Cybersecurity Basics 1 (incident response)

Incident Response Plan for Phishing Incident

1. Introduction

This incident response plan is designed to address a **phishing attack** and outlines the steps to detect, contain, eradicate, and recover from such incidents. The plan references notable phishing incidents, such as the **FACC (€42 Million)** and **Crelan Bank (€75.6 Million)** cases, where attackers impersonated high-level executives to deceive employees into transferring funds.

---

2. Phishing: An Overview

Phishing is a cyberattack where attackers impersonate legitimate entities to trick individuals into divulging sensitive information or performing unauthorized actions. In these incidents, phishing emails are used to manipulate employees into transferring large sums of money to fraudulent accounts.

Phishing in the FACC Incident (January 2016):

- **Attack Method:** An employee received an email appearing to be from the CEO, instructing them to transfer €42 million for an “acquisition project.”

- **Impact:** The employee complied and transferred the money, leading to a €42 million loss for FACC.

Phishing in the Crelan Bank Incident (February 2016):

- **Attack Method:** A similar phishing scam occurred when the attacker spoofed the bank's CEO and tricked an employee into transferring funds.

- **Impact:** The total damage, including remediation costs, amounted to €75.6 million.

Phishing in the Sony Pictures Incident (November 2014):

- **Attack Method:** The attackers sent phishing emails to Sony executives that appeared to be from Apple, asking for ID verification. This led to a significant data breach.

- **Impact:** The damage included the loss of 100 terabytes of data, the deletion of Sony's infrastructure via wiper malware, and financial losses of more than €80 million.

---

3. Detection of Phishing Incident

Method: Email Filtering and User Reporting

- **Automated Detection Systems:**

    - Implement advanced **email filtering** tools (e.g., Proofpoint, Microsoft Defender) to flag emails that contain suspicious attachments, URLs, or mismatched sender addresses. These tools can also analyze the content of emails to detect phishing attempts.

    - Use **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** to authenticate the legitimacy of incoming emails and detect spoofed emails.

- **User-Driven Detection:**

    - **Phishing Simulations:** Regularly test employees with simulated phishing emails to train them to recognize potential threats.

    - **Reporting Mechanism:** Create an easy process for employees to report suspicious emails, especially those that seem to come from senior executives or involve urgent requests.

    - **Training Programs:** Ensure employees are aware of the common tactics used in phishing attacks, such as requests for financial transactions or sensitive data.

---

4. Containment Strategy

Strategy: Immediate Isolation and Access Controls

- **Immediate Isolation of Affected Systems:**
    - If a phishing email leads to a compromised account or financial transaction, immediately isolate the affected system or account from the network. Disconnect the device from the internet and internal network to prevent further damage.
    - Disable the user account that may have been used to initiate the fraudulent transaction (e.g., the employee who transferred funds).
- **Communication and Transparency:**
    - Notify all relevant internal stakeholders (e.g., IT, legal, finance) about the breach, especially if financial transactions were involved.
    - Block external communication from suspicious email addresses or domains to prevent further phishing attempts.
- **Containment of Funds or Transfers:**
    - Contact financial institutions and involved third parties (banks) to reverse or stop any unauthorized transactions.
    - Trace and flag suspicious accounts that may have received funds, and work with law enforcement to freeze the accounts if possible.

---

5. Eradication of the Threat

Steps for Eradication:

- **Remove Malicious Emails and Content:**
    - Use email filtering systems to delete any malicious emails from all employee inboxes that contain phishing links, attachments, or spoofed domains.

    - Investigate any systems that interacted with phishing emails to ensure malware or scripts were not executed.

- **Credentials Reset and Authentication:**

    - Immediately **reset passwords** for affected employees and any accounts that may have been compromised, especially accounts with access to sensitive financial information.

    - **Enable Multi-Factor Authentication (MFA)** for all employees to add an additional layer of security and prevent unauthorized access.

- **Review of Access Logs and Systems:**

    - Conduct a thorough review of **access logs** to identify any unusual or unauthorized activities (e.g., logins from suspicious IP addresses).

    - Check for malware or spyware installed as a result of the phishing attack and use anti-malware tools to fully clean the affected systems.

---

6. Recovery and Restoration

Steps for Recovery:

- **Restore Systems and Data:**

    - If any systems were compromised, **restore them from secure backups** that have not been affected by the phishing attack. Ensure that all backups are scanned for any signs of infection.

    - Rebuild any systems or configurations that were affected by the phishing attack or subsequent malware infection.

- **Monitor for Recurrence:**

    - Set up alerts for any unusual activities that could signal the return of malicious actors. Monitor both internal and external communication channels for any signs of follow-up attacks.

    - Ensure that email filtering tools and threat detection systems are optimized to block phishing attempts in real-time.

- **Post-Incident Review:**
    - Conduct a thorough post-incident analysis to determine how the phishing attack occurred and identify areas where security policies may need improvement.
    - Evaluate employee training effectiveness and enhance phishing detection systems.
- **Reinforce Security Protocols:**
    - Based on the findings from the post-incident review, implement changes to strengthen security, such as:
        - **Enhanced Email Security Measures:** Configure email servers with stronger anti-phishing and anti-spoofing tools.
        - **Improved Employee Awareness:** Update employee training to reflect the latest phishing techniques and reinforce reporting procedures.

---

7. Conclusion

Phishing remains one of the most prevalent cyber threats, as evidenced by the significant financial losses experienced by organizations like FACC, Crelan Bank, and Sony Pictures. By following a structured incident response plan that emphasizes detection, containment, eradication, and recovery, organizations can mitigate the damage caused by phishing attacks and reduce the likelihood of future incidents. Ongoing employee education, robust security tools, and clear communication channels are critical components of an effective defense against phishing.

Security Policy

Certainly! Below is a **Security Policy Document** that outlines key **security rules/guidelines**, an **incident response plan**, and an explanation of how these policies and procedures maintain the **CIA Triad (Confidentiality, Integrity, Availability)**.

Security Policy Document: Phishing Incident Response and Protection

1. Introduction

This security policy document provides a framework for preventing, detecting, and responding to phishing attacks. Given the significant impact of phishing incidents on organizations (e.g., FACC, Crelan Bank, and Sony Pictures), the policy is designed to safeguard against phishing attempts, protect sensitive information, and ensure business continuity.

---

2. Key Security Rules/Guidelines

Rule 1: Email Security and Authentication

- **Guideline:** All incoming emails, particularly those requesting sensitive data or financial transactions, must be thoroughly verified before acting upon. This includes checking the email address, verifying URLs (hovering over links), and confirming the legitimacy of any unusual requests.

- **Policy:** Employees must use multi-factor authentication (MFA) for accessing email systems, especially for accounts with access to financial systems or sensitive data.

- **Training:** Employees will undergo regular phishing awareness training to recognize and report suspicious emails.

Rule 2: Segregation of Duties and Financial Transactions

- **Guideline:** Any financial transaction requests received via email must follow a strict verification process. No single individual should have sole authority over critical financial transactions.

- **Policy:** Financial transaction requests must be confirmed through an independent, non-email communication channel (e.g., phone call or in-person) with the requesting executive. No wire transfers exceeding €100,000 can be processed without multiple layers of confirmation.

- **Compliance:** A system of checks and balances will be in place to ensure that requests for large financial transfers are legitimate.

Rule 3: Incident Reporting and Response

- **Guideline:** Employees are required to immediately report any suspicious email, transaction request, or breach to the designated IT/security personnel.

- **Policy:** A dedicated incident response team (IRT) will be available 24/7 to address any security incidents. Employees must report phishing attempts, even if they appear to be unsuccessful, as soon as possible.

- **Compliance:** A secure and anonymous reporting mechanism will be established to allow employees to report phishing attempts without fear of retribution.

---

3. Incident Response Plan for Phishing Attacks

In case of a phishing incident, the following **Incident Response Plan** must be followed to contain, eradicate, and recover from the attack:

Step 1: Detection

- **Automated Tools:** Utilize email filtering systems (e.g., Proofpoint, Mimecast) to flag suspicious emails based on known phishing patterns (e.g., spoofed addresses, strange attachments, suspicious URLs).

- **Employee Reporting:** Employees must immediately report suspicious emails to the IT/security team via the established reporting mechanism.

- **Initial Assessment:** The IT team will quickly assess the reported phishing email to verify if the organization's systems have been compromised.

Step 2: Containment

- **Isolate Affected Systems:** Any compromised system or account must be disconnected from the network to prevent further spread of malware or unauthorized access.

- **Block Malicious Domains:** Use DNS filtering to block known malicious domains and stop any further attempts by the attacker to interact with the network.

- **Access Control:** Change credentials for any affected accounts, especially those involved in sensitive transactions. Implement MFA on all sensitive accounts.

Step 3: Eradication

- **System Cleanup:** Run full anti-malware scans on all affected systems to remove any malicious software or files.

- **Reset Accounts:** Reset passwords for all affected accounts and ensure that these passwords meet strong security requirements (e.g., length, complexity).

- **Patch Vulnerabilities:** If the phishing attack exploited any system vulnerabilities, patches and updates should be immediately applied to prevent re-exploitation.

Step 4: Recovery

- **Restore from Backups:** If systems were compromised, restore affected systems from clean backups. Ensure that these backups were not affected by the phishing attack.

- **Monitor Systems:** After recovery, continuously monitor the system for signs of reoccurrence of the phishing attack or any unusual activities (e.g., unexpected logins, unapproved transactions).

- **Post-Incident Review:** Conduct a thorough post-incident review to determine the root cause, assess the damage, and improve the organization's defenses against future attacks.

---

4. How These Policies Maintain the CIA Triad

The policies and procedures outlined in this document are designed to maintain and enhance the **CIA Triad**—**Confidentiality, Integrity, and Availability**—which are fundamental principles of information security.

Confidentiality

- **Preventing Data Leakage:** By enforcing strong email authentication measures (e.g., DMARC, SPF, DKIM) and multi-factor authentication (MFA), the risk of unauthorized access to sensitive data is minimized. Employees are trained to recognize phishing attempts that could compromise confidential information (such as credentials or financial data).

- **Access Controls:** Segregation of duties ensures that no single employee has unchecked access to sensitive systems, particularly financial accounts, reducing the risk of confidential data being leaked.

Integrity

- **Ensuring Data Accuracy:** The guideline requiring financial transactions to be independently verified before being processed ensures that only legitimate, authorized transfers are executed, maintaining the integrity of the organization's financial data.

- **Preventing Data Manipulation:** The incident response plan includes steps to identify and remove malware that could alter system data or transaction records. Continuous monitoring ensures the integrity of the organization's systems and prevents unauthorized alterations.

Availability

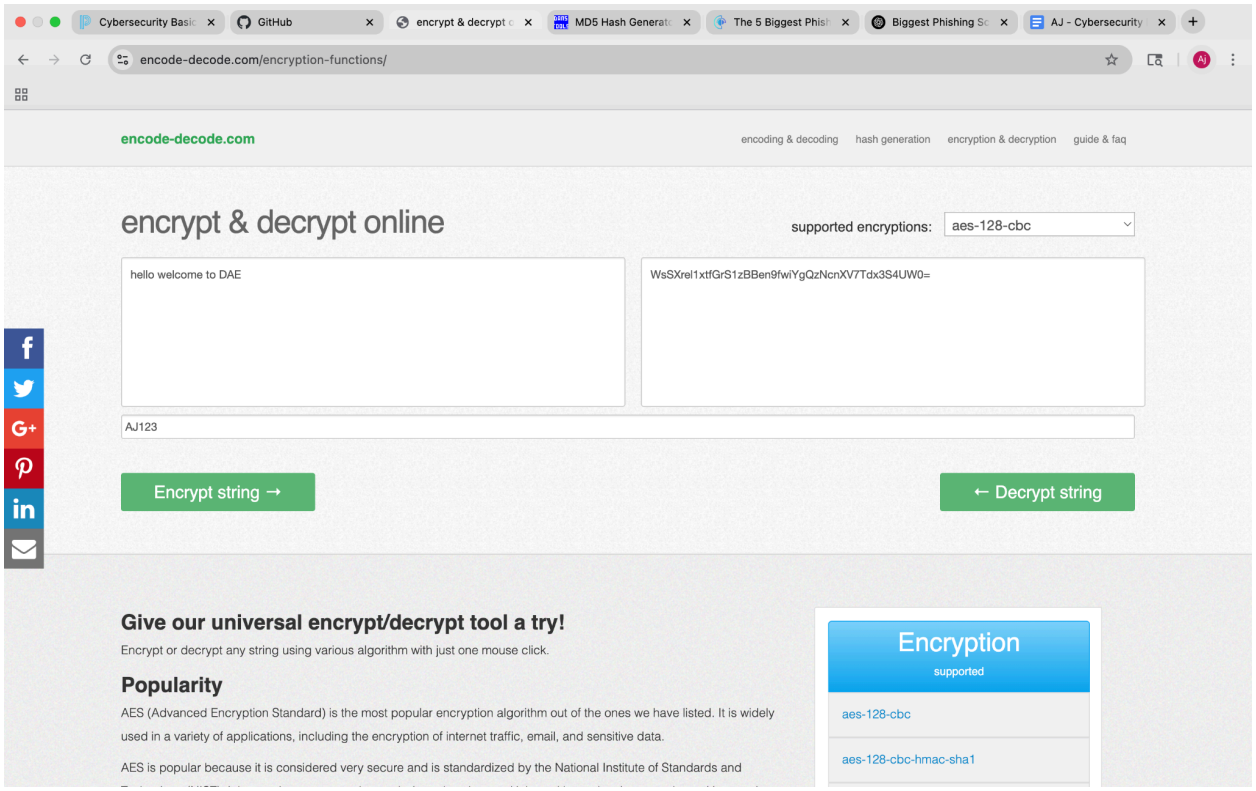
- **Ensuring Continuity of Operations:** By isolating affected systems and restoring from backups, the organization ensures that business operations can continue with minimal disruption. The incident response plan includes rapid containment and recovery steps to restore services in case of a breach.

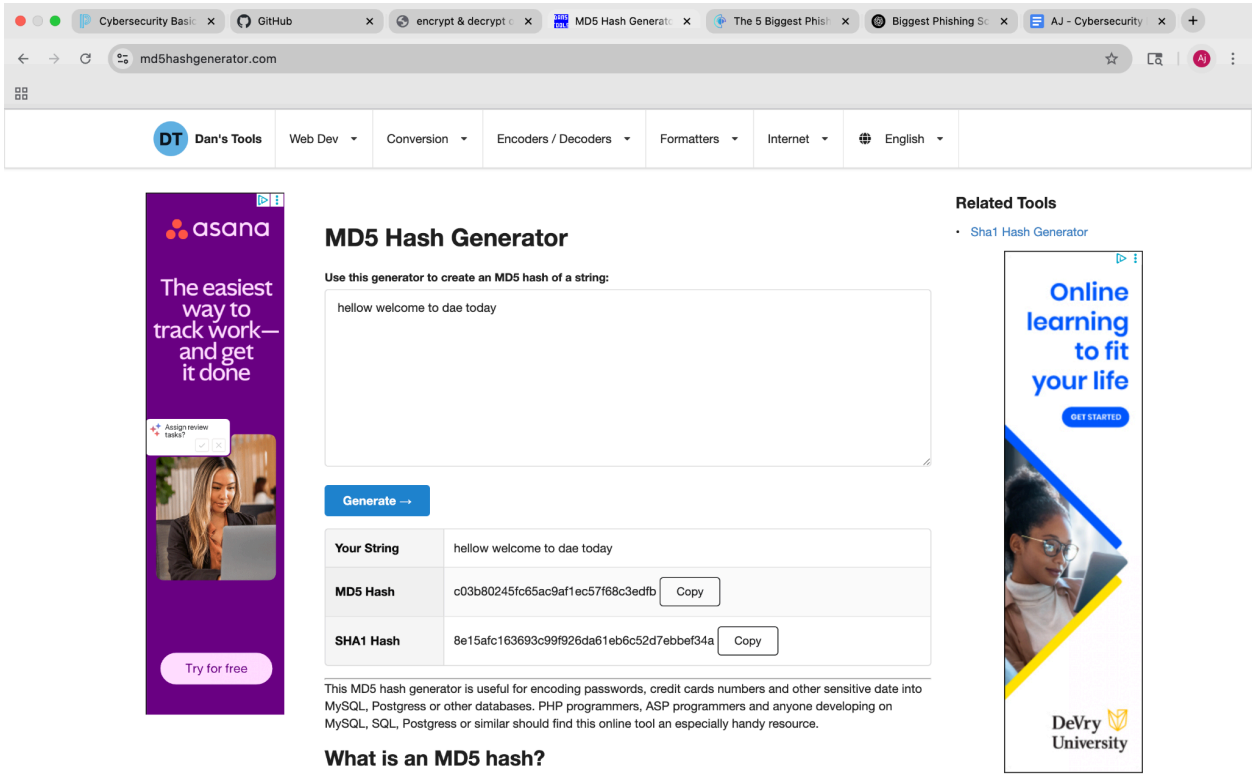
- **Business Resilience:** By implementing a robust reporting and response mechanism, the organization can quickly detect and mitigate phishing incidents, reducing downtime and ensuring that critical business processes are available without prolonged interruptions.

5. Conclusion

This **Security Policy Document** outlines essential rules and guidelines, along with a detailed **incident response plan**, to effectively detect, contain, and recover from phishing attacks. By adhering to these security policies, the organization ensures that the principles of the **CIA Triad**—Confidentiality, Integrity, and Availability—are upheld, and the risks associated with phishing are minimized. The implementation of these security practices is crucial in maintaining the organization's reputation, trustworthiness, and operational resilience.

Encryption Techniques





Legal and Ethical Compliance

Certainly! Below is the **Legal and Ethical Compliance** section integrated into your **Incident Response Plan**, which identifies relevant laws or regulations, addresses ethical considerations, and explains how the plan upholds these legal and ethical principles.

---

6. Legal and Ethical Compliance in the Incident Response Plan

Legal Compliance

When responding to a phishing incident, it is crucial to comply with relevant laws and regulations that govern data security, privacy, and breach notification. Below are two key legal frameworks that impact incident response:

1. General Data Protection Regulation (GDPR)

- **Overview:** The GDPR is a regulation in EU law that mandates strict guidelines on data protection and privacy. It applies to all organizations that process the personal data of EU residents, regardless of the organization's location. Under GDPR, organizations are required to protect personal data and notify authorities in the event of a data breach.

- **Relevance to Incident Response:** In case of a phishing attack that compromises personal data, the GDPR requires that the organization:

    - **Notify the relevant Data Protection Authorities (DPA)** within 72 hours if there is a high risk to individuals' rights and freedoms.

    - **Notify affected individuals** if their personal data has been compromised (e.g., email addresses, financial information, etc.).

    - Implement appropriate **security measures** to prevent unauthorized access to sensitive data and ensure compliance with data protection principles.

2. Sarbanes-Oxley Act (SOX)

- **Overview:** The Sarbanes-Oxley Act is a U.S. federal law that mandates specific practices in financial reporting, auditing, and internal controls to protect investors from fraudulent activities. It applies to publicly traded companies and has strict requirements

around corporate governance, financial accuracy, and transparency.

- **Relevance to Incident Response:** If a phishing attack impacts financial data or leads to unauthorized financial transactions (as seen in the FACC and Crelan Bank incidents), SOX compliance requires:
    - **Internal controls** to be put in place to prevent fraudulent activities.
    - **Reporting the incident** to senior executives and the board of directors in a timely manner.
    - Ensuring that **financial records** are secure and that any fraudulent transactions resulting from the phishing attack are identified and corrected.

Ethical Compliance

In addition to legal compliance, ethical principles are also critical when responding to security incidents. One major ethical consideration is the **protection of individuals' privacy and confidentiality**, particularly when sensitive information, such as personal data or financial details, is involved.

Ethical Consideration: Protection of Employee and Customer Privacy

- **Overview:** It is an ethical responsibility to protect the privacy of employees, customers, and any stakeholders whose data may be compromised during a phishing attack. Ethical considerations dictate that the response should prioritize:
    - **Transparency with Affected Individuals:** Organizations must notify affected individuals in a clear, honest, and timely manner. Withholding information or failing to disclose breaches can result in a loss of trust and reputational damage.
    - **Minimal Impact on Individuals:** The organization should take steps to minimize harm to those affected by the breach. This includes offering support, such as credit monitoring services for individuals whose personal information was exposed.

How the Incident Response Plan Upholds Legal and Ethical Compliance

The **Incident Response Plan** outlined in this document takes both legal and ethical compliance seriously, ensuring that the organization adheres to relevant regulations and upholds ethical standards throughout the incident handling process.

1. **Legal Compliance with GDPR and SOX:**

    - **Breach Notification:** If a phishing attack leads to a data breach, the plan ensures that the organization will **notify the relevant authorities** (such as Data Protection Authorities under GDPR) within 72 hours of detecting the breach. It will also notify affected individuals promptly, ensuring compliance with both GDPR and industry best practices for data protection.

    - **Financial Controls:** The plan requires that any **unauthorized financial transactions** resulting from the phishing incident are immediately reported to senior executives and rectified in line with **SOX compliance**. A clear communication channel is established to report the incident to regulatory bodies and ensure transparency and accountability.

2. **Ethical Compliance with Privacy and Transparency:**

    - **Transparency with Affected Parties:** The plan emphasizes that individuals whose personal data or financial information has been compromised will be notified swiftly, and support (such as credit monitoring) will be offered, in line with ethical practices. This is designed to minimize the harm caused by the breach and maintain trust with customers and employees.

    - **Privacy Protection:** The **containment strategy** includes steps to immediately isolate affected systems and prevent further unauthorized access to sensitive data. This minimizes the ethical risk of further compromising individual privacy.

    - **Integrity and Accountability:** The post-incident review process ensures that the organization takes full responsibility for the breach, identifies its root cause, and implements stronger measures to prevent similar breaches in the future, further upholding ethical accountability.

Conclusion

This **Incident Response Plan** not only provides a systematic approach to mitigating phishing incidents but also ensures compliance with **legal requirements** such as **GDPR** and **SOX**, as well as adherence to **ethical principles** related to privacy and transparency. By aligning with these legal and ethical frameworks, the organization demonstrates its commitment to protecting both its stakeholders and its reputation, while also ensuring full accountability in the event of a security breach.
