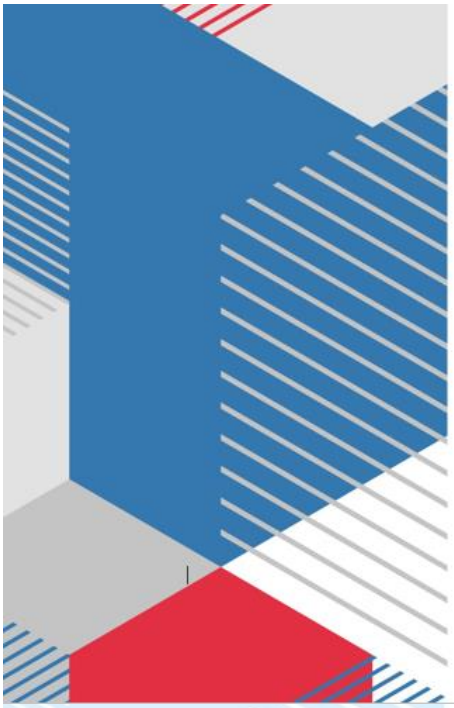

Co-funded by the European Union

Security Analysis and Risk Management

Lab Practical's and Case Studies

Security Analysis and Risk Management

Lab Practical's and Case Studies

Practical Sheet 1: Cybersecurity Risk Assessment Simulation

- Objective: Analyze cybersecurity threats and vulnerabilities using a risk assessment matrix.
- Tools Required: Nessus, OpenVAS, Risk Matrix Template.
- Procedure:
    1. Simulate a small business network setup.
    2. Perform a vulnerability scan using Nessus/OpenVAS.
    3. Identify and categorize threats and vulnerabilities.
    4. Use a risk matrix to prioritize risks.
    5. Propose mitigation strategies.
- Deliverable: Risk Assessment Report.

Practical Sheet 2: Incident Response Role-Playing Exercise

- Objective: Simulate a cybersecurity breach and develop an incident response strategy.
- Tools Required: Scenario document, response templates.
- Procedure:
    1. Divide students into teams (Security, IT, Management, PR).
    2. Provide a simulated data breach scenario.
    3. Develop a response plan following NIST guidelines.
    4. Simulate press communication and damage control.
    5. Discuss lessons learned.
- Deliverable: Incident Response Plan & Team Debrief.

Practical Sheet 3: Threat Modeling Workshop (STRIDE & PASTA)

- Objective: Analyze security threats using STRIDE & PASTA methodologies.
- Tools Required: STRIDE/PASTA templates, whiteboard, case study.
- Procedure:
    1. Select a sample application (e.g., online banking system).
    2. Identify potential threats using STRIDE.
    3. Perform attack simulation using PASTA.
    4. Document potential vulnerabilities and risks.
- Deliverable: Threat Model Report.

Practical Sheet 4: Vulnerability Scanning Lab

- Objective: Use vulnerability scanning tools to identify security weaknesses.
- Tools Required: Nessus, OpenVAS, Kali Linux.
- Procedure:
    1. Set up target virtual machines.
    2. Run Nessus/OpenVAS scans.
    3. Identify high-risk vulnerabilities.
    4. Suggest remediation steps.
- Deliverable: Vulnerability Scan Report.

Practical Sheet 5: Risk Analysis (Quantitative vs. Qualitative)

- Objective: Compare qualitative and quantitative risk analysis methods.
- Tools Required: Risk Calculation Sheet, Case Study Data.
- Procedure:
    1. Choose a fictional security incident.
    2. Perform qualitative analysis (impact severity, likelihood).
    3. Perform quantitative analysis (financial cost estimation).
    4. Compare results and applicability.
- Deliverable: Risk Analysis Report.

Practical Sheet 6: Risk Matrix & Framework Application

- Objective: Apply NIST and ISO 27005 risk assessment frameworks.
- Tools Required: Risk Matrix, Case Study.
- Procedure:
    1. Select a cybersecurity case study.
    2. Use NIST risk assessment methodology.
    3. Map risks in an ISO 27005 framework.
    4. Develop risk mitigation strategies.
- Deliverable: NIST/ISO Risk Report.

Practical Sheet 7: Security Controls Implementation Workshop

- Objective: Implement preventive, detective, and corrective controls.
- Tools Required: Firewalls, IDS, Data Backup Tools.
- Procedure:
    1. Set up a network environment.
    2. Implement firewall and IDS.
    3. Simulate malware attacks.
    4. Apply corrective measures (e.g., data backup).
- Deliverable: Security Control Report.

Practical Sheet 8: Business Continuity and Disaster Recovery Simulation

- Objective: Develop a business continuity and disaster recovery plan.
- Tools Required: Scenario Documents, BCP Templates.
- Procedure:
    1. Simulate a server failure due to ransomware.
    2. Create a disaster recovery plan.
    3. Assign roles for response execution.
    4. Evaluate recovery time objectives (RTO).
- Deliverable: Business Continuity Plan.

Practical Sheet 9: Compliance and Legal Scenario Analysis

- Objective: Analyze cybersecurity compliance requirements (GDPR, HIPAA, CCPA).
- Tools Required: Compliance Templates, Regulatory Documents.
- Procedure:
    1. Provide a data breach case study.
    2. Identify violations of GDPR, HIPAA, or CCPA.
    3. Suggest corrective actions.
- Deliverable: Compliance Report.

Practical Sheet 10: Cybersecurity Ethics Debate

- Objective: Explore ethical dilemmas in cybersecurity.
- Tools Required: Debate Guidelines, Ethical Case Studies.
- Procedure:
    1. Assign teams "For" and "Against".
    2. Debate privacy vs. security trade-offs.
    3. Discuss real-world ethical breaches.
    4. Present findings and ethical solutions.
- Deliverable: Debate Summary Report.

Practical Sheet 11: Network Risk Analysis Workshop

- Objective: Identify and mitigate network-related risks.
- Tools Required: Wireshark, Nmap, Network Topology Templates.
- Procedure:
    1. Map a network topology.
    2. Identify vulnerabilities (e.g., open ports).
    3. Implement mitigation strategies (e.g., firewall rules).
- Deliverable: Network Risk Report.

Practical Sheet 12: Access Control Simulation

- Objective: Implement and test access control models.
- Tools Required: Role-Based Access Control (RBAC) Systems.
- Procedure:
    1. Set up RBAC on a sample system.
    2. Assign roles and permissions.
    3. Simulate unauthorized access attempts.
    4. Evaluate effectiveness of access control.
- Deliverable: Access Control Report.

Case Studies and Further Reading

Case Study 1: MOVEit Transfer Data Breach (June 2023)

Overview: In June 2023, the MOVEit Transfer tool, renowned for securely transferring sensitive files, was targeted in a supply chain attack affecting over 620 organizations, including major entities like BBC and British Airways. Linked to the ransomware group Cl0p, this attack underscores the urgency of promptly patching vulnerabilities and securing web-facing applications to mitigate supply chain risks effectively.

(Reference: https://outshift.cisco.com/blog/top-10-supply-chain-attacks)

Background: MOVEit Transfer is widely used by organizations to manage and transfer sensitive data securely. Despite its reputation, a critical vulnerability allowed attackers to exploit the system, leading to unauthorized data access.

Attack Analysis:

- **Method:** Attackers exploited a zero-day vulnerability in the MOVEit Transfer application, allowing unauthorized access to the system.
- **Scope:** Over 620 organizations were affected, with data breaches impacting millions of individuals.
- **Impact:** Sensitive data, including personal and financial information, was compromised, leading to potential identity theft and financial fraud.

Incident Response:

- **Immediate Actions:** Organizations using MOVEit Transfer were advised to disable the application temporarily and apply security patches released by the vendor.
- **Mitigation Measures:** Enhanced monitoring of data transfers, implementation of additional security controls, and comprehensive audits of data access logs were recommended.

Lessons Learned:

- **Regular Updates:** The importance of timely application of security patches to prevent exploitation of vulnerabilities.
- **Supply Chain Security:** The need for rigorous security assessments of third-party tools and applications.
- **Incident Preparedness:** Establishing robust incident response plans to address supply chain attacks promptly.

Case Study 2: Okta Support System Breach (October 2023)

Overview: In October 2023, Okta, a leading provider of identity and authentication management services, disclosed a significant breach where threat actors gained unauthorized access to private customer data through its support management system. Despite security alerts, the breach went undetected for weeks, highlighting the vulnerability of widely used services like Okta to third-party supply chain risks. (Reference: https://outshift.cisco.com/blog/top-10-supply-chain-attacks)

Background: Okta provides identity and access management solutions to numerous organizations globally. The breach occurred through a compromise in their support management system, which attackers exploited to access sensitive customer information.

Attack Analysis:

- **Method:** Unauthorized access was gained through a vulnerability in Okta's support management system, allowing attackers to exfiltrate customer data.
- **Scope:** All customers utilizing Okta's support services were potentially affected, with data including personal information and support case details being compromised.
- **Impact:** The breach led to concerns over the integrity of identity management services and potential unauthorized access to client systems.

Incident Response:

- **Immediate Actions:** Okta initiated an investigation, notified affected customers, and worked to remediate the vulnerability in their support system.
- **Mitigation Measures:** Enhanced security protocols for support systems, increased monitoring for unauthorized access, and improved incident detection capabilities were implemented.

Lessons Learned:

- **Third-Party Risk Management:** The necessity of assessing and monitoring the security of support and ancillary systems.
- **Detection and Response:** Improving the ability to detect and respond to security alerts promptly to minimize potential damage.
- **Customer Communication:** The importance of transparent and timely communication with customers during security incidents.

These case studies highlight the evolving nature of cybersecurity threats and underscore the importance of proactive security measures, timely updates, and comprehensive incident response strategies to mitigate risks effectively.

Other Case Studies

1. British Library Cyberattack (October 2023)

Overview: In October 2023, the British Library suffered a ransomware attack by the hacker group Rhysida, resulting in the theft and subsequent public release of approximately 600GB of data after a ransom demand of 20 Bitcoin was not met. The attack significantly disrupted the library's services and operations. (Reference: https://en.wikipedia.org/wiki/British_Library_cyberattack)

Key Points:

- Attack Method: Ransomware deployed through phishing or brute-force attacks.
- Impact: Significant service disruptions, delayed payments to authors, and substantial financial costs for recovery.
- Response: Physical disconnection of affected servers and a gradual restoration of services over several months.

---

2. Kadokawa and Niconico Cyberattack (June 2024)

Overview: On June 8, 2024, Japanese media company Kadokawa and its subsidiary Niconico experienced a ransomware attack by the Russian-linked hacker group BlackSuit, leading to a significant data breach and service disruptions.

Reference: https://en.wikipedia.org/wiki/2024_cyberattack_on_Kadokawa_and_Niconico

Key Points:

- Attack Method: Ransomware attack initiated through a phishing attempt.
- Impact: Leakage of personal information of over 254,000 individuals and prolonged service outages.
- Response: Collaboration with law enforcement and cybersecurity experts, and implementation of enhanced security measures.

---

3. Viasat Cyberattack (February 2022)

Overview: On February 24, 2022, a cyberattack targeted Viasat's KA-SAT satellite network, disrupting broadband satellite internet access across Ukraine and parts of Europe. The attack involved the use of a new strain of wiper malware called "AcidRain," which was designed to remotely erase vulnerable modems and routers.

Reference: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

Key Points:

- Attack Method: Deployment of wiper malware to disrupt satellite communications.
- Impact: Significant internet service disruptions affecting tens of thousands of users.
- Response: Investigation by cybersecurity firms and implementation of measures to restore and secure services.

---

4. Equifax Data Breach (2017)

Overview: In 2017, Equifax, one of the largest credit reporting agencies, suffered a data breach that exposed the personal information of approximately 147.9 million Americans, 15.2 million British citizens, and about 19,000 Canadian citizens. The breach was attributed to the exploitation of a known vulnerability that had not been patched.

Reference: https://www.pentestpeople.com/blog-posts/the-top-5-most-dangerous-cyber-attacks-of-all-time

Key Points:

- Vulnerability Exploited: Unpatched software vulnerability.
- Impact: Exposure of sensitive information, including Social Security numbers, dates of birth, and addresses.
- Response: Criticism over poor security practices and delayed public notification; led to increased focus on the importance of timely patch management.