### **Report on 5 Real-World Web Application Attacks**

### **1. Equifax Data Breach (2017)**

### **Threats:** Exploitation of an unpatched vulnerability (Apache Struts CVE-2017-5638).

### **Vulnerabilities:**

### Outdated software.

### Insufficient patch management processes.

### **Affected Security Pillars:**

### **Confidentiality:** Sensitive personal data of 147 million people, including Social Security Numbers and financial information, was exposed.

### **Integrity:** Compromised data integrity due to unauthorized access.

### **Availability:** Limited disruption to services but potential for further exploitation.

### **Risk Analysis:**

### **Legal:** Regulatory fines exceeding $700 million imposed by the FTC.

### **Financial:** Direct and indirect costs, including remediation, legal fees, and credit monitoring.

### **Reputational:** Significant loss of public trust and customer confidence.

### **Remediation Measures:**

### Timely application of software patches.

### Regular vulnerability assessments and automated monitoring tools.

### **Risk Mitigation Strategies:**

### Implement a robust patch management system.

### Conduct regular third-party audits.

### Enforce strict access control policies.

### **Sources:**

### Federal Trade Commission report on Equifax breach.

### CVE database.

### **2. SolarWinds Supply Chain Attack (2020)**

### **Threats:** Supply chain compromise via malicious updates to the Orion IT monitoring platform.

### **Vulnerabilities:**

### Weak supply chain security practices.

### Lack of code integrity checks.

### **Affected Security Pillars:**

### **Confidentiality:** Unauthorized access to government and corporate networks.

### **Integrity:** Manipulation of sensitive systems and data.

### **Availability:** Potential disruption to critical systems.

### **Risk Analysis:**

### **Legal:** Potential violations of cybersecurity compliance standards.

### **Financial:** Costs related to incident response and system recovery.

### **Reputational:** Erosion of customer trust in the software provider.

### **Remediation Measures:**

### Enhanced code-signing practices.

### Strict vetting of third-party software dependencies.

### **Risk Mitigation Strategies:**

### Adopt zero-trust principles.

### Regularly audit supply chain components.

### Employ advanced threat detection mechanisms.

### **Sources:**

### CISA analysis of SolarWinds compromise.

### Microsoft Security Report.

### **3. Target Data Breach (2013)**

### **Threats:** Credential theft via a third-party HVAC vendor, leading to malware deployment.

### **Vulnerabilities:**

### Inadequate third-party access controls.

### Insufficient network segmentation.

### **Affected Security Pillars:**

### **Confidentiality:** Compromise of 40 million payment card details and 70 million customer records.

### **Integrity:** Data manipulation during transmission.

### **Availability:** Operational impact during remediation.

### **Risk Analysis:**

### **Legal:** Class-action lawsuits and regulatory scrutiny.

### **Financial:** Losses exceeding $200 million.

### **Reputational:** Damage to brand image and customer loyalty.

### **Remediation Measures:**

### Implement network segmentation.

### Use two-factor authentication for third-party access.

### **Risk Mitigation Strategies:**

### Establish rigorous vendor risk management programs.

### Conduct regular penetration testing and security assessments.

### **Sources:**

### Investigation reports by Verizon and Bloomberg.

### PCI Security Standards Council.

### **4. Log4Shell Vulnerability Exploitation (2021)**

### **Threats:** Remote code execution via the Apache Log4j library (CVE-2021-44228).

### **Vulnerabilities:**

### Unpatched and widespread use of vulnerable versions of Log4j.

### Lack of input validation.

### **Affected Security Pillars:**

### **Confidentiality:** Exposure of sensitive data through unauthorized access.

### **Integrity:** System compromise allowing attackers to alter data.

### **Availability:** Potential for ransomware attacks and system downtime.

### **Risk Analysis:**

### **Legal:** Non-compliance with regulatory standards on data protection.

### **Financial:** High costs related to patching and damage control.

### **Reputational:** Loss of user confidence due to security lapses.

### **Remediation Measures:**

### Update to patched versions of Log4j.

### Employ runtime application self-protection (RASP) tools.

### **Risk Mitigation Strategies:**

### Conduct regular dependency scans.

### Educate developers on secure coding practices.

### Use web application firewalls (WAFs) to filter malicious requests.

### **Sources:**

### Apache Foundation advisory.

### NIST National Vulnerability Database.

### **5. Uber Data Breach (2016)**

### **Threats:** Theft of developer credentials and unauthorized access to sensitive customer data.

### **Vulnerabilities:**

### Insecure credential management practices.

### Lack of multifactor authentication.

### **Affected Security Pillars:**

### **Confidentiality:** Exposure of driver and rider data, including names, email addresses, and phone numbers.

### **Integrity:** Compromised internal systems.

### **Availability:** Minimal direct service disruption.

### **Risk Analysis:**

### **Legal:** $148 million settlement with U.S. regulators.

### **Financial:** Fines, legal fees, and loss of market share.

### **Reputational:** Erosion of public trust and brand damage.

### **Remediation Measures:**

### Use of secure secrets management solutions.

### Enforcement of multifactor authentication (MFA).

### **Risk Mitigation Strategies:**

### Regularly rotate access keys and credentials.

### Monitor and audit access logs.

### Train employees on secure practices.

### **Sources:**

### Federal Trade Commission and DOJ reports.

### News reports by Reuters and Wired.