Cyber Security Compliance

Index

Introduction to Cyber Security Compliance

Cyber security compliance involves adhering to laws, regulations, and standards designed to protect information and systems from cyber threats. It ensures organizations implement adequate security measures to safeguard sensitive data and maintain the trust of stakeholders. Compliance is crucial in industries that handle sensitive information, such as finance, healthcare, and retail.

Key Compliance Frameworks and Standards

1. Cyber Security Compliance (GDPR, HIPAA, SOX)

- **GDPR (General Data Protection Regulation):** A regulation in the European Union focused on protecting personal data and privacy. It applies to organizations worldwide that process data of EU residents.

Practical Scenario: An e-commerce company collecting personal data from EU customers must comply with GDPR by implementing strong data protection measures, such as data encryption, and obtaining explicit consent for data processing.

- **HIPAA (Health Insurance Portability and Accountability Act):** A U.S. law that protects patient health information. It applies to healthcare providers, insurers, and other entities handling protected health information (PHI).

Practical Scenario: A hospital implements HIPAA compliance by ensuring that patient records are securely stored, access is restricted to authorized personnel, and data breaches are promptly reported.

- **SOX (Sarbanes-Oxley Act):** A U.S. law aimed at preventing corporate fraud by enforcing stringent financial reporting and internal controls. It includes provisions for data security, particularly in protecting financial information.

Practical Scenario: A publicly traded company implements SOX compliance by ensuring that financial data is accurate, secure, and accessible only to authorized personnel, with regular audits and controls in place.

2. ISO/IEC 27001 and ISO/IEC 27002

- **ISO/IEC 27001:** An international standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive company information, ensuring it remains secure.
- **ISO/IEC 27002:** A complementary standard providing guidelines and best practices for implementing the controls defined in ISO/IEC 27001.

Practical Scenario: A financial institution adopts ISO/IEC 27001 and ISO/IEC 27002 to protect customer data, including implementing access controls, conducting risk assessments, and training employees on information security policies.

3. PCI-DSS (Payment Card Industry Data Security Standard)

PCI-DSS is a set of security standards designed to protect cardholder data. It applies to organizations that handle credit card information, including merchants and payment processors.

Practical Scenario: A retail store follows PCI-DSS requirements by encrypting cardholder data, implementing strict access controls, and regularly testing security systems to prevent data breaches.

Penetration Testing Standards

1. OWASP (Open Web Application Security Project)

OWASP provides a framework for securing web applications, including the OWASP Top 10, which lists the most critical security risks to web applications.

Practical Scenario: A web development company uses OWASP guidelines to secure its applications by addressing vulnerabilities like SQL injection and cross-site scripting (XSS) during development and testing.

2. WASC (Web Application Security Consortium)

WASC provides standards and best practices for web application security, including the WASC Threat Classification, a detailed list of web security risks.

Practical Scenario: A cybersecurity firm conducts a penetration test on a client's web application using the WASC Threat Classification to identify and mitigate potential threats.

3. SANS25

The SANS Top 25 is a list of the most dangerous software errors that can lead to vulnerabilities. It provides guidance on preventing and mitigating these errors.

Practical Scenario: A software company uses the SANS Top 25 to audit its codebase, identifying and fixing common vulnerabilities like buffer overflows and insecure cryptographic storage.

4. PTES (Penetration Testing Execution Standard)

PTES provides a comprehensive framework for conducting penetration tests, including pre-engagement, intelligence gathering, threat modeling, and exploitation.

Practical Scenario: A penetration tester uses PTES to plan and execute a thorough security assessment of a client's network infrastructure, identifying and exploiting vulnerabilities to demonstrate potential risks.

5. OSSTMM (Open Source Security Testing Methodology Manual)

OSSTMM is a comprehensive security testing methodology covering various aspects of security, including information security, physical security, and process security.

Practical Scenario: A security consultant uses OSSTMM to conduct a holistic assessment of an organization's security posture, including testing physical security controls, evaluating information security policies, and assessing network security.

Risk Governance & Risk Management

Risk governance involves establishing a framework for managing risk within an organization. Risk management involves identifying, assessing, and prioritizing risks, followed by implementing strategies to mitigate or manage those risks.

Practical Scenario: A financial institution establishes a risk governance framework, including a risk management team responsible for conducting regular risk assessments, identifying potential threats, and implementing controls to mitigate those risks.

Cyber Crime & Classification of Cyber Crimes

Cyber crimes involve illegal activities conducted via the internet or other digital means. They can be classified into various categories, including:

1. **Cyber Fraud:** Deceptive practices to gain financial advantage (e.g., phishing, identity theft).
2. **Cyber Espionage:** Unauthorized access to confidential information, often for political or economic gain.
3. **Cyber Terrorism:** Using digital means to disrupt, damage, or terrorize for political or ideological reasons.
4. **Cyber Vandalism:** Malicious activities aimed at disrupting services or defacing websites (e.g., DDoS attacks, defacement).

Practical Scenario: A company suffers a cyber fraud incident where attackers use phishing emails to gain access to employee accounts, stealing sensitive information. The incident is classified as cyber fraud and reported to law enforcement for investigation.

NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides guidelines for improving cybersecurity practices within organizations. It includes five core functions: Identify, Protect, Detect, Respond, and Recover.

Practical Scenario: A healthcare provider adopts the NIST Cybersecurity Framework to improve its cybersecurity posture. This includes conducting regular assessments (Identify), implementing access controls (Protect), monitoring for threats (Detect), developing an incident response plan (Respond), and establishing backup and recovery processes (Recover).

Case Studies

Case Study 1: Target Data Breach

Scenario: In 2013, Target experienced a massive data breach, exposing the credit and debit card information of over 40 million customers. The breach was caused by attackers exploiting a vulnerability in Target's network, gaining access through a third-party vendor.

Lessons Learned:

- Importance of vendor management and third-party risk assessments.
- Need for regular security assessments and vulnerability management.
- Implementation of robust incident detection and response mechanisms.

Case Study 2: Equifax Data Breach

Scenario: In 2017, Equifax suffered a data breach affecting over 147 million customers. The breach was due to an unpatched vulnerability in a web application, allowing attackers to access sensitive information, including Social Security numbers and credit card details.

Lessons Learned:

- Criticality of timely patch management and vulnerability remediation.
- Importance of data encryption and access controls.
- Need for comprehensive incident response and communication plans.

Lab Guide for Cyber Security Compliance

Lab Setup:

1. **Environment:** Virtual machines simulating a corporate network, including a domain controller, workstations, and web servers.
2. **Tools Required:**
   - Vulnerability scanning tools (e.g., Nessus, OpenVAS)
   - Compliance assessment tools (e.g., CIS-CAT, NIST CSF tools)
   - Penetration testing tools (e.g., Metasploit, Burp Suite)
   - Risk assessment tools (e.g., FAIR, OCTAVE)

Lab Activities:

1. **Compliance Assessment:**
   - Conduct a compliance assessment for GDPR, HIPAA, and PCI-DSS using automated tools.
   - Identify gaps and recommend remediation measures.
2. **Penetration Testing:**
   - Perform a penetration test on a simulated web application, following OWASP and PTES standards.
   - Identify vulnerabilities and demonstrate exploitation techniques.
3. **Risk Assessment:**
   - Conduct a risk assessment using the NIST Cybersecurity Framework.
   - Identify critical assets, potential threats, and existing controls.
   - Develop a risk treatment plan.
4. **Incident Response Simulation:**
   - Simulate a cyber incident, such as a data breach or ransomware attack.
   - Follow incident response procedures, including containment, eradication, and recovery.
   - Conduct a post-incident review and document lessons learned.