Ensuring Regulatory Compliance Through Structured Incident Response

By

Mohammad Hanzala

Scenario :

You are a cybersecurity analyst at a mid-sized e-commerce company. The company recently detected suspicious activity on its payment gateway servers. A preliminary investigation revealed the following:

- Multiple failed login attempts from a single IP address
- An unusually high volume of traffic during non-business hours.
- Several customer complaints about unauthorized transactions on their credit cards.
- Logs indicating an outdated software version running on the server.

Problem Elaboration :

1. Multiple failed login attempts from a single IP address this is typically occur due to a **brute force attack**, **credential stuffing**, or **misconfigured automated scripts**. Attackers may be trying to guess passwords systematically or use leaked credentials to gain unauthorized access. It could also result from legitimate users repeatedly entering incorrect credentials.
2. An unusually high volume of traffic during non-business hours this indicates a **Distributed Denial of Service (DDoS) attack**, **data exfiltration attempts**, or **automated scanning by bots**. Attackers is trying to exploit the low monitoring period to overwhelm systems, steal data, or find vulnerabilities.
3. Several customer complaints about unauthorized transactions on their credit cards typically result from **data breaches**, **phishing attacks**, or **malware infections**. The Attacker may have gained access to sensitive payment information through compromised systems, stolen credentials, or intercepted transactions, this leads to fraudulent activity.

4. Logs indicating an outdated software version running on the server may be the reason for the incidents because **outdated software often contains known vulnerabilities** that attackers can exploit. These vulnerabilities may allow unauthorized access, data theft, or remote code execution, leading to issues like brute force attacks, unauthorized transactions, or abnormal traffic spikes. Due to which the attacker has somehow gain the internal access and exploited the data. This is the reason of unauthorized transactions on customer's credit cards.

As a Cybersecurity analyst in a company, I would approach this situation systematically to ensure that the potential incident remediated effectively. Below are my immediate and future action based on the preliminary findings:

Solution :

1. Containment Strategy :

a) Isolate the affected Systems : Immediately identify the affected payment gateway servers. Disconnect them from the network to prevent further unauthorized transactions. Redirect traffic to backup servers or failover systems to ensure continuity for legitimate transactions.

b) Implement Temporary Controls: Blocking the IP address from which multiple failed login attempts originated. Temporarily disable non-essential services on the server to reduce the attack surface.

c) Enable Two-Factor Authentication (2FA): Enforce 2FA on all administrative accounts to prevent unauthorized access.

d) Deploying Firewall and IDS : Using a **Firewall** to filter and monitor HTTP requests to the payment gateway server. Deploying **IDS** or **IPS** for live traffic monitoring**.**

e) Notifying Customers : Informing customers about potential downtime and reassure them that their security is the first priority.

Ensuring legitimate traffic is routed through unaffected servers and maintain transparent communication with customers to minimize disruption.

2. Log Analysis :

a) Prioritized Log Entries : Looking for failed login attempts, especially those from unusual IP addresses or using weak credentials.

Example : Authentication failure for admin from IP x.x.x.x

b) Traffic Anomalies : Identifying login or transaction attempts during non-business hours. Also looking for the unexpected system reboots, service restarts, or performance degradation.

Tools for Log Analysis:

- Splunk : Comprehensive log analysis and visualization.
- ELK Stack (Elasticsearch, Logstash, Kibana) : Real-time monitoring and querying of logs.
- Graylog : Centralized log management with pattern detection.

3. Tool Selection :

a) Real-Time Monitoring of Traffic : Tools like Snort or Suricata can monitor network traffic for malicious activity.

b) Security Information and Event Management (SIEM) : Tools like Splunk or QRadar to aggregate and analyze log data, identify patterns, and alert on anomalies.

c) Endpoint Detection and Response (EDR) : Solutions like CrowsStrike or SentinelOne for continuous monitoring and response on endpoints.

d) Web Application Firewalls (WAF) : WAFs can protect web applications from attacks like SQL injection and cross-site scripting.

Reasoning :

- NIDS : Provides real-time detection of network-based attacks.
- SIEM : Correlates logs from multiple sources to identify complex attacks.
- WAF : Protects web applications from common web vulnerabilities.

4. Impact Assessment (Incident Report Section) :

a) Financial Impact : Loss of revenue due to unauthorized transactions and system downtime. Also costs associated with incident response, investigation, and remediations.

b) Operational Risks : The containment and recovery process might temporarily disrupt payment processing, affecting sales and customer experience.

c) Reputational Impact : Loss of customer due to unauthorized transactions, leads to negatively impact on reputation and future trust.

5. Customer Communication (Notification Email) :

Subject: Important Security Notice (Unauthorized Transactions)

Dear Customer,

We regret to inform you that we have detected unauthorized transactions on our company gateway. Our team is actively investigating the situation and has taken immediate steps to contain and address the issue.

Please review your recent transaction and report any suspicious activity to our support team at support@company.com.

We are committed to ensuring your security and will keep you updated on our progress.

Thank you for your understanding and cooperation.

Sincerely,

abc Pvt Ltd support Team.

6. Post-Incident Recommendations(Preventive Measures) :

a) Strong Password Policies : Enforce strong password policies, including password complexity requirements and regular password changes. Multi-Factor Authentication (MFA) should be implemented for all administrative access to add an additional layer of security.

b) Enhanced Continuous Monitoring : Establish continuous monitoring protocols using SIEM and EDR tools to detect and respond to suspicious activities promptly.

c) User Behavior Analytics (UBA) : UBA tools like Exabeam or Varonis to detect deviations from normal user behavior. By watching compromised accounts or insider threats analysis can be done to check behaviour pattern.

By this approach and implementing these measures, provides a comprehensive guide to handling the incident, ensuring immediate conataiment ensure you to reduce the likelihood of future incidents.