International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 11, November-2020

Cloud Security in the Retail Industry

Balaji Karumanchi
Natsoft Corporation
Irving, TX, USA

Abstract:- With the change in consumer behaviour and trends, organizations are transforming their outlook towards the business. As a result, they are developing and implementing digital applications and adopting various cloud service models.
As retailer operations migrate to the cloud from traditional environments, cyber threats have increased in volume, sophistication, and influence, making it more difficult for organizations to sense, address, and defend against advanced security threats. Cloud security threats are consistently evolving and with the incremental rate of cloud adoption, cyber criminals are also using progressively more complex techniques to target the retail environment.

In the midst these risks, how the industry adopts a cloud service, defines a cloud service model, and deploys their services becomes crucial in the overall equation.

CYBER ATTACK TRENDS

With the rapid evolution of digital Omni channels, the interconnected, agile and direct nature across these channels has inevitably led to a change in the associated cyber threat landscape, attracting cyber criminals target organizations and their customers, across all major sectors. With emerging innovation, in the last 24 months, we have also witnessed significant service disruption across these industrial processes and systems due to re-occurring cyber-attacks.

Even though the attack patterns are evolving and getting sophisticated year by year, cyber criminals have been targeting the sectors, which are primarily in the midst of digital transformations such as Information Technology, Finance, Retail, and Public sector organizations. Likewise *blast radius* of cybercrimes is getting bigger and expensive – according to a 2019 data breach report from Ponemon Institute and IBM Security, the global average cost of a data breach has incremented by approx. 12%, in the last five years to $3.92 million.

To analyse the evolving degree of threats – as per Verizon's DBIR annual 2020 report – approx. 45% of the breaches from 2018, were due to cyber criminals who were successful in exploiting vulnerabilities i.e. unpatched vulnerabilities existing in the IT assets and employed stolen or brute forced credentials to infiltrate into a given environment.

Out of those, 86% of the breaches were financially motivated and the actors driving these threats were majorly external actors which indicate that a value chain across adversaries exists, behind most of the cybercrimes and associated hacking attempts.

The cybercrimes and associated threat vectors that get triggered by these actors are evolving rapidly with adversaries persistently targeting specific processes and technologies, which if successfully exploited, can cause significant damage to an organization's reputation, resulting in considerable financial and operational impact.

As of 2020, the cloud has officially entered its second decade, and its prevalence is increasing, as "cloud first" becomes the expected approach to IT. Despite its longevity, cloud computing still suffers from confusion and hype. Also, longstanding concerns such as cloud computing security, and cloud governance continue to muddle the opinions and approaches of CIOs, architects, and IT leaders.

While the cloud service provider's security is often a focus, managing cyber risk is a shared responsibility between the organizations and the associate cloud provider, depending on the services provisioned for as per the shared responsibility model.

CYBER SECURITY RISKS ACROSS THE RETAIL INDUSTRY

The threat landscape is ever evolving and increasingly challenging. Customer data with such retail institutions and firms have been increasing at a rapid pace. Along with such largescale IT transformations to the cloud, as per Forbes, in the last 24 months – the maturity and sophistication of cyber threat variants have also drastically increased, with multiple cyber-crimes affecting millions of potential targets.

As per the incremental service provisioning in retail, more data will be generated in the next two years than was generated ever before. Customer data is thus, one of the major drivers for cyber criminals which makes the retail industry one of the primary targets for cyber-attacks. We can divide the cyber risks across the retail industry into the following four major categories.

1. **Loss of Data and Data Security Risks** – As the data protection is the responsibility of organizations provisioning the business services across the cloud - service and deployment models, lack of data protection controls and unrestricted access may lead to:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 11, November-2020

a. unauthorized disclosure of customer information
b. excessive and unauthorized access to an organization's sensitive or critical information such as customer data, residing in the cloud

2. **Modern Attack Surface - Application Security** – Insufficient independent security reviews on newly developed applications and APIs may result in vulnerabilities that can be exploited due to programming errors or misconfiguration. This could result in many unmitigated vulnerabilities in the client's environment, including those that could be easily exploited by an attacker to gain unauthorized access to the environment.

   The lack of application vulnerability patching and software upgrades for custom created applications puts an organizations' application and associated services at risk for malicious activity and attacks.

3. **Security operations across the cloud environment** – Lack of controls (such as log management and review) to detect unauthorized changes to your configured cloud computing systems, platforms and infrastructure may lead to security incidents go unnoticed and may have an operational impact to the availability of the core services provisioned via the cloud.

   Lack of cloud security configuration guidelines, hardening frameworks, and security controls may lead the cloud computing architects to follow ad-hoc security practices which may impact the security of the environment and may keep the cloud application and services vulnerable to potential attack vectors.

4. **Third Party (Vendor) Assurance:** As organizations are dependent on cloud provider's controls, the Cloud Service Provider's or third parties providing cloud services that are inconsistent with the contractual obligations pertaining to security, may lead to loss of Confidentiality, Integrity, and Availability of information for the cloud customers.

   Inadequate fair and formal processes in the selection of Cloud Service Provider may result in potentially selecting a service provider that cannot meet the business and security requirements of the organization.

The four key major techniques via which cyber criminals target retail organizations include:

- *Account takeover* by the use of robotic attacks, web injection, and Man-in-the-Middle or Man-in-the-Browser – *Account peeking* is one of the most used tactics by cyber criminals to sanction legitimate credentials, identify potential higher value accounts and recognize the security criteria's which must be compromised to make an unauthorized transaction – successful.

- Business Logic Abuse or the use of portal's functionality for malicious or exploitative purposes (e.g., abuse of loyalty point programs or shopping cart functionality, fraudulent account set up, scripted attacks to find valid codes). The impact of such activity has a direct influence on legitimate customers due to potential unauthorized use of digital offers or coupons, and to an organization's bottom-line due to overall decrease in revenue either via exploiting the offers or because of scripted attacks causing overhead to the retail portal and facilitating site scraping by competitors.

- Distributed-Denial-of-Service or DDOS attack on the application layer is another major tactic wherein, multiple streams of network/illegitimate application traffic coordinated by bot's attempts to overwhelm the application service/serveries environments, for bringing down the service, impacts the customer experience.

- Cloud environment probing is another tactical method used by cyber criminals to conduct reconnaissance and identify security vulnerabilities to prepare for a cyber-attack.

INCORPORATING SECURITY ACROSS THE CLOUD

Cloud is a major change in the way retail sectors are using and deploying information technology, primarily because, with Cloud, businesses gain greater flexibility on IT architecture and sourcing, maximize efficiency (cost vs value), accelerate time to value, reduce time to start up and complete projects.

Based on the business decision, an organization is adopting – Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), from a risk standpoint, before we protect against sophisticated threats – it is highly recommended to:

1. Identify the threat landscape for the cloud environment/ architecture as per the service models and
2. Conduct a threat modeling exercise as per the current state of architecture to identify the top security threats/risks across the business and associated exposure areas

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 11, November-2020

Once an organization identifies the major risks and associated threats to the business, before they implement technology capabilities across the services, they should emphasize on encompassing security features and controls across the following six security domains, which would give them an overarching cloud security coverage.

1. **Identity and Access Management:** Providing customers and employees the appropriate access to respective retail environments and loyalty systems based on their business function and their "need to know" is crucial. For instance, defining governance processes to efficiently manage user lifecycle and ensuring authentication and authorization controls are implemented to protect the access of loyalty confidential data is crucial from an industry standpoint.

2. **Application Security:** Defining application security management controls for front-end, middleware, and backend application layers enable the organization to ensure the application is securely developed, deployed, and integrated with the cloud service functions.

3. **Data Protection and Privacy:** Ensuring preventive and detective controls are enforced to protect customer and business data within the cloud ecosystem, helps to mitigate the major risks associated with data exfiltration. Developing the relevant security processes and equipping the organization's contact centers to comply with data privacy regulations is another aspect that organizations should emphasize from a data standpoint.

4. **Cyber Threat & Incident Management:** Building incident management processes and security monitoring use cases to efficiently detect and respond to cyber threats is fundamental to get visibility from a governance standpoint.

5. **Infrastructure Security:** Security controls should be defined across the in-scope infrastructure components as per the architecture to protect supporting servers, endpoints, and cloud instances from unauthorized access and external attacks.

6. **Retail Fraud Management:** Security controls should be tailored and defined as per the business to detect fraudulent activities of loyalty members, admins or agents. This would enable an organization to trigger alerts on frauds exploiting the digital offers, customer's data and associated program takeaways.

PROTECTION AGAINST THE RISKS

With an ever increasing movement of e-commerce applications and services to cloud service models SaaS, PaaS, and IaaS – traditional endpoint and network security tools are no longer adequate to identify threats across the substantial adopters of public cloud resources, such as retail sector.

This "situational awareness" is a vital component of an organization's overall cloud security posture and critical to preserving the confidentiality, integrity, and availability of its information assets.

With the advancement across machine learning and artificial intelligence capabilities, we are now in a position to use the technology capabilities to enforce the relevant security controls against the identified threats for a given cloud architecture or service model. Thus, to limit the cloud security risks and to define a secure equation, we would recommend the following:

1. Executive's across the retail sector should have a mandate to:
    a. Establish cloud security governance and oversight via a framework for cloud security and create an organization wide security policy for the cloud environment
    b. Develop a strategy to manage cloud security risks as the business moves to the cloud against the identified risks across the organization's cloud space
    c. Define the organization's risk appetite

2. At an operational and tactical level, a cloud architect should ensure that:
    a. Cloud security baselines, policies, and standards are followed for the cloud environment
    b. Cloud security reference architectures for various cloud models are defined
    c. Protection and governance capabilities are put into action to manage to cloud cyber risks
    d. Platform specific security controls are designed and implemented (for instance, SaaS specific data access restrictions)
    e. Cloud testing tools and processes to audit are implemented to review the application and associated services hosted in the cloud
    f. The cloud environment is monitored for anomalies and alert for action, as appropriate
    g. Provide oversight, checks and balances, and enterprise level policies and standards

Cloud drives greater economic value for clients with automation, innovative delivery models, and outcome based constructs, but at the same time, it is necessary to recognize that these recommendations and how an organization's methodology to protect cloud needs to occur, to mitigate threats from the evolving risk landscape.