Us-Cert Incident Reporting Timelines

Introduction

The United States Computer Emergency Readiness Team (US-CERT) plays a crucial role in the nation's cybersecurity framework by providing timely and actionable information to protect against cyber threats. Reporting cyber incidents to US-CERT is essential for national security, enabling a coordinated response to mitigate and prevent further damage. This report outlines the key incident reporting timelines and requirements for organizations to comply with US-CERT guidelines.

1. Reporting Categories and Timelines

US-CERT categorizes incidents based on their severity and potential impact. Each category has specific reporting timelines to ensure prompt and appropriate responses.

1.1. Category 1: Emergency (Critical Infrastructure)

- **Definition:** Incidents that pose an immediate threat to critical infrastructure, national security, or public health and safety.
- **Reporting Timeline:** Within 1 hour of detection.
- **Examples:** Large-scale denial of service attacks, significant data breaches affecting critical infrastructure, and malware infections on systems controlling critical operations.

1.2. Category 2: Significant Incident

- **Definition:** Incidents that have a significant impact on an organization's operations or pose a substantial threat to national security or public confidence.
- **Reporting Timeline:** Within 2 hours of detection.

- **Examples:** Targeted cyberattacks on major financial institutions, widespread ransomware attacks, and breaches involving sensitive government data.

1.3. Category 3: Moderate Incident

- **Definition:** Incidents that have a moderate impact on an organization's operations but do not pose an immediate threat to national security or critical infrastructure.
- **Reporting Timeline:** Within 4 hours of detection.
- **Examples:** Unauthorized access to non-critical systems, phishing campaigns that do not result in significant data loss, and malware infections on non-critical systems.

1.4. Category 4: Minor Incident

- **Definition:** Incidents that have a minor impact on an organization's operations and do not pose a threat to national security or critical infrastructure.
- **Reporting Timeline:** Within 24 hours of detection.
- **Examples:** Low-level malware infections, unsuccessful phishing attempts, and minor data breaches involving non-sensitive information.

1.5. Category 5: Ongoing Malicious Activity

- **Definition:** Incidents involving ongoing malicious activity that has not yet caused significant damage but could escalate if not addressed.
- **Reporting Timeline:** Within 1 hour of detection.
- **Examples:** Detection of advanced persistent threats (APTs) or indicators of compromise (IOCs) suggesting a potential larger attack.

2. Reporting Process

2.1. Initial Notification

- **Content:** Initial reports should include basic information about the incident, such as the type of incident, affected systems, and initial assessment of impact.

- **Method:** Submit the report through US-CERT's online reporting portal, email, or phone.

2.2. Follow-Up Reports

- **Content:** Provide detailed information as it becomes available, including root cause analysis, mitigation actions taken, and any further impact assessment.
- **Frequency:** Continuous updates should be provided as new information is discovered and the situation evolves.

3. Legal and Regulatory Compliance

- **Federal Agencies:** Must comply with the Federal Information Security Modernization Act (FISMA) reporting requirements and coordinate with the Department of Homeland Security (DHS) and other relevant agencies.
- **Private Sector:** While reporting is generally voluntary, compliance with US-CERT guidelines can enhance an organization's cybersecurity posture and support national security efforts.

4. Best Practices

- **Preparedness:** Develop and maintain an incident response plan that includes procedures for reporting to US-CERT.
- **Training:** Regularly train employees on recognizing and reporting cyber incidents.
- **Communication:** Establish clear lines of communication with US-CERT and other relevant authorities to facilitate timely reporting and response.

Conclusion

Timely and accurate reporting of cyber incidents to US-CERT is vital for national cybersecurity. Adhering to the established timelines and processes ensures a coordinated response, minimizing the impact of cyber threats and enhancing the overall security posture of organizations and the nation.