AGILEBLUE

Automation. Visibility. Confidence.

Online Retail Organizations

Whitepaper

AgileBlue, 2021

Overview

The retail industry has seen a major shift into the digital space in the past 10 years. With more and more retailers transitioning to online models, information technology (IT) teams are being stretched thin to keep up with the demand. Retailers must work to keep their financial and customer data out of the hands of cybercriminals.

Since consumers are increasingly turning to online shopping for almost anything they need, online retailers are collecting and storing more of their personal data to fulfill and ship orders around the world. Online retailers usually experience a high volume of targeted attacks due to the opportunity to access PII and PCI. With some bad actors being successful in these targeted attacks, consumers are taking their business elsewhere and demanding safer systems.

A majority of online retailers use Security Information and Event Management (SIEM) platforms to monitor cyberthreats, which are helpful to a certain extent. While the SIEM notifies IT staff about a potential security threat, it doesn't help the team with next steps and mitigating the threat. AgileBlue's SOC-as-a-Service not only uses advanced threat detection and Machine Learning to alert IT teams about threats, but it also provides teams with automated responses.

At a Glance: Verizon data breach report – NAICS 44-45 (2021 Study):

- 725 incidents; 165 confirmed data disclosure.
- System intrusion, social engineering, and basic web application attacks accounted for about 80% of breaches in this sector.
- 84% of data breaches were caused by external actors, while 17% originated from internal employees.
- 99% of breaches are financially motivated.
- 83% of data compromised consisted personal and payment information.
- The most common asset attacked are retailers' servers.
- >50% of retailers admit they cannot adequately protect IoT devices.

Dangers of Cyberthreats

Extremely sensitive and valuable data resides in the online retail environment everything from PCI data, personally identifiable information (PII), and to credit card information. The loss of this data and intellectual property has a major impact on a company's brand reputation and customer loyalty. When consumers and business customers place their trust and their money in an institution, its reputation for information security is paramount.

Dangers of Cyberthreats Against Online Retailers

Extremely sensitive and valuable data resides in the online retail environment everything from PCI data, personally identifiable information (PII), and to credit card information. The loss of this data and intellectual property has a major impact on a company's brand reputation and customer loyalty. When consumers and business customers place their trust and their money in an institution, its reputation for information security is paramount.

Infrastructure at online retailers is constantly evolving to support line-of business initiatives. While traditionally this has focused on on-premises assets, cloud services in the form of software-as-a-service SaaS) and infrastructure-as-a service (IaaS) are becoming more commonplace as cloud providers address the security concerns of online retailers. Still, the addition of cloud services increases an online retailer's "attack surface" and adds to their cybersecurity risk equation.

Cybersecurity Challenges in the World of Online Retail

Retailers have greatly benefited from the digital transformation. Consumerism used to be a solely an in person experience but has now people can shop with the click of a button. Paper-based records and communications have long been replaced by email, connected databases, VOIP, cloud-based software-as-a-service (SaaS) solutions, and more. Unfortunately, these improvements in operational efficiency also come with increased risks. While retailers have been relatively quick to adopt and deploy promising technologies, they have yet to appropriately address the related security concerns.

Today's cybercriminals hold a strategic advantage, as they can launch attacks at a fraction of the cost–in terms of time, complexity, and resources–that online retailers must typically spend to defend against them. This asymmetric nature of cybercrime is particularly pronounced in smaller firms that may lack the financial resources or have access to skilled security professionals. What's particularly alarming for the online retail industry is that the global cybercrime economy generates an annual profit of $1.5 trillion with online retail making up a large part of this sum due to attacks that access customer and company financial information.

Retail's New Normal According to McKinsey:

Mobile payments have grown in popularity among consumers	Mobile app orders for all retailers have increased in the past year
New or adjusted loyalty programs value customers	Technology implemented into physical stores to increase safety and convenience

Targeted Attacks on Online Retailers

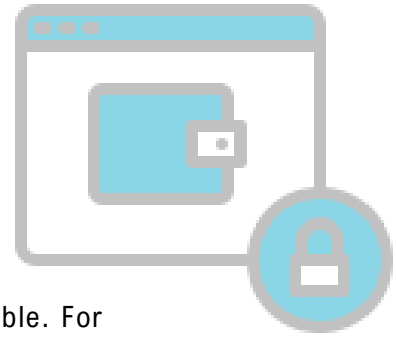
While online retailers of all sizes must comply with frameworks such as PCI-DSS that govern the industry, they face even greater risks and challenges from today's cyberthreats. A single data breach can cause widespread harm to an online retailer, including the exposure of confidential customer information. Cybercriminals continue to devise new attack methods. Below are the top four methods of cyberattacks online retailers have suffered:

Ransomware is a type of malware that either threatens to block access to a victim's data, publish it, or destroy it unless a ransom in cryptocurrencies is paid. Online retailers may install AV or endpoint protection platform (EPP) solutions on employee endpoints, real-time threat intelligence, or custom threat detection logic, but without having an expert team to

carefully analyze alerts and event log data, an attack can go unnoticed. These attacks have become particularly notorious for their ability to evade traditional endpoint controls.

Phishing attacks seek to obtain sensitive information such as usernames, passwords, social security numbers or credit card numbers. Attackers typically operate under the guise of a trustworthy entity, such as a website for a popular retailer, or the login page for an email or messaging service. Email security solutions that offer real-time analysis of URLs in emails, email attachments, and web objects can help with detection. But email security solutions are often unable to flag an embedded malicious URL or attachment before the victim interacts with it. In such cases, firms without continuous network monitoring, Active Directory (AD) monitoring, or advanced monitoring for any deployed SaaS applications are left vulnerable.

Brute-force login attacks involve threat actors systematically attempting password or passphrase combinations until finding correct combinations and accessing restricted resources protected by passwords. In-depth analysis of Active Directory logs and SaaS application login activity are the primary methods used to detect such attacks. Unfortunately, working with authentication data logs is complex and may require analyzing terabytes of data.



Attacks on unpatched servers and infrastructure are specifically designed to exploit weaknesses and vulnerabilities in servers and other Internet-facing systems. In a vast majority of such attacks, patches are publicly announced and made available. For appropriate defense, retailers' access to advanced vulnerability scanning tools for system hardening and alerting. Ideally, they should also deploy continuous network monitoring tools with customized rules to detect anomalous scanning requests coming into Internet-facing entities.

AgileBlue's SOC-as-a-Service, delivers the following capabilities at a simple and predictable monthly pricing model – essentially enabling online retailers to take advantage of managed security operations:

- Fully managed, cloud-based SIEM
- User Behavior Analytics
- Machine Learning Engine
- External threat intelligence
- 24x7 monitoring and alerting
- Automated compliance reporting
- Multi-cloud monitoring – AWS, Azure, Google Cloud

A New Approach for a Secure Future: Adopting SOC-as-a-Service

A SOC-as-a-service enables online retailers to address the listed security gaps that result in the cyberattacks covered in the prior section going undetected. Using a managed SOC service gives companies complete centralized visibility into their networks' security and the ability to leverage existing point products and security investments. It also creates access

to regular vulnerability assessments and enables firms to establish a detailed and customized incident response plan.

The time for the retail industry to make strategic security improvements is now. Effective cybersecurity makes online retailers more prepared, more resilient, and better protected so that they can continue to fulfill their obligations and represent the needs of their clients.

About AgileBlue

AgileBlue is a managed breach detection company with an Autonomous SOC-as-a-Service for 24x7 monitoring, detection and guided response for cloud, digital infrastructures, and applications. AgileBlue provides their clients with enhanced visibility regarding cyber risk via the AgileBlue analytics reporting dashboard. The company offers a proprietary risk scoring algorithm including industry comparisons and risk analysis trends. AgileBlue's Silencer technology significantly reduces false positives with a 95% confidence score on incident alerts based on their proprietary machine learning and user behavior analytics.

Ready to protect your company? Contact Us.