Jacob Daley
SDSU Software Development

Assignment- Event Report Submission (iam-1-cybersecurity-current-event-report)

Event Overview:

The Broadvoice data breach occurred in October 2020. An unsecured database belonging to the VoIP provider Broadvoice exposed more than 350 million customer records, including voicemail transcripts, personal details, and other sensitive information.

Type of Attack:

Vulnerability Discovery:

The vulnerability was discovered by a security researcher who stumbled upon an unprotected database while scanning the internet for misconfigured databases (MacKeeper).

Exploitation of Vulnerability:

Attackers did not exploit the vulnerability in the traditional sense; instead, the exposure resulted from Broadvoice's failure to secure its database. The data was left exposed to anyone with internet access, making it susceptible to unauthorized access and potential misuse.

Preventive Security Measures:

- **Database Security:** Ensuring that all databases are secured with proper authentication mechanisms.
- **Regular Audits:** Conducting regular security audits to identify and rectify misconfigurations (Sustainable Business Toolkit).
- **Encryption:** Encrypting sensitive data to protect it from unauthorized access even if exposed.
- **Access Controls:** Implementing stringent access controls to limit who can view or modify the data.

Ukraine Ransomware Attack

Event Overview:

In June 2017, Ukraine experienced a widespread ransomware attack known as NotPetya. The attack initially targeted Ukrainian organizations but quickly spread globally, causing significant disruption and financial losses.

Type of Attack:

This was a ransomware attack, where malicious software encrypts a victim's files and demands a ransom for the decryption key (Ascot IT Services).

Vulnerability Discovery:

The attackers exploited a vulnerability in the MEDoc accounting software widely used in Ukraine. The software update mechanism was compromised, allowing the ransomware to be distributed through legitimate update channels.

Exploitation of Vulnerability:

The NotPetya ransomware spread across networks using the EternalBlue exploit, a vulnerability in Microsoft Windows. Once inside a system, it encrypted files and demanded a ransom payment in Bitcoin.

Preventive Security Measures:

- **Patch Management:** Regularly update and patch software to protect against known vulnerabilities.
- **Network Segmentation:** Segmenting networks to limit the spread of ransomware.
- **Backup Strategies:** Maintaining regular and secure backups to restore data without paying ransom.
- **Employee Training:** Educating employees on recognizing phishing attempts and safe practices to avoid malware infection.

These reports provide a comprehensive understanding of the attacks' nature, how they were executed, and the measures that could have been taken to prevent them.

Twilio Data Breach

Event Overview:

In July 2024, Twilio, a prominent cloud communications platform, confirmed a data breach that exposed 33 million phone numbers associated with the Authy app. Authy is Twilio's two-factor authentication service, making the breach particularly concerning due to the potential misuse of sensitive authentication data (SecurityWeek).

Type of Attack:

This incident involved a data breach caused by unauthorized access to Twilio's systems, which led to the leak of sensitive user information.

Vulnerability Discovery:

The breach was discovered after hackers publicly leaked the stolen data, prompting Twilio to investigate and confirm the extent of the breach. The attackers may have gained access through a compromised administrative account, although the specific methods used by the attackers remain under investigation (SecurityWeek).

Exploitation of Vulnerability:

The attackers exploited weaknesses in Twilio's security protocols to gain unauthorized access to the Authy user phone numbers database. This breach highlights the risks associated with storing large volumes of sensitive user data and the importance of securing access to administrative accounts (InsecureWeb).

Preventive Security Measures:

- **Multi-Factor Authentication (MFA):** Twilio could have enforced more robust MFA protocols for administrative accounts to prevent unauthorized access.
- **Regular Security Audits:** Conducting frequent security audits to identify and patch vulnerabilities in the system (SOS-CA).
- **Access Controls:** Implementing stringent access controls and monitoring to detect and respond to unauthorized access attempts.
- **Data Encryption:** Encrypting sensitive data at rest and in transit to protect it from unauthorized access.

Investigation of Russian Hack on London Hospitals

Event Overview:

In June 2024, a cyberattack attributed to Russian hackers targeted NHS provider Synnovis, affecting hospitals in London. The attack led to significant operational disruptions, with hundreds of surgeries and medical appointments being canceled (SecurityWeek).

Type of Attack:

This was a sophisticated cyberattack, likely involving ransomware or similar malicious software designed to disrupt critical infrastructure and operations.

Vulnerability Discovery:

The attack was discovered when hospital systems began experiencing outages and disruptions. Investigations revealed that the attackers had gained access to the network, likely exploiting a combination of phishing and unpatched software vulnerabilities (ManageEngine).

Exploitation of Vulnerability:

The attackers likely used phishing emails to gain initial access to the hospital's network. Once inside, they exploited unpatched vulnerabilities in the software to escalate their privileges and deploy ransomware, causing widespread disruption (SecurityWeek).

Preventive Security Measures:

- **Phishing Training:** Providing regular training to staff on recognizing and avoiding phishing attempts.
- **Patch Management:** Ensuring that all software is kept up to date with the latest security patches.
- **Incident Response Plan:** Developing and regularly testing an incident response plan to quickly contain and mitigate the effects of an attack.
- **Network Segmentation:** Segmenting the network to limit the spread of ransomware and other malicious software within the organization (Aviso Consultancy).

These reports highlight the importance of robust security practices and the need for continuous vigilance in the face of evolving cyber threats. By learning from these incidents, organizations can better protect themselves and mitigate the impact of future attacks.

Works Cited

MacKeeper. “Data Privacy + Cybersecurity Insider.” *Data Privacy and Security Insider*. https://www.dataprivacyandsecurityinsider.com/tag/mackeeper/.

Sustainable Business Toolkit. “How to Protect Sensitive Data: Secure Your Future.” *Sustainable Business Toolkit*. https://www.sustainablebusinesstoolkit.com/how-to-protect-sensitive-data/.

Ascot IT Services. “Blog.” *Ascot PC*. https://www.ascotpc.com/blog.

SecurityWeek. *Various articles*.

InsecureWeb. “Security Breach at suomi24.fi: Sensitive Data Exposed.” *InsecureWeb*. https://insecureweb.com/security-breach-at-suomi24-fi-sensitive-data-exposed/.

SOS-CA. “Cybersecurity Solutions for Small Businesses.” *SOS-CA*. https://sos-ca.com/cybersecurity-for-small-businesses/.

ManageEngine. “The Shubert Organization Data Breach Exposes Payment Card Data of Its Customers.” *ManageEngine*. https://www.manageengine.com/ca/log-management/phishing-attacks/shubert-organization-data-breach.html.

Aviso Consultancy. “8.21 Security of Network Services.” *Aviso Consultancy*. https://www.avisoconsultancy.co.uk/iso-27001-2022-annex-a/8-21-security-of-network-services/.