick-and-mortar retailers welcome customer transactions that originate from customer-owned devices. To meet digital transformation initiatives, traditional retailers are employing IoT devices, such as chip readers for automatic checkout, and location-based beacons that can send alerts to customers' smart phones, pitching loyalty discounts and in-store offers. To ensure product availability, some retailers are employing smart shelves that detect weight changes and product movements using RFID tags and sensors. Put it all together and omni-channel and smart-store technologies are blending online, in-store, and location-based services for seamless customer experiences. All of this requires complex IT services. And to top it off, retail chains must make it happen at widely distributed store locations.

A retailer's back-end operations can be equally complicated as they employ several connected business technologies. This includes Point of Sale (POS), Electronic Data Interchange (EDI), automatic identification, and other tech integrate supply chains for Quick Response programs that minimize inventory and labor costs. But as widely reported in headline media coverage, retail systems are being hacked. Four U.S. restaurant chains reported the compromise of their payment systems with malware that stole customers' payment card information.[2] "As payment card data passed through a restaurant's server, the PoS malware copied from the magnetic stripe the card number, expiration date, and internal verification code; the cardholder's name was also available in some cases."[3]

---

[1] Brian Krebs, "BriansClub" Hack Rescues 26M Stolen Cards, Krebs on Security, as viewed on October 16, 2019. https://krebsonsecurity.com/

[2] "Four U.S. Food Chains Disclose Payment Card Theft vis PoS Malware," by Ionut Illascu, BleepingComputer, October 3, 2019

[3] Ibid.

One report showed that 80-90% of the people who log in to a retailer's e-commerce site are hackers using stolen data.[4]

Adding yet further complexity, retail employees access corporate services, such as scheduling software through personal, lightly-protected home computers and smart phones. And with many industries, retailers are moving critical IT workloads from corporate data centers to cloud facilities. Software-as-a-service (SaaS) applications are processed outside retailers' environments.

The big question for IT and cyber security professionals is: have retail IT environments in their race to digitize operations become too complex and distributed to keep secure? Let's look at the retail threat landscape.

Online retailers face new enemies

According to the U.S. Department of Homeland Security, "The retail and consumer products industry faces an increasing number of sophisticated cyber-attacks from nation-state cyber-attackers, criminal cyber-attack-groups, and politically and socially motivated hackers, often planning, coordinating, and implementing cyber-attacks in an integrated manner on a national, multi-national, or global level."[5]

From this, it's easy to see how bad actors can throw more resources into cyberattacks than retailers can muster, given the worldwide shortage of cyber security professionals. In 2019, researchers reported 234 attacks on major retailers resulting in 139 confirmed data breaches.[6] One report showed that 80-90% of the people who log in to a retailer's e-commerce site are hackers using stolen data.[7]

Connecting to suppliers, accounting firms, law firms, and other third-party partners increases retailers' threat of becoming ensnared in sophisticated 5th generation cyberattacks that use multi-vector attacks to spread rapidly from partner to partner on a global scale.

[4] "Kylie Bielby, Retail Sector Unprepared for Increasingly Sophisticated Cyber Attacks, Homeland Security Today, May 7, 2019 https://www.hstoday.us/subject-matter-areas/cybersecurity/retail-sector-unprepared-for-increasingly-sophisticated-cyber-attacks/

[5] "If you bought anything from these 19 companies recently, your data may have been stolen," by Dennis Green, et al, Business Insider, August 15, 2019

[6] 2019 Data Breach Investigations Report—Verizon Enterprise ...

[7] "If you bought anything from these 19 companies recently, your data may have been stolen," by Dennis Green, et al, Business Insider, August 15, 2019

Streamlined cyber security protects complex retail IT

While it seems that retail operations are too complex to keep reliably secure, there are strategies that you can employ to effectively reduce the complexity of retail-industry cyber security and to increase its effectiveness.

Consolidated security architecture

As retailers move to add technologies such as cloud deployments, SaaS, mobility, and IoT devices, it is tempting to add a cyber security point solution to protect each new component. However, this strategy results in a patchwork of security devices that can leave gaps for opportunistic attackers. Plus, adding point solutions means the security team must monitor numerous user interfaces to find and respond to an overwhelming number of diverse security alerts.

Optionally, complexity can be addressed by deploying a consolidated security architecture that can secure each threat vector and offers data-loss-prevention and forensic-analysis tools. This strategy lets retailers cover all customer-facing technologies and infrastructure components whether on-site, SaaS, and in cloud environments, along with mobile devices. All vectors can then be monitored and managed through a single interface.

A consolidated security architecture for all threat vectors has other advantages. When cyber security components talk to each other, they offer more effective protection against 5th generation multi-vector attacks. IT staff can keep tabs of the whole environment all at once. Streamlined monitoring raises security effectiveness while it lowers the burden on and the cost of security staffing.

Within this five minutes, today's polymorphic malware can change to avoid detection systems and spread throughout your network.

Prevention

Inspect the user manuals of many cyber security products and services, and you'll find mention of a minimum five-minute window in which to detect in-progress malware attacks. Within these five minutes, today's polymorphic malware can change to avoid detection and spread throughout your network. Cyber security that depends on detection can fail to prevent malware from entering your systems. This is one possible factor to explain the retail industry's high number of data breaches and numerous alerts and remediation solutions that plague cyber security teams.

There are options. Cyber security solutions can now offer proactive attack prevention to stop malware threats before they penetrate a network. Preventing attacks in this manner further simplifies and reduces the workload required of retailers' security and IT teams. Today, cyber prevention means using advanced techniques that rely increasingly on artificial intelligence (AI) and/or machine learning (ML) and behavioral analysis. There is one caveat. An AI engine for threat prevention must be trained by receiving massive amounts of threat data or it can either miss threat categories or be attacked by being fed intentionally misleading input. Small cyber security providers are unlikely to have access to sufficient threat intelligence to adequately train their AI/ML engines for effective threat prevention.

Conclusion

With digital-first initiatives in full swing, retail organizations can expect even further complexity with their IT systems. Implementing a consolidated security architecture that extends advanced threat prevention to your retail environment, streamlining cyber security operations and increasing security effectiveness. Retail IT is complex. However, with the right strategy, an organization can apply the security to enable online operations and protect sensitive customer data.

A case in point

"Security is not an option for retailers. We hold the details of millions of customers' credit cards; hacking those details can have a catastrophic impact on our corporate reputation. Check Point allows us to work smarter." – John Shi, Manager, Network and Systems Security Engineering, Smart and Final

Learn how this retailer tightened up cyber security to protect itself from increasingly sophisticated professional hackers. The organization's improved visibility into the threat environment is enabling this retailer to grow more rapidly than ever before. Get details here.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com