February 2, 2024

Data Security

DSMM - Maple Mapping

PREPARED BY:

Auradee Castro (c0866821)

Bhumika Rajendra Babu (c0867081)

Lakshmi Kumari (c0867090)

Maricris Resma (c0872252)

TABLE OF CONTENTS

I. Case Study Overview

Maple Mapping contains sensitive data with regards to customer location data related to location-based services. Because of this, the company shall come up with data security policies and solutions that follow regulations to ensure safeguarding of data.

II. Security Breach Scenario

Occurrence

An employee falls victim to a phishing email and unknowingly provides their login credentials to an attacker. With these credentials, the attacker gains unauthorized access to the company's internal systems, including the customer database. (Social Engineering: Definition & 6 Attack Types, n.d.)

Once inside, the attacker installs malware on the company's servers, which starts collecting sensitive customer data and transmitting it to a remote server controlled by the attacker. The malware also gives the attacker backdoor access to the company's systems, allowing them to continue exfiltrating data even after the initial breach is discovered.

Meanwhile, the company's security team notices unusual network activity but fails to recognize it as a serious threat until it's too late. By the time they realize the extent of the breach, the attacker has already stolen a significant amount of sensitive customer data, which is now being sold on the dark web.

Sensitive Data

Maple mapping stores vast amounts of customer data due to the reservation feature of the ParkSmart App. Details include the following:

- Personal Information (Name, Age, email, Address)
- Payment details
- reservation history
- Location Data (reservations, parked location history, current location)
- Car information (car type and license)

Consequences of the Data Breach

This Data breach will result to serious financial loss and and PR problem for Maple Mapping. All the possible consequences are further listed below:

- **Customer Loss:** customers lose trust in the company's ability to protect their data
- **Lawsuits:** Regulatory fines for non-compliance with data protection laws, and significant financial losses due to reputational damage and the costs of remediation efforts.
- **Operational Disruption:** Dealing with a data breach can disrupt normal business operations as resources are diverted to manage the incident. This can lead to productivity losses and delays in delivering products or services to customers.
- **Intellectual Property Theft**: In cases where the breach involves theft of intellectual property or trade secrets, the company may suffer competitive disadvantages as its proprietary information is exposed to competitors or the public.
- **Loss of Competitive Advantage:** If a company's sensitive information, such as customer data or business strategies, is compromised, it can lose its competitive advantage in the market as competitors may exploit the stolen information.
- **Impact on Shareholder Value:** A significant data breach can negatively impact a company's stock price and shareholder value, especially if the breach results in a public outcry or widespread media coverage.
- **Financial Loss:** Due to the aforementioned consequences, this will eventually lead to serious financial loss to the company
- **Reputation Damage:** Due to losing trust, this can have long-term effects on the company's ability to attract new customers and retain existing ones.

III. SECURITY POLICIES

Here are a list of the recommended security practices and policies to be followed to better protect the Maple Mapping location-based data services from potential threats and minimize the risk of data breaches. (10 Data Security Best Practices: Simple Methods to Protect Your Data, n.d.)

- **Security Devices:** Protect network from unauthorized access by implementing Firewall
- **Data Encryption:** Encrypt all location-based data both in transit and at rest to prevent unauthorized access. Use strong encryption algorithms and ensure that keys are managed securely.

- **Access Control:** Through ACL, Implement strict access controls to limit who can view and modify location-based data. Use role-based access control (RBAC) to ensure that only authorized personnel can access sensitive data.
- **Authentication and Authorization:** Require strong authentication methods such as multi-factor authentication (MFA) for accessing location-based data services. Ensure that users have appropriate permissions based on their roles.
- **Data Minimization:** Only collect and store the minimum amount of location data necessary for the intended purpose. Regularly review and delete any unnecessary data to minimize the risk of exposure in case of a breach.
- **Secure APIs:** If your location-based data service offers APIs, ensure that they are secure by implementing proper authentication, authorization, and rate limiting to prevent abuse and unauthorized access.
- **Secure Development Practices:** Follow secure coding practices when developing location-based data services to minimize vulnerabilities. Regularly conduct code reviews and security testing to identify and address any potential issues.
- **Data Masking:** When displaying or sharing location-based data, consider using data masking techniques to obfuscate sensitive information such as exact coordinates or identifiable landmarks.
- **Employee Training:** Provide regular training to employees on security best practices, especially regarding the handling of sensitive location-based data. Educate them about the risks of social engineering attacks and phishing attempts.
- **Incident Response Plan:** Have a well-defined incident response plan in place to quickly detect, respond to, and recover from any security incidents involving location-based data services. Regularly test and update the plan as needed.
- **Compliance with Regulations:** Ensure that your location-based data services comply with relevant data protection regulations

IV. Security Awareness Campaign

The security awareness campaign created for this project is an infographic video with a quiz in the end. It conveys the importance of data security and the security policies that Maple Mapping recommends in order to protect the business data. The link for the video can be found: https://www.canva.com/design/DAF7LqyKiZY/Q5lyQQsAOAeWMPKnYe8OLQ/edit?utm_content=DAF7LqyKiZY&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

References

10 Data Security Best Practices: Simple Methods to Protect Your Data. (n.d.). Retrieved from https://www.ekransystem.com/en/blog/data-security-best-practices

Social Engineering: Definition & 6 Attack Types. (n.d.). Retrieved from https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for