Introduction and Structure of CERT in the Real World

By

Parnian Malekzadeh

Arefeh Pourmohammadi

Project Report for Fundamentals of Secure Computing Course

July 2024

Dr Mohammad Hossein Manshaei

ABSTRACT

The Computer Emergency Response Team (CERT) plays a critical role in the cybersecurity framework of organizations. This project report explores the origins, structure, roles, and challenges faced by CERTs in today's digital landscape. By analyzing the history and development of CERTs, we gain insights into their essential functions, such as incident handling, vulnerability mitigation, and policy implementation. Furthermore, we discuss various team and staffing models that enhance CERT effectiveness and the importance of collaboration and communication within and outside the organization. Through case studies and current model evaluations, this report aims to highlight the key aspects and challenges of CERTs in maintaining cybersecurity resilience.

Contents

Chapter 1

Introduction

A Computer Emergency Response Team (CERT), also called a Computer Security Incident Response Team (CSIRT), is a special group of information security experts. They focus on protecting, detecting, and responding to cybersecurity incidents in an organization. CERTs can work in big companies like banks or serve many organizations through commercial services. They are the first line of defense against cyber threats and work to reduce the impact of problems like data breaches and denial-of-service attacks.

The first CERT was created by the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University in 1988. Since then, CERTs have become key parts of cybersecurity for businesses, critical infrastructure, and government agencies. Their main goal is to control security incidents, reduce damage to operations and reputation, and help recover and improve systems after a crisis(Killcrece et al., 2003).

CERTs follow a model of "protect, detect, and respond." This means they take steps to secure assets before an incident, set up systems to quickly find security problems, and create plans to handle and recover from incidents. When a security breach is suspected, the CERT team evaluates the situation, checks available tools, finds signs of the breach and determines its impact. During a crisis, CERTs might suggest or use specific tools, like an agile SecOps platform such as Sekoia.io XDR, to manage the situation if the organization's own resources are compromised.

After a crisis, CERTs recommend ways to improve the organization's security, prevent future incidents, and enhance overall security. This can include better risk management, continuous monitoring for vulnerabilities, and using threat intelligence services like SEKOIA.IO CTI. By offering these services, CERTs help organizations not only handle incidents but also prevent them from happening again by continually improving their security measures (TechTarget, 2023).

The rest of this article is organized to provide a comprehensive understanding of CERTs. Chapter 2 delves into the history of CERT, tracing its origins and early developments. Chapter 3 explores the structure and organization of CERTs, detailing the various team models, staffing strategies, and collaboration mechanisms. Chapter 4 outlines the critical roles of CERTs, including identifying and responding to cyber incidents, analyzing and mitigating vulnerabilities, developing cybersecurity policies, and providing training and awareness programs. Chapter 5 discusses the incident handling process, from preparation and detection to containment, eradication, and post-incident activities. Chapter 6 presents case studie of CERT responses, illustrating real-world applications and lessons learned. Chapter 7 addresses the challenges faced by current CERT models, highlighting issues such as lack of funding, insufficient management support, and inadequate coordination mechanisms. Finally, Chapter 8 provides the conclusion, summarizing the key insights and emphasizing the importance of addressing the challenges faced by CERTs to improve their capability to respond to and mitigate cyber threats, thereby bolstering the overall security posture of the organizations they serve.

Chapter 2

History of CERT

2.1 Early Beginnings

Ideas about forming teams to handle computer security incidents and emergencies were discussed long before the Morris Worm incident in 1988. These early concepts proposed augmenting existing security management groups to protect host systems and network services. However, due to a lack of awareness and funding, these ideas were not implemented.

The Morris Worm Incident

The release of the Morris Worm in November 1988 spurred the creation of the first Computer Security Incident Response Team (CSIRT). Written by a 23-year-old college student, the worm exploited various vulnerabilities, infecting about 10% of the 60,000 to 80,000 hosts on the ARPANET (now the Internet), causing widespread disruptions.

After containing the worm, the National Computer Security Center and DARPA held meetings to discuss future prevention and response strategies. A postmortem on November 8, 1988, highlighted the need for better communication among analysis teams and timely distribution of corrective measures, noting that the lack of a formal coordination method hindered the response.

2.2 Establishment of CERT/CC

Recognizing the communication problem, DARPA decided to fund a coordination center for Internet security incidents. They chose the Software Engineering Institute (SEI) at Carnegie Mellon University to establish this center, which became the CERT Coordination Center (CERT/CC). Opening in December 1988, CERT/CC quickly began receiving incident reports. Initially staffed by personnel from other SEI programs, the team expanded to include full-time members (Cichonski et al., 2012).

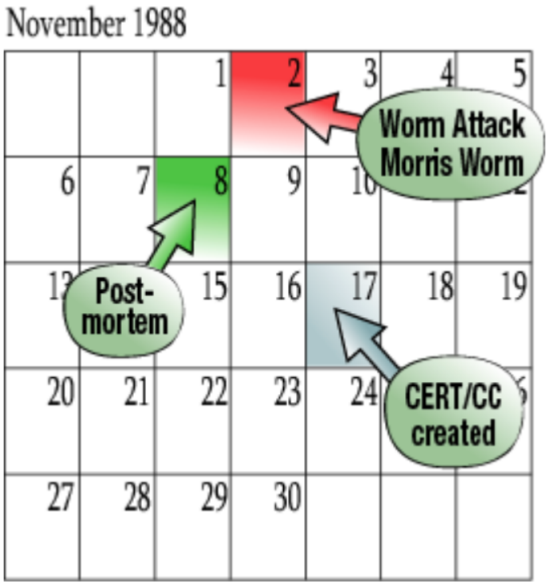

Figure 2.1: Timeline of Worm Attack and Creation of CERT/CC (Killcrece et al., 2003)

Growth of CERTs

The goal was never to have just one CERT. Following CERT/CC's model, other organizations such as the Department of Energy (DoE), NASA, NIST, and the U.S. military established their own teams to focus on their constituencies.

2.3 Creation of FIRST

In August 1989, CERT/CC organized a workshop to discuss further coordination among response teams, leading to the formation of the Forum of Incident Response and Security Teams (FIRST). This network aimed to share information, prevent incidents, and coordinate responses. By September 2003, FIRST had 151 member organizations worldwide.

European and Asia Pacific Developments

The first European CSIRT was established in France within the Space Physics Analysis Network. By the early 1990s, European research networks formed CSIRTs like CERT-NL in the Netherlands and DFN-CERT in Germany. Efforts to create a centralized European coordination center, EuroCERT, faced challenges but underscored the importance of regional cooperation.

In the Asia Pacific region, AusCERT was established in 1993, followed by teams in Korea, Japan, and Singapore. These teams formed the Asia Pacific Security Incident Response Coordination (APSIRC) Working Group, which later became APCERT, to enhance regional coordination.

United States Initiatives

In the United States, numerous CSIRTs have been established across various sectors, including military, government, education, and critical infrastructure. The U.S. Department of Homeland Security (DHS) and Carnegie Mellon University announced the formation of US-CERT in 2003 to coordinate national efforts to prevent and respond to cyber attacks (Killcrece et al., 2003).

Chapter 3

Structure and Organization of CERT

Effective incident response is crucial for any organization to handle security incidents efficiently and minimize damage. A Computer Emergency Response Team (CERT) plays a pivotal role in analyzing incidents, determining their impact, and restoring normalcy. This article delves into the structure, staffing, and communication strategies necessary for a successful CERT, supported by the organizational diagram provided.

A CERT should be accessible to anyone within the organization who discovers or suspects an incident. Depending on the incident's magnitude and personnel availability, one or more team members will manage the situation. Incident handlers are responsible for analyzing incident data, determining the impact, and taking appropriate actions to mitigate damage and restore normal services. The success of the CERT heavily depends on the cooperation and participation of individuals throughout the organization (Cichonski et al., 2012).

3.1 Team Models

The structure of a CERT can vary based on the organization's size and geographic distribution. Here are the primary models (Cichonski et al., 2012):

1. **Central CERT:**

- A single team manages incidents across the entire organization. This model is effective for smaller organizations or those with minimal geographic diversity in their computing resources. The central team handles all aspects of incident response, ensuring a unified approach and streamlined communication.

2. **Distributed CERTs:**

   - Multiple teams are responsible for different segments of the organization. This model is suitable for large organizations or those with significant geographic spread, ensuring local teams can respond promptly. Coordination among teams is crucial to maintain consistency in incident response processes and facilitate information sharing. This is particularly important as multiple teams may encounter components of the same incident or similar incidents.

3. **Coordinating CERT:**

   - This team provides advisory services to other teams without direct authority over them. For example, a department-wide team may assist individual agencies' teams. This model acts as a central hub for strategy and best practices, similar to a CERT for CERTs.

3.2 Staffing Models for CERTs

Organizations can choose from several staffing models based on their specific needs and resources (Cichonski et al., 2012):

1. **In-house Employees:**

   - All incident response activities are performed internally. This model ensures control and direct oversight but may require significant investment in training and

resources. The organization performs all of its incident response work, with limited technical and administrative support from contractors.

2. **Partially Outsourced:**

   - Combines in-house efforts with outsourced services. Common arrangements include outsourcing 24/7 monitoring of intrusion detection sensors, firewalls, and other security devices to managed security services providers (MSSPs). The MSSP identifies and analyzes suspicious activity and reports each detected incident to the organization's CERT. Some organizations perform basic incident response work in-house and call on contractors to assist with handling more serious or widespread incidents.

3. **Fully Outsourced:**

   - All incident response activities are outsourced, typically to an onsite contractor. This model is ideal for organizations that need full-time incident response capabilities but lack qualified personnel. It is assumed that the organization will have employees supervising and overseeing the outsourcer's work. A single employee, with one or more designated alternates, should be in charge of incident response. In a fully outsourced model, this person oversees and evaluates the outsourcer's work.

3.3 Collaboration and Support

A CERT's success depends on collaboration with various internal and external groups. Internally, key collaborators include (Cichonski et al., 2012):

- **Management:** Establishes incident response policy, budget, and staffing. Management is held responsible for coordinating incident response among various

stakeholders, minimizing damage, and reporting to Congress, the Office of Management and Budget (OMB), the General Accounting Office (GAO), and other parties.

- **Information Assurance:** Information security staff members may be needed during certain stages of incident handling to alter network security controls, such as firewall rulesets.
- **IT Support:** IT technical experts, such as system and network administrators, assist with their skills and understanding of the technology they manage daily. This understanding ensures appropriate actions for the affected systems.
- **Legal Department:** Reviews incident response plans for compliance with laws and federal guidance, including the right to privacy. Legal experts guide on legal ramifications, evidence collection, prosecution of suspects, or lawsuits.
- **Public Affairs and Media Relations:** Manages media communications to ensure consistent and accurate information dissemination, adhering to the organization's policies on media interaction and information disclosure.
- **Human Resources:** Assists with disciplinary actions if an employee is involved in an incident.
- **Business Continuity Planning:** Ensures incident response aligns with business continuity processes. Incident handlers should communicate impacts to business continuity planners to fine-tune business impact assessments, risk assessments, and continuity of operations plans.
- **Physical Security and Facilities Management:** Provides access to facilities and manages physical security breaches, coordinating logical and physical attacks if necessary.

3.4 Communication with Outside Parties

Effective communication with external parties is crucial for incident response. Organizations should establish clear procedures for interacting with the following groups (Cichonski et al., 2012):

- **Media:** Designate media contacts, train them to handle inquiries, and ensure consistent messaging. Establish media communication procedures that comply with the organization's policies on media interaction and information disclosure.
- **Law Enforcement:** Establish relationships with law enforcement agencies, understand reporting procedures, and avoid jurisdictional conflicts. The CERT should become acquainted with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them.
- **Incident Reporting Organizations:** Report incidents to entities like US-CERT and ensure compliance with reporting requirements. FISMA requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT).
- **Other Outside Parties:** Coordinate with ISPs, software vendors, other incident response teams, and affected external parties. An organization may want to discuss incidents with other groups, including Internet service providers, owners of attacking addresses, software vendors, other incident response teams, and affected external parties.

3.5 Types of CERTs

CERTs can be classified into several types based on their scope, affiliation, and the entities they serve. The main types of CERTs include:

Figure 3.1: Communications with Outside Parties (Cichonski et al., 2012).

(a) **National CERTs:** These are established by governments to protect national critical infrastructure and respond to large-scale cyber threats. National CERTs often coordinate with other national and international cybersecurity agencies to address threats that cross borders. Examples include the United States Computer Emergency Readiness Team (US-CERT) and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).

(b) **Government CERTs:** These CERTs are focused on protecting government agencies and their digital assets. They work to secure sensitive government information and systems from cyber threats. An example is the UK National Cyber Security Centre (NCSC), which provides cybersecurity support to the UK government.

(c) **Academic CERTs:** These CERTs operate within academic institutions, protecting the information systems and networks of universities and research centers. They also contribute to cybersecurity research and education. Examples include the University of California, Berkeley's Information Security and Policy Office, and the Georgia Tech Information Security Center (GTISC).

(d) **Private Sector CERTs:** Established by private companies, these CERTs focus on protecting corporate networks, systems, and data. They handle incidents that impact the business operations of the company and work to safeguard intellectual property and customer information. Examples include Microsoft's Digital Crimes Unit (DCU) and IBM's X-Force Incident Response and Intelligence Services (IRIS).

(e) **Sectoral CERTs:** These CERTs serve specific sectors such as finance, healthcare, or energy. They address the unique cybersecurity challenges and regulatory requirements of their respective sectors. Examples include the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Energy Sector Security Consortium (EnergySec).

Chapter 4

Roles of CERT

CERTs (Computer Emergency Response Teams) play a critical role in maintaining the security and resilience of an organization's networks and systems. Their specific tasks and responsibilities in network management include identifying and responding to cyber incidents, analyzing and mitigating vulnerabilities, developing and implementing cybersecurity policies and procedures, and providing cybersecurity training and awareness. Each of these roles is expanded below to provide a comprehensive understanding of CERTs' functions.

4.1 Identifying and Responding to Cyber Incidents

One of the primary roles of CERTs is to identify and respond to cyber incidents. This involves continuous monitoring of the organization's networks and systems to detect signs of cyber attacks, such as unusual network traffic, unauthorized access attempts, or malware infections. CERTs use a variety of tools and techniques, including intrusion detection systems (IDS), security information and event management (SIEM) systems, and threat intelligence feeds to stay alert to potential threats.

When an incident is detected, CERT coordinates the response efforts. This may involve isolating affected systems to prevent the spread of the attack, conducting forensic analysis to understand the scope and nature of the incident, and restoring systems and data from backups. In addition, CERTs work closely with other teams and stakeholders, such as IT departments, legal teams, and external partners, to manage the incident's

impact and ensure a coordinated response. Communication is key during this process, as timely and accurate information sharing can help mitigate the incident's effects and prevent future occurrences.

CERTs also document each incident thoroughly, detailing the actions taken, the lessons learned, and any improvements that can be made to the incident response process. This documentation is essential for refining response strategies and enhancing the organization's overall cybersecurity posture.

4.2 Analyzing and Mitigating Vulnerabilities

Another crucial responsibility of CERTs is to analyze and mitigate vulnerabilities within the organization's networks and systems. This involves staying up-to-date with the latest cyber threats and vulnerabilities by monitoring security advisories, threat intelligence reports, and vulnerability databases. CERTs perform regular vulnerability assessments and penetration testing to identify potential weaknesses in the organization's infrastructure.

Once vulnerabilities are identified, CERTs provide guidance on how to mitigate or eliminate them. This may involve applying patches, reconfiguring systems, or implementing additional security controls. CERTs also issue alerts and advisories to inform relevant stakeholders about new threats and recommended countermeasures. These advisories often include detailed information on the nature of the threat, its potential impact, and steps that can be taken to protect against it.

Coordination with other organizations and agencies is also a key aspect of this role. CERTs often participate in information-sharing initiatives and collaborate with industry peers, government agencies, and cybersecurity communities to develop and implement effective countermeasures against emerging threats. This collaborative approach helps enhance the overall security posture of not just the organization, but the broader

ecosystem in which it operates.

4.3 Developing and Implementing Cybersecurity Policies and Procedures

CERTs play a vital role in developing and implementing cybersecurity policies and procedures. They work closely with other teams and stakeholders to establish a comprehensive framework for protecting the organization against cyber threats. This involves setting standards and guidelines for secure network design and configuration, as well as developing security controls and protocols tailored to the organization's specific needs and risk profile.

Developing cybersecurity policies includes defining roles and responsibilities, establishing incident response procedures, and outlining acceptable use policies for network and system resources. CERTs ensure that these policies are aligned with industry best practices and regulatory requirements, providing a robust foundation for the organization's cybersecurity strategy.

Implementation of these policies requires collaboration with various departments, including IT, legal, and human resources. CERTs conduct regular audits and assessments to ensure compliance with established policies and identify areas for improvement. They also facilitate the integration of security measures into the organization's daily operations, promoting a culture of cybersecurity awareness and vigilance.

In addition to policy development and implementation, CERTs continuously review and update policies to adapt to the evolving threat landscape. This proactive approach ensures that the organization remains resilient against new and emerging cyber threats.

4.4 Providing Cybersecurity Training and Awareness

A critical component of CERTs' responsibilities is providing cybersecurity training and awareness programs. These programs aim to educate employees and other stakeholders about the importance of cybersecurity and equip them with the knowledge and skills needed to manage cyber risks effectively.

CERTs develop and deliver a variety of educational materials and programs, including online courses, workshops, seminars, and interactive training sessions. These programs cover topics such as recognizing phishing attempts, securing personal and corporate devices, using strong passwords, and understanding the organization's cybersecurity policies and procedures.

Promoting best practices and guidelines for cybersecurity is also an essential aspect of CERTs' training efforts. They create awareness campaigns to highlight current threats and vulnerabilities, providing practical advice on how to stay safe online. These campaigns often use multiple communication channels, such as email newsletters, intranet portals, and social media, to reach a wide audience.

In addition to employee training, CERTs may also engage with external partners and customers to raise awareness about cybersecurity issues and promote a unified approach to managing cyber risks. This external outreach can include hosting public webinars, participating in industry conferences, and contributing to community initiatives focused on cybersecurity education.

By fostering a culture of cybersecurity awareness, CERTs help ensure that all members of the organization understand their role in protecting the organization's information assets and are prepared to respond effectively to potential cyber threats (GeeksforGeeks, 2024).

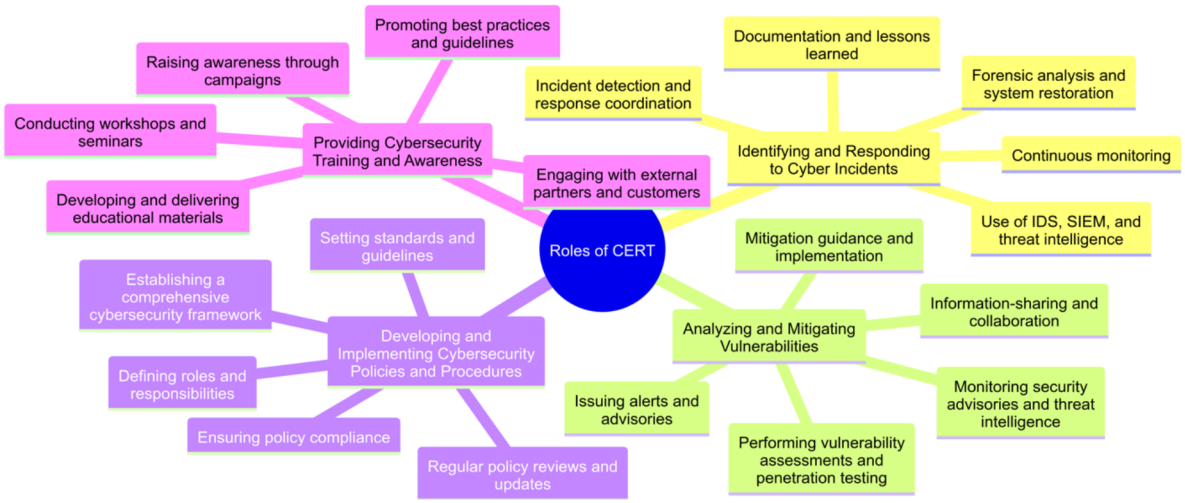

Figure 4.1: Roles of CERT

Chapter 5

Handling an Incident

The incident response process involves several key phases. Initially, organizations prepare by establishing and training an incident response team and acquiring the necessary tools and resources. During this phase, they implement controls based on risk assessments to reduce the number of incidents, though some residual risk remains. Detection and analysis are critical for identifying security breaches and understanding their severity. Depending on the incident's severity, the organization can contain and recover from it, often cycling back to detection to check for further issues, such as additional malware infections. Finally, a post-incident report is issued, detailing the cause, cost, and preventative measures for future incidents (Cichonski et al., 2012).

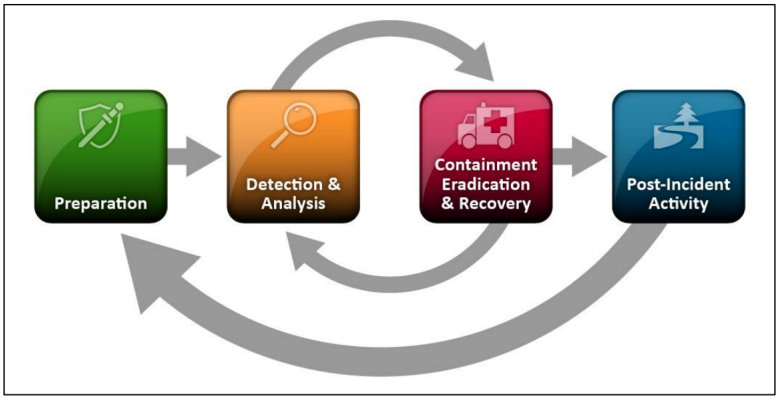

Figure 5.1: Incident Response Life Cycle (Cichonski et al., 2012)

5.1 Preparation

Incident response methodologies emphasize preparation, involving the establishment of an incident response capability and securing systems, networks, and applications. Although incident prevention is typically not the responsibility of the incident response team, it is fundamental to the success of incident response programs. Preparation includes equipping the team with tools and resources necessary for handling incidents, such as communication devices, encryption software, digital forensic workstations, laptops, backup devices, and various incident analysis software. Organizations should have multiple communication mechanisms and a "jump kit" for quick deployment during investigations (Cichonski et al., 2012).

Preparing to Handle Incidents

The incident response team should have access to various tools and resources, including up-to-date contact information, on-call schedules, incident reporting mechanisms, and issue tracking systems. Communication tools like smartphones and encryption software are vital for secure communications. Incident analysis tools such as digital forensic workstations, packet sniffers, and forensic software help gather and analyze evidence. Spare hardware, blank media, portable printers, and evidence gathering accessories facilitate efficient incident handling.

Incident Analysis Resources

Incident handlers should have access to resources like port lists, OS documentation, network diagrams, and baselines of expected network activity. Cryptographic hashes of critical files speed up incident analysis and verification. Clean OS images and application installations are crucial for restoring systems after an incident.

Preventing Incidents

To minimize incidents, organizations should implement robust security controls. Regular risk assessments help identify and prioritize risks for mitigation. Hosts should be properly configured and continuously monitored, following the principle of least privilege. Network security should enforce denial of unauthorized activities. Malware prevention software should be deployed across all levels, including hosts, servers, and client applications. User awareness and training programs educate users about security policies, reducing the frequency of incidents. Sharing lessons learned from past incidents helps users understand the impact of their actions on organizational security.

5.2 Detection and Analysis

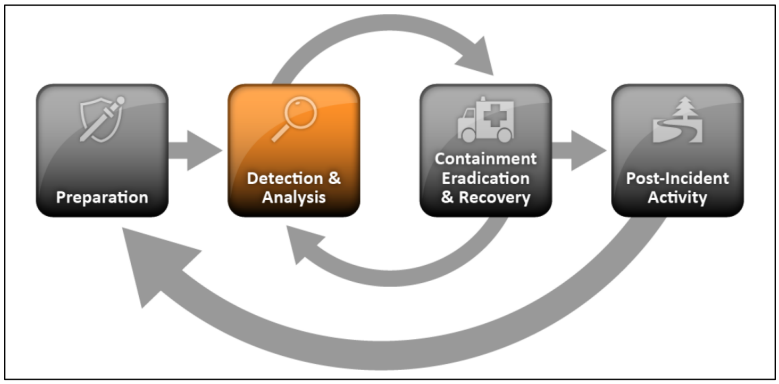

Figure 5.2: Incident Response Life Cycle (Detection and Analysis) (Cichonski et al., 2012)

Attack Vectors and Incident Handling

Incidents can occur through various attack vectors, making specific instructions for every scenario impractical. Organizations should be prepared for any incident but focus on common vectors like external media, brute force, web-based attacks, email-

based attacks, impersonation, improper usage, and equipment loss/theft. Each type requires different response strategies (Cichonski et al., 2012).

Signs of an Incident

Detecting incidents is challenging due to numerous detection methods and potential signs, such as IDPS alerts, antivirus software, and user reports. Indicators can be precursors (signs that an incident may occur) or actual signs (an incident is occurring or has occurred). Precursors include web server vulnerability scans and new exploit announcements. Indicators include intrusion detection alerts, unusual log entries, failed login attempts, and abnormal network traffic.

Sources of Precursors and Indicators

Sources include alerts from IDPS, SIEMs, antivirus software, and logs from operating systems, network devices, and applications. Public information on vulnerabilities and reports from internal and external parties also provide valuable insights. Correlating data from multiple sources is essential for effective incident detection.

Incident Analysis

Incident analysis involves evaluating indicators to determine legitimacy, despite challenges like false positives and numerous indicators. Effective analysis includes profiling networks, understanding normal behaviors, maintaining log retention, performing event correlation, synchronizing host clocks, keeping a knowledge base, and using search engines and packet sniffers. Filtering data and seeking assistance are also essential strategies.

Incident Documentation

From the moment an incident is suspected, document all relevant facts, including system events, conversations, and observed changes. Use a logbook or digital means for documentation. All actions should be timestamped and signed by the incident handler. Maintain records securely, restricted to authorized personnel, with information logged in an issue tracking system detailing status, summary, indicators, actions taken, and evidence gathered.

Incident Prioritization

Prioritize incidents based on impact and recovery effort, considering functional impact, information impact (confidentiality, integrity, availability), and recoverability effort. Handle incidents based on these factors, not on a first-come, first-served basis. Establish an escalation process for timely responses if initial contact fails.

Incident Notification

After analysis and prioritization, notify relevant parties, including the CIO, head of information security, local security officers, system owners, HR, public affairs, legal department, US-CERT, and law enforcement if necessary. Provide status updates during handling and prepare multiple communication methods, including email, internal websites, telephone calls, and in-person briefings, for effective communication.

5.3 Containment, Eradication, and Recovery

Choosing a Containment Strategy

Containment is crucial to prevent incidents from escalating. It allows time for remediation and involves decisions like shutting down or disconnecting systems. Predetermined strategies based on acceptable risks and incident types make these decisions easier. Criteria for strategy selection include potential damage, evidence preservation, service availability, resource requirements, effectiveness, and duration. Using a sandbox to monitor attackers can be considered but must be legally vetted.

Evidence Gathering and Handling

Evidence gathering is essential for incident resolution and legal proceedings. Proper documentation and preservation, including chain of custody records, are critical. Evidence should be collected according to legal standards to ensure court admissibility. Key information includes identifying details, handling individuals, and timestamps. Early evidence collection, like system snapshots, captures the state before changes

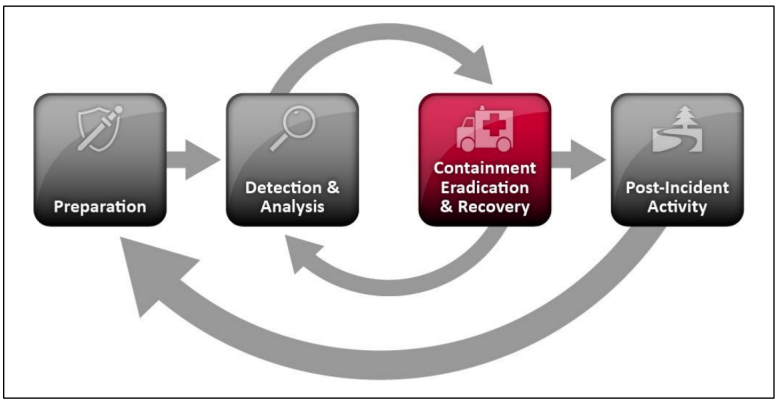

Figure 5.3: Incident Response Life Cycle (Containment, Eradication, and Recovery) (Cichonski et al., 2012)

occur. Training users and administrators in evidence preservation is important.

Identifying the Attacking Hosts

Identifying attacking hosts is important but secondary to containment and recovery. Methods include validating IP addresses, researching via search engines, using incident databases, and monitoring communication channels. Treat information from these sources as leads, not definitive facts.

Eradication and Recovery

Eradication involves removing incident components and addressing vulnerabilities. Identifying all affected hosts is crucial. Recovery restores systems to normal operations, ensures functionality, and prevents recurrence by applying patches, changing passwords, and enhancing security. This may involve restoring from backups, rebuilding systems, or tightening network security. Higher logging and monitoring levels are often implemented. Phased eradication and recovery prioritize quick, high-value changes to improve security, with longer-term changes following.

5.4 Post-Incident Activity

Lessons Learned

Incident response teams must evolve continuously. Hold "lessons learned" meetings after major incidents to review timelines, performance, procedures, and improvements. Document outcomes for future reference and update policies. Comprehensive records support immediate and future responses.

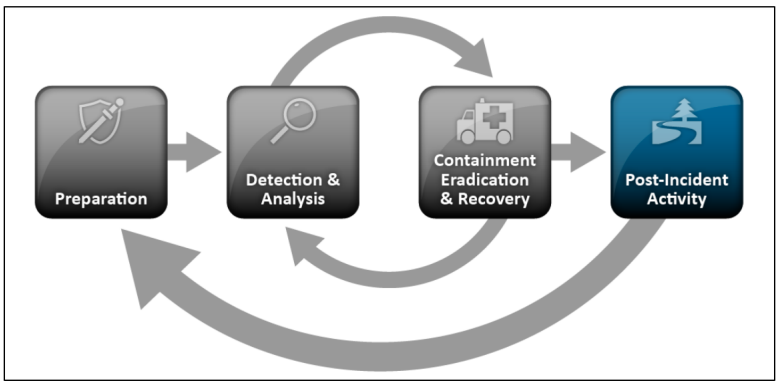

Figure 5.4: Incident Response Life Cycle (Post-Incident Activity) (Cichonski et al., 2012)

Using Collected Incident Data

Collected data justifies funding and identifies weaknesses. Track metrics like incident count, labor hours, and phase durations. Assess documentation, precursors, indicators, and damage. Use audits to refine incident response programs continuously.

Evidence Retention

Develop policies for retaining evidence, considering prosecution timelines and data retention policies. Balance storage costs and maintain functional equipment for accessing evidence.

5.5 Incident Handling Checklist

Manage incidents by analyzing indicators, documenting evidence, prioritizing response, and reporting. Contain, eradicate, and recover by securing evidence, addressing vulnerabilities, and restoring systems. Follow up with reports and lessons learned meetings.

5.6 Recommendations

Acquire necessary tools, prevent incidents with secure systems, identify indicators, and establish reporting mechanisms. Enforce logging, profile behaviors, and maintain documentation. Prioritize incidents and handle evidence properly. Use lessons learned meetings to improve security measures (Cichonski et al., 2012).

Chapter 6

Case Studie of CERT Responses

Show Me the Money

In early January, an attacker exploited a SQL injection vulnerability on a web page hosted on WEB1, located in a DMZ of a small business unit acquired by the victim organization. This unit had full connectivity to the organization's environment. By exploiting the SQL injection vulnerability, the attacker executed commands on DB1 with local administrator privileges using the 'xp_cmdshell' extended stored procedure to download and execute malware. A firewall misconfiguration allowed the attacker to execute SQL commands against 'intDB1', a database server within the corporate environment. Over the next few weeks, the attacker conducted reconnaissance, implanted a backdoor, and cracked the password hash for the local administrator account on 'intDB1', gaining administrative access to most systems. They installed keystroke-logging malware and extracted password hashes from multiple systems, including a domain controller.

By mid-February, the attacker had implanted over 20 backdoors from three malware families: BKDOOR, PROXY, and BKDNS. BKDOOR allowed full control of victim systems, PROXY redirected connections, and BKDNS tunneled C2 traffic through DNS queries/responses. The attacker stole data, including usernames, passwords, network architecture, and financial systems data, by exploring system administrators' files and establishing RDP connections with stolen credentials.

By June, the attacker discovered the jump server (JMPSRV) used by system adminis-

trators to access the restricted network handling sensitive financial data. They monitored RDP connections and reviewed keystroke logger output, identifying systems processing or storing cardholder data. Using stolen documents and reconnaissance, the attacker found 90 such systems and installed BKDOOR malware on five systems in the financial environment. They configured PROXY malware on JMPSRV to communicate with another PROXY instance on the primary mail exchanger (MAIL), which had direct Internet access. Over three months, the attacker captured millions of instances of cardholder data from all 90 systems, transferring data out using BKDOOR malware.

After roughly 10 months, a system administrator discovered abnormal TCP port 80 communication from MAIL to a foreign IP address, prompting an incident response. The response involved immediate containment, comprehensive investigation, and eradication to remove the attacker from the environment, taking less than two months.

The incident response faced numerous challenges, including searching for indicators of compromise across all systems, analyzing multiple operating systems, investigating network traffic, and understanding complex financial systems. The remediation team implemented an immediate containment plan, developed a comprehensive remediation approach, and executed a sweeping eradication event. This case study demonstrates the need for robust incident detection and response capabilities, continuous monitoring, and comprehensive security measures to protect sensitive financial data from sophisticated attackers (Luttgens and Pepe, 2014).

Chapter 7

Challenges in Current CERT Models

CERTs face various challenges that can hinder their effectiveness, frequently discussed in academic settings, conferences, and professional venues. Key challenges include lack of funding, insufficient management support, a shortage of trained incident handling staff, poorly defined missions and authority, and inadequate coordination mechanisms (Killcrece et al., 2003).

Common Challenges

(a) **Lack of Funding:** Insufficient financial resources limit the acquisition of necessary tools, hiring skilled staff, and maintaining operations.

(b) **Lack of Management Support:** Difficulty in gaining support from upper management, making it hard to implement necessary security measures and response procedures.

(c) **Shortage of Trained Staff:** Difficulty in finding and retaining qualified personnel, requiring continuous training and development.

(d) **Poorly Defined Mission and Authority:** Lack of clear missions and authority leads to confusion and inefficiency, requiring well-defined mission statements.

(e) **Inadequate Coordination Mechanisms:** Effective incident response requires seamless coordination among units, CSIRTs, and sites, with challenges in collaboration and information sharing.

Chapter 8

Conclusion

CERTs face various challenges that can hinder their effectiveness, frequently discussed in academic settings, conferences, and professional venues. Key challenges include lack of funding, insufficient management support, a shortage of trained incident handling staff, poorly defined missions and authority, and inadequate coordination mechanisms. Addressing these issues requires a concerted effort to secure financial resources, gain management backing, recruit and retain skilled personnel, clearly define roles and responsibilities, and enhance coordination and information sharing among different units and organizations. By overcoming these challenges, CERTs can significantly improve their capability to respond to and mitigate cyber threats, thereby bolstering the overall security posture of the organizations they serve.

References

Cichonski, Paul et al. (Aug. 2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. Recommendations of the National Institute of Standards and Technology, Department of Homeland Security, and Scarfone Cybersecurity. Gaithersburg, MD: National Institute of Standards and Technology.

GeeksforGeeks (2024). *Computer Emergency Response Team (CERT)*. Accessed: 2024-07-04. URL: https://www.geeksforgeeks.org/computer-emergency-response-team-cert/.

Killcrece, Georgia et al. (Oct. 2003). *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon University: CMU/SEI-2003-TR-001, ESC-TR-2003-001, Networked Systems Survivability Program.

Luttgens, J.T. and M. Pepe (2014). *Incident Response & Computer Forensics*. 3rd. New York, NY, USA: McGraw-Hill.

TechTarget (2023). *CERT (Computer Emergency Readiness Team)*. Accessed: 2024-07-05. URL: https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team.