1st Assignment

Web Application Security

Sanjith R

(241059044)

1. SolarWinds Supply Chain Attack

Incident Details:
The SolarWinds supply chain attack was discovered in December 2020. It involved the compromise of SolarWinds' Orion software, affecting global organizations, including U.S. government agencies and private companies. The attackers injected malicious code into the software updates, which were then distributed to thousands of clients. This led to the exposure of sensitive information and significant operational disruptions. The estimated losses from this attack exceed $100 million.

Threats and Vulnerabilities:
- Threats: Nation-state actors exploiting third-party software.
- Vulnerabilities: Weak supply chain security, insufficient monitoring of software updates.
- Affected Security Pillars: Confidentiality (data exfiltration), Integrity (malicious code injection), Availability (disrupted operations).

Risk Analysis:
Impact:
- Legal: Compliance violations (GDPR, HIPAA).
- Financial: Loss of millions in remediation costs and lost contracts.
- Reputational: Loss of trust among clients and stakeholders.

Remediation Measures:
- Implement a robust software supply chain security program.
- Conduct thorough audits of third-party software.
- Ensure multi-factor authentication (MFA) for critical systems.

Risk Mitigation Strategies:
- Enforce strict access controls and privilege management.
- Employ continuous monitoring for abnormal system behaviors.
- Conduct regular vulnerability assessments of third-party vendors.

2. Equifax Data Breach

Incident Details:
The Equifax data breach occurred in 2017 and affected systems in the United States. Hackers exploited a known vulnerability in the Apache Struts framework, leading to the exposure of personal data, including Social Security numbers, birth dates, and addresses, of 147 million individuals. The total cost of the breach, including settlements and remediation, exceeded $1.4 billion.

Threats and Vulnerabilities:
- Threats: Exploitation of unpatched software (Apache Struts vulnerability).
- Vulnerabilities: Inadequate patch management.
- Affected Security Pillars: Confidentiality (147 million records exposed).

Risk Analysis:
Impact:
- Legal: Massive fines under GDPR.
- Financial: Settlement costs exceeding $700 million.
- Reputational: Permanent loss of consumer trust.

Remediation Measures:
- Maintain an up-to-date patch management process.
- Regularly scan systems for known vulnerabilities.
- Deploy a Web Application Firewall (WAF).

Risk Mitigation Strategies:
- Conduct employee training on security awareness.
- Use automated tools for vulnerability detection and patching.
- Adopt zero-trust architecture.

3. Log4Shell Vulnerability (CVE-2021-44228)

Incident Details:
The Log4Shell vulnerability was disclosed in December 2021 and had a global impact, affecting enterprise applications and cloud services relying on the Log4j library. Attackers exploited this vulnerability to execute arbitrary code remotely, potentially compromising sensitive user data and disrupting business operations. The worldwide remediation costs from this vulnerability are estimated to run into billions of dollars.

Threats and Vulnerabilities:
- Threats: Remote Code Execution (RCE) via Log4j library.
- Vulnerabilities: Poor input sanitization in logging systems.
- Affected Security Pillars: Confidentiality, Integrity, Availability.

Risk Analysis:
Impact:
- Legal: Class-action lawsuits and regulatory scrutiny.
- Financial: Losses from ransomware deployment.
- Reputational: Damaged brand image due to widespread media coverage.

Remediation Measures:
- Update to Log4j versions with patched vulnerabilities.
- Disable features like JNDI lookup if not needed.
- Implement strict input validation.

Risk Mitigation Strategies:
- Conduct security audits of all third-party libraries.
- Monitor application logs for unusual patterns.
- Use Intrusion Detection Systems (IDS) to flag exploit attempts.

4. Capital One Data Breach

Incident Details:
In March 2019, Capital One suffered a data breach due to a hacker exploiting misconfigured cloud resources. The breach exposed personal data from 106 million credit card applications in the United States and Canada. The financial impact included over $80 million in penalties and additional remediation costs, alongside reputational damage.

Threats and Vulnerabilities:
- Threats: Exploitation of cloud misconfigurations.
- Vulnerabilities: Insufficient IAM policies.
- Affected Security Pillars: Confidentiality (106 million records exposed).

Risk Analysis:
Impact:
- Legal: Fines under data protection laws.
- Financial: Over $80 million in penalties.
- Reputational: Loss of consumer confidence.

Remediation Measures:
- Conduct regular cloud security audits.
- Implement robust IAM policies with the principle of least privilege.
- Use encryption for data at rest and in transit.

Risk Mitigation Strategies:
- Employ continuous monitoring for cloud environments.
- Deploy automated tools to detect misconfigurations.
- Enforce endpoint protection and secure APIs.

5. **Marriott International Data Breach**

Incident Details:
The Marriott data breach was discovered in November 2018 and affected the Starwood guest reservation database. Attackers gained unauthorized access through compromised third-party credentials, exposing sensitive personal information, including passport numbers, of approximately 500 million customers. The financial losses included GDPR fines exceeding $23 million and substantial remediation costs.

Threats and Vulnerabilities:
- Threats: Unauthorized access via compromised third-party credentials.
- Vulnerabilities: Lack of strong authentication mechanisms.
- Affected Security Pillars: Confidentiality (500 million customer records exposed).

Risk Analysis:
Impact:
- Legal: GDPR fines of over $23 million.
- Financial: High costs for legal fees and consumer compensation.
- Reputational: Negative publicity and loss of customer loyalty.

Remediation Measures:
- Enforce MFA across all user accounts.
- Monitor and audit third-party access.
- Encrypt sensitive customer data.

Risk Mitigation Strategies:
- Perform regular penetration testing.
- Establish a dedicated incident response team.
- Provide security training for employees and partners.