INTRODUCTION

Cyber threats are a constant reality, targeting individuals and organizations alike. Every organization must be prepared to respond effectively to any type of cyberattack, from phishing to brute force attacks. This playbook outlines a comprehensive approach to security, encompassing prevention, detection, containment, recovery, and post-incident analysis. By implementing these strategies, organizations can mitigate the risks associated with cyber threats, protect their data and systems, and maintain business continuity.

Playbook 1: Phishing

1. Introduction

Phishing is a type of cybercrime often executed by email, telephone call or text message. Someone pretends to be a legitimate institution to "bait" individuals to provide their sensitive information such as personally identifiable information, banking and credit card information, and passwords. The attackers can use the sensitive information to access important accounts or sell them, resulting in identity theft and financial loss of the victims.

This article provides common processes and procedures for our organization to identify and investigate phishing attacks.

2. Preparation Stage

2.1 Incident Response Team Structure

- **Team Manager**: Leader of the incidence response team, responsible for leading and coordinating the whole team, act as a liaison with upper management and other teams and organizations, defuse crisis situations, and ensuring that the team has the necessary personnel, resources, and skills. Bring in outside experts with deep technical knowledge if necessary.
- **Technical Director**: A senior technical expert with strong technical skills and phishing incident response experience. Capable of developing hypotheses about phishing incidents and their technical solutions, determining major technical changes to make. Manage and provide advice

to the technical team during an incident.

- **Incident Handler**: A skilled professional who is trained to handle phishing incidents including intrusion detection, analysis and network administration. Proficient in attacked system and applications affected by phishing attacks.
- **Forensics expert**: Determine the compromised users accounts and systems affected by the phishing attack. Collect and preserve evidence and keep detailed logs.
- **Malware Analyst**: A professional who collects and analyzes information from the phishing message and attachment. Expert in forensics.
- **Vulnerability Assessment Expert**: Conducts assessments to identify weaknesses in organizational systems and applications.
- **Communications Specialist**: Individual responsible for managing internal and external communications during an incident. Provide updates to each group. Make sure each group's needs are communicated.
- **Legal and Compliance Representative**: Reviews incident response plans. Ensures the incidence response team operates within the law and complies with relevant regulations.

2.2 Incident Response Team Services

- Intrusion Detection
- Incident Response
- Advisory Distribution
- Education and Awareness
- Information Sharing

2.3 Dependencies within Organization

- **Management Office**. Establishes incident response policy, budget, and staffing. Responsible for coordinating incident response among various stakeholders.

- **Human Resources**. Involved if an employee is suspected of causing the phishing incident on purpose.

- **Public Affairs and Media Relations**. If the phishing messages were forwarded from internal email accounts to external addresses, a need may exist to inform the media and, by extension, the public depending on the impact of the incident.

- **Business Continuity Planning Team**. If the phishing incident is affecting business operations, business continuity planning professionals should be notified to minimize operational disruption during severe circumstances

2.4 Tools and Resources

Hardware and Software:

- **Digital Forensic Workstations and Backup Devices:** Set up dedicated workstations equipped with digital forensic tools to create disk images, preserve log files, and save other relevant phishing incident data. Make sure these workstations are set up in an isolated environment not connecting to the organization's production network.

- **Laptops:** Prepare laptops with necessary software for report writing (e.g Microsoft Office), data analyzing and packets sniffing. Reinstall all software before using in a new incident.

- **Spare Workstations, Servers, and Networking Equipment:** Keep a stock of spare equipment in office or set up virtual machines that can be used for restoring backups and trying out malware attached with the phishing email.

- **Evidence Gathering Accessories:** Maintain devices including digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape.

- **Blank removable media**

- **Basic networking equipment and cables.**

Incident Analysis Resources:

- **Network diagrams and lists of critical assets**: such as database servers

- **Documentation** for OSs, applications, protocols, and intrusion detection and antivirus product

- **Port lists,** including commonly used ports

Incident Handler Communications and Facilities:

- **Internal Contact information** for team members including office phone numbers, wireless phone numbers, email addresses and instructions for verifying the contact's identity

- **External Contact Information** for organizations such as law enforcement and other agencies outside the organization.

- **Secure storage facility** for securing evidence and other sensitive materials such as devices affected by the phishing attack.

3. Handling Stage

3.1 Preventing Phishing Incidents

3.1.1 Anti phishing tools and technology (Kosinski, Matthew)

1. **Spam filters and email security software:** identify phishing emails and other spam messages with machine learning algorithms and shared technical information. Move suspicious emails to an isolated folder, including attachments for further investigation.

2. **Antivirus and antimalware software**: detect and neutralize malicious files or code carried by phishing emails.

3. **Web filters can:** stop users from visiting known malicious websites and display alerts whenever users attempt to visit suspicious websites.

4. **Multifactor authentication**: make it harder for hackers to take over user accounts. Even if the phishers steal passwords, they still need to provide a second factor like a fingerprint or personal signature to be authenticated.

3.1.2 User Training

Educate employees of our organization about the damage of phishing attacks, policies and procedures regarding appropriate use of devices, networks, email systems, and applications to avoid phishing attacks. Teach employees how to recognize the signs of phishing attempts and what procedure they should take when they receive suspicious emails and SMS messages. Provide employees with easy and clear steps to report phishing attempts to the IT or security team.

Typical signs of a phishing message include:

1. Sentences to invoke strong emotions and pressure (Kosinski, Matthew), such as:

-"We have detected illegal activity. Pay this fine now, or else you will be arrested."

- "There is a problem with your account or financial information. You must update it immediately to avoid losing access."

- "This invoice is overdue. You must pay it immediately, or we will shut off your service."

2. Requests for money or sensitive data

3. Poor spelling and grammar because many phishing gangs operate internationally

4. Generic messaging with no further details to explain the problem precisely

5. Fake URLs and email addresses

3.1.3 Policies and practices

Establish policies and practices to avoid incident. Our organization should forbid employees from initiating monetary transfers over email. Require employees to verify requests for money or information by contacting the requester through means other than those provided in the message.

3.2 Detection and Analysis

3.2.1 Initial Detection

The detection of phishing incident is usually triggered in two ways:

- **Report from users:**

Employees of our organization who finished security training programs can identify suspicious messages and report them to the security team with provided instructions.

- **Automated alerts:**

Email filters can detect phishing emails from suspicious addresses. Antivirus and antispam software can detect and neutralize malicious files or code carried by phishing emails. These tools can automatically quarantine the email and security alerts are triggered when event occurs and sent to designated address which can be reviewed by the security team.

3.2.2 Verify Attack Vectors

- **Email**: Phishing attacks are usually executed via an email message or attachment. For example, hide the malicious code inside an attached document or include a link to a malicious website in the body of an email message.
- **SMS**: Phishing messages containing malicious links or request sensitive information.
- **Phone Calls**: Phishing attackers trick victims into giving up sensitive personal information over the phone.

3.2.3 Incident Analysis

Collect information and evidence

After a phishing incident is detected, we must use delegated tools to collect information of the incident.

1. Save the original phishing message in an isolated environment.

2. If attack is conducted through the phone, collect incoming phone numbers of the message or call.
3. If attack is conducted through email, collect following items:
    - The email address of the sender
    - The recipient of the email
    - The subject line of the email
    - The message of the email
    - The attachment of the email
4. Preserve logs from email servers, web servers, and network devices showing the path of the phishing email.
5. Preserve logs showing login attempts, file access, and other relevant activities.
6. Create disk images of affected systems to capture the state of the system at the time of the incident.

Preservation of the Evidence

1. Document chain of custody, including who controlled the evidence, who secured the evidence, and who obtained the evidence.
2. Document all the collection tools and methods used.
3. Store digital evidence in a secure, access-controlled environment.
4. Use encryption to protect digital evidence in storage.

Identify the type of phishing

Based on attack vectors and message contents, find out which kind of phishing attack it is. (InfoSec Institute) for example, is it:

1. Spear Phishing (Targeting an individual or organization using personalized information including name, position to make email legitimate)
2. Clone Phishing (Replicates and alters a legitimate email that the recipient has received previously to include malicious links or attachments.)
3. Whaling (High stakes emails targeting senior executives within an organization.)
4. Social engineering (targeting lower-ranking employees such as administrative assistants to give out corporate secrets.)
5. Vishing (Uses phone calls instead of emails to deceive the target.)
6. Smishing (Uses text messages instead of emails to deliver the malicious contents, targeting wireless devices especially smartphones.)

First Report about the status of incidents

With the use of issue tracking system and other applications, the incident response team should provide initial incident report including the following:

- A summary of the incident
- Current status of the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Impact assessments related to the incident
- Comments from incident handlers
- Next steps to be taken

Incident Prioritization

Determine the priority level based on critical systems affected, data compromised, scope, disruption time, reputation impact and financial impact:

1. **Critical**: The phishing incident is causing disruption of critical service affecting large number of users, or large amount of sensitive information was compromised. May cause severe damage to organization’s reputation and financial status. Law enforcement will be involved. **Escalation action to management required.**

2. **High**: Incident is causing organization no longer able to provide some critical services to limited number of users, or sensitive or proprietary information was changed or deleted, time to recovery is unpredictable, additional resources and outside help are needed to recover.

3. **Medium**: Incidents causing minor problems or errors for users. or unclassified proprietary information was accessed or exfiltrated.

4. **Low**: Incidents only affecting efficiency of the service, doesn’t have serious impact on users. No sensitive information was exfiltrated, changed, deleted, or otherwise compromised.

Escalation to CIO and Legal Department:

Inform management of the **critical** incident and its impact immediately after prioritization so the organization can notify affected parties, such as customers, partners, and employees. Prepare to notify the public media and law enforcement if necessary.

3.3 Containment, Eradication, and Recovery

3.3.1 Containment

1. Alert and notification

2. Disconnect Affected Systems

3. Block Malicious Senders

4. Block dangerous file types from running such as exe.

5. Check authentication methods

3.3.3 Eradication

1. Remove Phishing Emails
2. Scan and Clean Systems
3. Apply software updates and patches

3.3.3 Recovery

1. Restore service
2. Implement Security Measures
3. Review and update security policies
4. Monitor for Recurrence

4. Post-Incident Stage

4.1 Review Lessons:

According to the NIST Computer Security Incident Handling Guide (Cichonski et al.), hold a “lessons learned” meeting with all involved parties several days after a major incident. Review what occurred, what was done to intervene, and how well intervention worked. Ask questions including:

- Exactly what happened during the phishing incident? Include time stamps.
- Were the documented procedures followed by the incident response team?
- Were any steps or actions taken that might have inhibited the response?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar

incidents?

4.2 Update the IR playbook:

Update the playbook with findings and recommendations during detection, analysis, containment, eradication and recovery.

4.3 User Education and Training:

Conduct post-incident training sessions to educate users on recognizing and avoiding phishing attacks. Share lessons learned from the incident to improve overall awareness.

4.4 Coordination and information sharing:

Coordinate and share information with partners and external organizations to strengthen the organization's ability to effectively respond to IT incidents.

The incident response team should designate who can see which pieces of incident information. It may also be necessary to perform data sanitization or scrubbing to remove sensitive pieces of data from the incident information without disturbing the information on precursors, indicators, and other technical information.

Legal representative must make sure there is no legal issues regarding data sharing.

4.5 Perform Evidence Retention

Email messages should be retained for only 180 days unless it is necessary (required by management office)

5. Conclusion

This playbook has reviewed the necessary steps that incident response team need to take in case your organization is impacted by a phishing attack. In the past five years, phishing has become the most popular cyber crime types. In order to avoid such type of threats, it is crucial to make sure that the security technology of your organization is up to date, and the employees are trained to face any suspicious types of messages and report them to the security team immediately.

Playbook 2: Malware infection

1. Introduction

Malware presents a very dangerous threat for an organization, particularly within the highly dynamic financial sector, which handles its clients' crucial, sensitive information. Further to that last episode, this time I provide the incident response playbook that can be applied aspirationally and implemented, so that you in the financial sector organization would be able to handle and effectively respond to threats of malicious infections within the current setting of the enterprise.

According to NIST 800-61 Revision 2, or simply put NIST 800-61r2, the following guide presents a systematic approach for:

- Locate the Web pages where your site is Malware infected.
- Stop page of tomorrow`s Malware delivery
- Get rid of the Malware from the affected system
- Recover changes brought by the Malware.
- Lessons learned so that we respond to a future crisis better

2. Preparation Stage

2.1 Policy and Plan Development:

- Create and implement a financial sector regulation based incident response policy, such as PCI DSS, GLBA.
- Write an incident response plan that should include a malware-specific procedure.

2.2 Team Members, Roles, and Responsibilities

Incident Response Team (IRT) :

IRM (Incident Response Manager):

- **Responsibilities:** Supervising the scenario and the actions of the incident response, cooperation with other departments, and meeting the statutory requirements.
- **Role:** Supervising the IRT, the central decision unit within the IRT and, due to cooperative responsibility, most responsible for communication with other participating units.

Security Analysts:

- **Responsibilities:** Check: Sum, discretionary analysis, and containment of the process. Supervision of security systems' status and evaluation of the alarms received, Implementation of activities that prevent interaction of infected devices.
- **Role:** The other group of stakeholders is the front liners who consider the technical factors in response to the incident.

IT Support team:

- **Responsibilities:** Help in the brushing away process by restoring systems, assess the viability of the back-up, and administer a fix or improvement.
- **Role:** In communication with people affected by the system loss and technical support in combing back the systems.

Legal and Compliance Officers:

- **Responsibilities:** Complying with all the rules surrounding legal and regulatory for the response. Managing the processes of communication with whether the procedures of the regulators and the concerned parties.
- **Role:** Legal advisory work and compliance work as a legal department.

Public Relations (PR) Officers:

- **Responsibilities:** Another functional process in communication is managing the non-internal communication for maintaining the organization's image. Contacting media and writing press releases.

- **Role:** Designing messages for public communication and contacting the media.

2.3 Tools and Resources Required

Software Resources

- Antivirus and Anti-Malware Software
- Security Information and Event Management (SIEM) System
- Endpoint Detection and Response (EDR) Tools
- Forensic Analysis Tools
- Backup and Recovery Solutions
- Network Monitoring Tools
- IDPS—Intrusion Detection and Prevention Systems
- Incident Management Software
- Threat Intelligence Platforms
- Encryption Tools

Hardware Resources

- High-Performance Workstations
- Dedicated Servers
- Network Segmentation Equipment
- Secure Storage Devices
- Backup Appliances

- Portable Forensic Workstations
- Network Tap Devices
- UPS—Uninterruptible Power Supplies.
- Regular status and impact of the incident to the senior management
- Directions to the affected department regarding measures of containment and changes in operations

2.4 Communications Plan

Internal Communication:

- Any probable malware incident detection must be immediately brought to the notice of the IRT.
- Updates on the status and impact of the incident to senior management from time to time.
- Clearly define instructions to affected departments regarding containment measures and operational changes.

External Communication:

- External cybersecurity experts or coordination with law enforcement, if required

Clients will be contacted and companies must inform clients about the incident and what data has been affected

- Public statements to be issued through the Public Relations Officer so that there can be consistency in messaging

Documentation and Reporting:

- Detailed documentation to be kept on all the activities regarding incident response.
- Create a detailed incident report to be used for internal scrutiny and for compliance purposes.

Produce and distribute lessons learned across all relevant stakeholders for use in making future incident response efforts more effective.

2.5 Training and Awareness

- Period-line training to the IRT on latest malware threats and how to response to them.
- Period-line implementation of awareness to all employees on how to detect the common vector of malware, for instance, phishing.

3. Detection and analysis Stage

- Detection and analysis are right at the core of the incident response process. This is where a malware presence is detected, an understanding of its behavior is achieved, and its effects are evaluated for impact. Accurate detection and analysis would thus warrant an informed and timely response, which in turn limits damage and guarantees quick recovery. This section therefore explains the procedures and best practices in detection and analysis of malware incidents in a financial-sector-based setting.

3.1 Monitoring

Continuous Monitoring:

- **Network Monitoring:** Use network-based Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor all the traffic to and from network continuously. The numbers of tools are available for network monitoring which work on the details of received or transmitted packets and check for the anomalies that are possible indications of malware infection.
- **Endpoint Monitoring:** An EDR tool should be deployed on all endpoints in order to monitor the traces of malware. Such visibility into endpoint activity in real time allows the system to raise the alarm about anything that may suspiciously appear commonly, it is something like strange modifications in files, registries, or executing processes.

- **Security Information and Event Management:** Logging all activities and events such as those from network devices, servers, and applications are done in a SIEM system. Correlation rules and threat intelligence feeds in the SIEM system determine if a security incident might be occurring.

3.2 Identification

Initial Alert and Triage:

- **Alerts:** IDS, EDR, and SIEM are among the security tools that generate alerts sourced from predefined rules and threat signatures. Every alert has to be triaged to understand the validity and severity of the finding. This is conducted to understand whether the alert is a false positive, a benign event, or mapping out an infection of malware.
- **Incident Classification:** If an alert is found to be a real incident, then it has to be classified based upon the organization's incident classification schema. This could be of different shapes or types, like identifiers "malware infection," "phishing," "data breach," etc. Every category holds some response category created for that form of incident.

Isolation of Infected Systems:

Prompt Isolation - Once a malware infection is detected, the infected systems should be promptly disconnected from the network to prevent its further propagation. There exist various isolation schemes like pulling out network cables, disabling network interfaces in the systems, or executing the network segmentation schemes by altering the network switch configuration.

Forensic Information Preservation - Infected systems should not be powered down. Malware may strip all volatile data from these systems, which can potentially hold several forensic values. Other methods of isolation should be utilized.

Log Data: Collect pertinent log files from infected systems and networking devices. Logs record the chronology of information, both before and after the infection, thus discovering from and tracking about what the malware's source is and what the malware did.

Memory Dumps: The capturing of memory dumps from infected systems. Further analysis can be carried out in memory to reveal more about running processes, network connections, and whether malware resides in memory.

File Samples: Gather the malware identified suspicious files and executables found until now on infected systems. These samples are very crucial in malware analysis.

3.3 MALWARE Analysis:

- **Static Analysis:** It is the one where the analysis of the malware file is done without running the same to get info on how is its structure, behavior, and capabilities. Analyze code with disassemblers and decompiles to find malicious functions.

- **Dynamic Analysis**: Executing the malware in a controlled environment, like a sandbox, to observe the manner of activity as it takes place. Dynamic analysis helps to comprehend the behavior of malware like methods knitted to propagate and patterns visible in communication, delivery of payloads, and so on.

- **Behavioral Analysis:** Observing the pattern of behavior demonstrated by the malware throughout, showing the changes made on processes in the system, network activity, and files. Behavioral analysis exposes the life time and intentions of malware. Indicators of Compromise (IoC) :

- **Identification:** Identified during analysis, IoCs could include file hashes, IP addresses, domain names, registry keys, and network patterns associated with the malware. IoCs are basically used as a signature in marking the presence of malware and in detecting another infection.

- **Dissemination:** The IoCs would then have to be shared with key relevant internal stakeholders like the security team, much really should be done followed by the appropriate external partners and threat intelligence communities. IoCs should be disseminated and help proactively identify and protect other threats.

Root Cause Analysis :

- **Initial Point of Entry:** Establish the initial vector through which the malicious software infiltrated the organization's network. Common vectors for infiltrating an organization's network include spear-phishing e-mails, drive-by downloads, and exploiting software or vulnerabilities in a system.
- **First Impacted User:** Note who or which system was the first to be affected by the malware. This can help to trace the malware and potentially identify further infected systems.
- **Propagation Path:** Scan the malware propagation path to understand how it proliferated across the network. This involves identification of the compromised accounts, technique of lateral movement and escalation of privileges.

Impact Assessment:

- **Data Exfiltration:** Determine whether sensitive data was ex-filtrated by the malware. This is accompanied by traffic analysis to understand any off-network data copying and searching the logs for a forbidding kind of access pattern.
- **System Impact:** Establish the effect of the malware on anointing systems. Do the malware result in data corruption, degrading performance, or ceasing services? This would be important to establish in determining focus on recovery.
- **Business Impact:** Establish the scope of the malware into hindering daily business operations, quest for finance loss, denting the reputation, and even effects that may come about during recovery, which may even have regulatory implications. This may help one articulate with stakeholders and qualify decisions taken during the recovery process.

3.4 Incident Severity Classification (0-3)

- Incident severity levels determine the priority of measures to be taken with respect to the impact and urgency of an incident. The following describes, in detail, the information severity levels from 0 to 3.

Severity 0: Informational

Description: Something that can have no real effect on the organization, not a threat to operations, but is recorded for tracking and auditing.

Examples:

- Security that has done their standard scan.
- Users on systems who log in successfully.
- Systems that are being updated on their regular schedule.

Response:

- There is no action that must be taken with it at the moment. It is reviewed during periodic audits.

Severity 1: Low

Definition: Minor occurrences that do not compromise an organization's operation or information.

Examples:

- Failed login attempts with no evidence of a direct attack
- Non-essential warnings generated from a security device

Response:

- Establish a log and tracking record of the event
- Periodic review at regular security meetings

Severity 2: Medium

- **Definition:** Numerous incidents that have the potential to compromise parts of the organization's data or operations, but are contained and controlled with minimal disturbance.

Examples:

- The discovery of a contained non-propagating malware on a single system.
- Unauthorized access attempts failing their objectives.

Response:

- Incident analysis.
- Cybersecurity countermeasures.
- Continual monitoring

Severity 3: High

Definition: A significant incident that impacts multiple system or multi-users and poses a threat or causes the disruption of normal business operations and the exposure of sensitive information.

Examples:

- Multi-System Spread of Malware Unauthorized Access to Sensitive Data with no known evidence of data exfiltration

Response:

- Notify the IRT Begin to contain and reduce the impact. Investigation - Analyze - Fully Implement Notify Management and incident related stakeholders

Severity Impact Examples Response Actions

Severity	**Impact**	**Examples**	**Response Actions**
0	Informational	Routine security scans, successful logins, system updates	Log and review during audits
1	Low	Failed login attempts, non-critical	Log, monitor, review during

		alerts	security meetings
2	Medium	Non-spreading malware, unsuccessful unauthorized access attempts	Investigate, apply controls, monitor
3	High	Spreading malware, unauthorized access to sensitive data	Activate IRT, contain, mitigate, report to management

4. Containment, Eradication, Recovery

4.5 Containment

- Containment is the immediate response phase following detection of a malware infection. The general objective at this stage is to prevent the spread of the detected malware to the various organizational systems and networks. Effective containment strategies are required to limit the impact of the incident, to preserve evidence for further investigation, and for operational continuity.

Containment Objectives :

- **Limiting Spread:** The objective at this stage is basically to isolate infected systems or portions of a network such that the malware cannot further propagate.

- **Preservation of Evidence:** At this containment stage, measures taken must be tactical in a way to preserve as much evidence as possible pertaining to the incident. Such evidence is very vital for forensic analysis in terms of finding out the extent and impact the malware had.

- **Damage Minimization**: It is possible to reduce the damage to operations and data integrity that the malware might have caused to any operation if the malware was isolated. This is necessary to sustain business activities and trust from customers.

Containment Measures:

- **Quarantining:** When malware is detected, the system involved should always be disconnected from the network or as a quarantine by network-segmentation means at once, to curtail the further infection from proliferating to other workstations or different sections within the network as a whole.
- **Network Segmentation:** Establishing network segmentation helps in containment because it isolates critical systems and data from the infected parts of the network. This kind of strategic partitioning contains the effect or reach of malware with lateral movement to reduce its impact.
- **Use Access Control Mechanisms:** Access restriction at user and system levels should be done so that the spread into the infected access area or device is controlled. It could be that some containment activity required in elimination preparation is still being worked on, but it will take some time.
- **Temporary Mitigations:** Some temporary general computer practices include temporary solutions or workarounds set up, such as disabling some services or the ports that the malware might be using to limit the range of activity while more permanent containment or eradication measures are developed.
- **Communication and Coordination:** Maintain clear communication within the incident response team and with relevant stakeholders (such as IT staff, management, legal/compliance teams) throughout the containment phase. Effective coordination ensures that containment measures are executed swiftly and accurately.

4.2 Eradication

- Having the malware properly contained, the action moves into the phase of eradication pertaining to incident response. At this stage, the scope centers on wiping all traces of malware lodged within targets to restore them to normal, healthy conditions, as well as associated systems, thereby eliminating re-infestation. It should be systematic and comprehensive to ensure that the organizational environment is free from the threats of the malware.

Objectives of Eradication

- **Complete Eradication:** By far, the greatest task force should be aimed at totally removing the malware from all the central systems, devices, and networking environments. This eliminates or closes out the points through which the malware can access the organization's infrastructure.
- **System Level Remediation:** Restore affected systems to a known good state through removal of malware-induced changes and configurations that may affect the security and functioning of the system.

Eradication Measures

- **Prevent Re-infection:** Adopt proactive measures with security hardening to avert future occurrences, aiming to patch vulnerabilities through which the malware may have entered. An understanding of the type of malware, behavioral patterns, and methodology of propagation through detailed malware analysis is done as part of the execution to achieve total eradication.
- **Deployment of remediation tools:** Advanced antivirus, malware removal tools and forensic techniques should be used to scan and remove the malware in infected systems. This may include automated tools for detection and elimination of malware; manual interventions may be used in complex or other cases of resistant infections.
- **System Validation and Verification:** After the malware has been cleaned, the systems and settings that it had corrupted might need to be validated, to ascertain the fact that the recovery has been brought back. System functionality shall also be verified to assure that systems function as expected once restored.
- **Documentation and Reporting:** Document all actions taken during the eradication process, including findings from malware analysis, the tools used, and changes on the configuration of systems. Prepare comprehensive incident reports for internal review, regulatory reporting, and for future reference.

- **Post-Eradication Testing:** Conduct post-eradication testing to confirm that the sources have been erased and that systems have been secured and restored to working order. The testing would help in pointing out residual malware or system weaknesses that may need to be further attended to.

4.3 Recovery

- After the containment and eradication process proves successful, the organization now embarks on the recovery stage of its incident response work. Recovery is the part where the organization just as equally makes sure that any systems, data, and services affected are put back into proper functioning as new security measures are applied to evade similar incidents. This part has to be done with extreme care; affected systems get tested and proofed to avoid malfunction and leaks before the normal operation of business is allowed to be carried out.

Objectives of the Recovery

- **Business Operation Restoration**: Restore those systems and services that have been negatively impacted by the incident—something that will actually help in their recovery of regular business operations—in a way that it minimizes any adverse impact on customers and stakeholders.
- **Verification of Data Integrity:** Verification of data that has been restored from backup sources in order to check the correctness and integrity of data to ensure that no data was lost or corrupted during the incident. Restore from secure backups to maintain data consistency and reliability.
- System Resilience: To enhance system security, patches will be implemented in order to make a system resilient against such vulnerabilities revealed by the malware incident.

Recovery Actions:

  - **Data Restoration and Validation**: Data recovery will be carried out through secure backup sources, ensuring the data is free from malware and also valid and correct. This, however, should also entail integrity checking of the backup data as well as integrity checking of the data to avoid any data loss or corruption.

- **System Validation and Testing**: Validate the restored systems, applications, and services by significant, comprehensive testing to ascertain their functionality and security. Check to see whether any remaining forms of malware or performance issues can potentially impact system operations.

- **Security Enhancements**: Strengthen security with the aid of security patches, updates, and configuration alterations for the prevention of reinfection by the malware. Make an extra network separation with robust access control and good monitoring capability for easy detection and effective prevention of any similar incident.

- **User and Staff Training:** Training camps and sessions on incident learnings for the employees about new security measures and best practices to avoid woes from further malware infections. Remind users periodically on the benefits of good hygiene to prevent cybersecurity incidents, and the need to report any suspicions immediately.

- **Documentation and Review:** Document all the recovery steps undertaken, which include the procedures followed in recovery, system change, and enhancement in security. Carry out a general review of the response process that can get lessons learned and some areas of improvement.

5. Post-Incident Activity

- Which is the most critical in this incident response lifecycle through a financial institution's cybersecurity framework. This is done to assess the adeptness of the incident response process in a systematic manner, to learn from the incident, reenforce actions, and improve overall resilience in the face of future incidents. This becomes a vital activity in the creation of an environment where risks are minimized, the institution's security measures are strengthened, and trust in its capability to safeguard sensitive clientele information and maintain compliance with regulatory requirements is sustained.

5.1 Purpose of Post-Incident Activity

Evaluate Incident Response Effectiveness:

- **Assessment:** Carefully examine the incident response plan and procedures followed during the malware infection incident.
- **Effectiveness:** Evaluate the intensity of response actions taken, such as containment, eradication, and recovery efforts, just to mention a few. This will define the incident where the incident response team was working under intense pressure and whether this response was made according to predefined protocols and guidelines.

Examine Incident Timeline and Activities:

- **Timeline Analysis:** Follow the trail of timeline of events that led to, during, and aftermath of the incident including identification, taking containment action, eradication effort, and the timeline to recover it.
- **Action Taken:** Analyze the real time actions by the IRT including management, IT personnel and all the relevant actors. Analyze the rightfulness, correctness, and timeliness of those decisions against the available stages of incident response.

Perform Root Cause Analysis:

Identifying causes: Conduct a root cause analysis to determine what factors and vulnerabilities led to the incident of malware infection. Investigate how the malware entered: through phishing attacks, unpatched systems, or any other vectors.

Gap Analysis: Determine gaps in security controls, procedures, or human factors that let the incident either happen or escalate. Note the weaknesses in detection capabilities and response procedures, or gaps in employee awareness that need work.

Summarize Lessons Learned:

- **Record insight**: Record lessons learned in the course of incident response, including key findings, insights, and observations.

- **Recommendations:** Formulate recommendations on lessons learned to enhance incident response procedures critically, thereby strengthening cyber defenses and the overall organization's resiliency.
- **Knowledge sharing:** Share documented insights and recommendations with relevant stakeholders-such as executive management, IT teams, security staff, legal, and compliance departments.

Update Incident Response Procedures

- **Incorporate Learnings:** Revisit and update the incident response procedures, protocols, and guidelines using the findings from the incident review and root cause analysis.
- **Enhance Protocols:** Include best practices, corrective measures, and preventative steps to close off found gaps and answer better for incident responses.
- **Training and Awareness**: Integrate the lessons learned from incident response into training programs and awareness sessions for employees. Educate staff on revised procedures, cybersecurity best practices, and their roles in preventing and responding to future malware incidents.

Communication of Findings and Recommendations

- **Stakeholder Engagement:** Communicate incident findings, recommendations, and corrective actions to relevant stakeholders within the organization.
- **Transparency:** Promote transparency by providing easily understandable and clear information on the consequences of the incidents, lessons learned, and corrections performed to improve cybersecurity resilience.

- **Executive Briefings:** Elaborate briefings must be provided to the executive management for the effect of the incident, effectiveness of response, and the action that has been taken in providing the security posture and regulatory compliance is improved.

Execute Remediation Action

- **Corrective Response Actions:** Implement remediation efforts and corrective actions identified the Incident Response Review process.
- **Security Enhancements:** Updated security controls, policies, and procedures prevent the leveling of identified vulnerabilities and effectively stop incidents from spreading further.
- **Continuous Improvement**: Lead and embrace the culture of continuous improvement by feeding the feedback and observation of response activities into ongoing cybersecurity efforts and strategy planning.

Improve Training and Awareness

  - **Educational Campaigns**: Execute targeted training and awareness sessions on incident response protocols, cybersecurity hygiene, and on the importance of the time-bound reporting and response process for staff members.
  - **Simulation Exercises:** Tabletop exercises and simulations for practice on incident response scenarios to test revised procedures and assist with building team coordination and communication.

Role of Post-Incident Activity in the Financial Company:

- **Protection of Sensitive Information:** Protection of sensitive client information and financial data from further cyber threats and vulnerabilities.
- **Trust and Image:** Assurance to customers that the institution has a commitment to protecting their trust and the appropriate maintenance of a cyber-safe environment.
- **Compliance and regulatory requirements:** ability to meet the industrial regulatory compliance requirements in the area, such as GDPR, PCI-DSS, and others specific to the industry. This is necessary.

- **Building Operational Resilience:** Build operational resilience into your institution to ensure it continues to function properly and independently through cyber incidents.
- **Risk Mitigation:** Lessen the potential for direct financial loss, confidence-damaging loss, and legal implications.

Playbook 3: Ransomware attack

1. Introduction

Ransomware is a type of malicious software designed to block access to a computer system or data until a ransom is paid. This type of cybercrime can result in significant financial loss and operational disruption for organizations. This playbook outlines the processes and procedures necessary to identify, respond to, and recover from ransomware attacks within your organization.

2. Preparation Stage

2.1 Incident Response Team Structure

- **Team Manager**: Leads and coordinates the incident response team, liaises with upper management and other teams, manages crises, and ensures the team has the necessary personnel, resources, and skills. Brings in external experts if needed.
- **Technical Director**: Develops hypotheses about ransomware incidents, determines major technical changes, and manages the technical team during an incident.
- **Incident Handler**: Detects, analyzes, and responds to security incidents. Proficient in the attacked systems and applications.
- **Forensics Expert**: Identifies compromised systems and analyzes the ransomware. Collects and preserves evidence and maintains detailed logs.
- **Malware Analyst**: Analyzes the ransomware and its behavior, specializing in forensics.
- **Vulnerability Assessment Expert**: Identifies weaknesses in organizational systems and applications.
- **Communications Specialist**: Manages internal and external communications during an incident, provides updates, and ensures clear communication across groups.
- **Legal and Compliance Representative**: Reviews incident response plans to ensure legal

compliance and adherence to relevant regulations.

2.2 Incident Response Team Services

- Intrusion Detection
- Incident Response
- Advisory Distribution
- Education and Awareness
- Information Sharing

2.3 Dependencies within the Organization

- **Management Office**: Establishes incident response policies, budgets, and staffing. Coordinates incident response among stakeholders.
- **Human Resources**: Involved if an employee is suspected of intentionally causing the ransomware incident.
- **Public Affairs and Media Relations**: Informs the media and public if the ransomware has widespread impact.
- **Business Continuity Planning Team**: Notified to minimize operational disruption if the ransomware incident affects business operations.

2.4 Tools and Resources

Hardware and Software:

- **Digital Forensic Workstations and Backup Devices**: Dedicated workstations for digital forensics, isolated from the production network.
- **Laptops**: Equipped with necessary software for reporting, data analysis, and packet sniffing.
- **Spare Workstations, Servers, and Networking Equipment**: Stocked for restoring backups

and testing malware.

- **Evidence Gathering Accessories**: Includes digital cameras, audio recorders, chain of custody forms, evidence storage bags, tags, and evidence tape.

Incident Analysis Resources:

- Network diagrams and lists of critical assets
- Documentation for OSs, applications, protocols, and security products
- Port lists, including commonly used ports

Incident Handler Communications and Facilities:

- Internal and external contact information for team members and relevant organizations
- Secure storage facility for evidence and sensitive materials

3. Handling Stage

3.1 Preventing Ransomware Incidents

3.1.1 Anti-Ransomware Tools and Technology

1. **Endpoint Detection and Response (EDR) Tools**: Monitor and respond to security threats on endpoints.
2. **Antivirus and Antimalware Software**: Detect and neutralize malicious files.
3. **Web Filters**: Prevent users from visiting known malicious websites and alert them to suspicious pages.
4. **Backup Solutions**: Regularly back up critical data to ensure recovery in case of a ransomware attack.
5. **Network Segmentation**: Limit the spread of ransomware by segmenting the network.

3.1.2 User Awareness and Training

Educate employees about the policies and procedures for network, system, and application use. Train them to recognize and respond to ransomware attempts and provide easy reporting methods for suspicious activities.

Signs of a ransomware attack include:

- Unexpected encryption of files
- Ransom notes demanding payment in cryptocurrency
- Inability to access certain files or systems

3.1.3 Policies and Practices

Establish policies to prevent incidents, such as forbidding the installation of unauthorized software and requiring regular backups.

3.2 Detection and Analysis

3.2.1 Initial Detection

- **Report from Users**: Employees trained to identify and report suspicious activities.
- **Automated Alerts**: Security tools detect ransomware activities and trigger alerts.

3.2.2 Verify Attack Vectors

Ransomware attacks can be executed through various vectors such as email, malicious websites, and infected software.

3.2.3 Incident Analysis

Collect Information and Evidence:

1. Identify and isolate infected systems.
2. Collect ransom notes and messages.
3. Preserve logs from affected systems and network devices.

4. Create disk images of affected systems.

Preservation of Evidence:

1. Document the chain of custody.
2. Document all collection tools and methods.
3. Store digital evidence securely.
4. Use encryption for digital evidence in storage.

Identify the Ransomware Type:

Determine the type of ransomware attack (e.g., crypto ransomware, locker ransomware, scareware, etc.).

First Report on Incident Status:

Provide an initial incident report including:

- Summary of the incident
- Current status
- Related incidents
- Actions taken
- Impact assessments
- Comments from handlers
- Next steps

Incident Prioritization:

Determine the priority level based on the impact on critical systems, data compromise, scope, disruption time, reputation impact, and financial impact.

Escalation to CIO and Legal Department:

Inform management of critical incidents and their impacts to notify affected parties and potentially the public media and law enforcement.

3.3 Containment, Eradication, and Recovery

3.3.1 Containment

1. Alert and notification
2. Disconnect affected systems
3. Block malicious IPs and domains
4. Implement network segmentation
5. Verify and strengthen authentication methods

3.3.2 Eradication

1. Remove ransomware from systems
2. Scan and clean systems
3. Apply software updates and patches

3.3.3 Recovery

1. Restore systems from backups
2. Implement enhanced security measures
3. Review and update security policies
4. Monitor for recurrence

4. Post-Incident Stage

4.1 Review Lessons

Hold a “lessons learned” meeting to review the incident and the response, asking questions such as:

- What happened during the ransomware incident?
- Were the documented procedures followed?
- Were any actions taken that inhibited the response?
- What would be done differently next time?
- How could information sharing be improved?
- What corrective actions can prevent similar incidents?
- What precursors or indicators should be watched for in the future?

4.2 Update the IR Playbook

Incorporate findings and recommendations from the incident into the playbook.

4.3 User Education and Training

Conduct post-incident training sessions to educate users on recognizing and avoiding ransomware attacks, and share lessons learned to improve awareness.

4.4 Coordination and Information Sharing

Share information with partners and external organizations to enhance the organization's incident response capabilities. Ensure data sharing complies with legal requirements.

4.5 Perform Evidence Retention

Retain evidence related to the ransomware attack for a specified period as required by management and legal guidelines.

5. Conclusion

This playbook outlines the necessary steps for the incident response team to handle ransomware attacks effectively. As ransomware has become a significant cyber threat in recent years, it is crucial to keep security technologies up to date and train employees to recognize and report suspicious activities immediately. This playbook serves as a comprehensive guide for preparing, handling, and recovering from ransomware incidents.

Playbook 4: Web Application Breach

A web application breach occurs when an attacker successfully exploits vulnerabilities in a web application to gain unauthorized access to sensitive data, disrupt operations, or cause other harm. These breaches can range from simple data theft to complex attacks that compromise entire systems.

Web application breaches are a significant security threat, with consequences that can impact an organization's reputation, finances, and customer trust. Understanding the common attack vectors, implementing preventative measures, and establishing a robust incident response plan are essential for mitigating the risks associated with these breaches.

Incident Response Framework for Web Application Breach

1. Introduction:

- **Authority:** This framework is authorized by Management and applies to all individuals and teams involved in handling web application breaches.
- **Purpose and Scope:** This document defines the process for responding to web application breaches, encompassing the identification, analysis, containment, eradication, recovery, and post-incident analysis phases.
- **Audience:** This framework is intended for all employees, IT staff, security personnel, and relevant stakeholders involved in managing web application security.

2. Organizing a Computer Security Incident Response Capability:

- **Events and Incidents:**
  - **Event:** Any occurrence that could potentially compromise web application security, including suspicious activity, failed login attempts, and network anomalies.
  - **Incident:** An event that has been confirmed to have compromised web application security, causing data loss, system disruption, or other negative impacts.
- **Need for Incident Response:**

    - A robust incident response capability is crucial for mitigating the impact of web application breaches, protecting sensitive data, and maintaining business continuity.
- **Incident Response Policy, Plan, and Procedure Creation:**
    - **Policy:** Define clear roles and responsibilities, communication protocols, escalation paths, and legal obligations related to incident handling.
    - **Plan:** Outline the steps involved in responding to a web application breach, including communication, containment, eradication, recovery, and post-incident analysis.
    - **Procedures:** Provide detailed instructions for performing specific tasks during incident response, such as logging evidence, isolating compromised systems, and restoring backups.
    - **Sharing Information With Outside Parties:** Establish a clear framework for collaborating with law enforcement, security vendors, and other external parties, ensuring compliance with legal and regulatory requirements.

3. Handling an Incident:

- **Preparation:**
    - **Preparing to Handle Incidents:**
        - **Regular Vulnerability Assessments:** Conduct regular penetration testing and vulnerability assessments to identify and fix security flaws in web applications.
        - **Secure Development Practices:** Implement secure development practices throughout the software development lifecycle to minimize vulnerabilities.
        - **Monitoring and Logging:** Implement robust monitoring systems to detect unusual activity and log all relevant events for later analysis.
        - **Incident Response Team Training:** Train the incident response team on handling web application breaches, including technical skills, communication

protocols, and legal considerations.

        - **Pre-Incident Communication Plan:** Define communication channels and roles for notifying stakeholders, including users, management, and external parties, about a web application breach.

    - **Preventing Incidents:**
        - **Strong Authentication and Authorization:** Implement multi-factor authentication and strong password policies to prevent unauthorized access.
        - **Input Validation and Sanitization:** Validate and sanitize all user input to prevent injection attacks like SQL injection and Cross-Site Scripting (XSS).
        - **Secure Configuration:** Ensure that web servers and application frameworks are configured securely, with unnecessary services disabled.
        - **Regular Patching and Updates:** Patch vulnerabilities promptly to mitigate known security weaknesses.
        - **Web Application Firewall (WAF):** Implement a WAF to protect against common web application attacks and block malicious traffic.

- **Detection and Analysis:**
    - **Attack Vectors:** Identify common attack vectors for web applications, such as:
        - SQL Injection
        - Cross-Site Scripting (XSS)
        - Cross-Site Request Forgery (CSRF)
        - Remote Code Execution (RCE)
        - Brute Force Attacks
        - Denial-of-Service (DoS) attacks
    - **Signs of an Incident:** Monitor for indicators like:

    - Unusual traffic patterns
    - Error messages
    - Database queries
    - Increased login attempts
    - User complaints
    - Alerts from security tools
  - **Sources of Precursors and Indicators:**
    - **Security Information and Event Management (SIEM):** Collect and analyze security data from various sources to identify potential breaches.
    - **Web Application Firewalls (WAFs):** Detect suspicious activity and block malicious requests.
    - **Log Files:** Analyze log files from web servers, databases, and network devices to identify anomalies.
    - **Security Tools:** Utilize security tools like intrusion detection systems (IDS) and vulnerability scanners to identify potential threats.
  - **Incident Analysis:**
    - **Determine the Scope of the Breach:** Identify the affected systems, data compromised, and the potential impact.
    - **Identify the Attacker:** Determine the attacker's techniques, motives, and potential targets.
    - **Analyze the Attack:** Understand the specific attack methods used and how the web application was compromised.
    - **Identify Root Cause:** Determine the vulnerabilities that allowed the attack to succeed.
  - **Incident Documentation:**

        - **Detailed Logs:** Maintain a log of all actions taken during incident response, including timestamps, involved personnel, and decisions made.
        - **Evidence Collection:** Gather and preserve evidence from affected systems and network devices for forensic analysis and legal purposes.
        - **Timeline of Events:** Create a timeline of the breach, outlining the sequence of events from initial detection to containment.
        - **Communication Records:** Document all communication with stakeholders, including internal teams, management, and external parties.
    - **Incident Prioritization:**
        - **Severity:** Categorize incidents based on their severity, prioritizing those with the highest potential impact.
        - **Impact:** Assess the impact of the breach on business operations, reputation, and financial implications.
        - **Urgency:** Determine the urgency of the response based on the speed of the attacker's actions and the risk of further damage.
    - **Incident Notification:**
        - **Internal Communication:** Notify relevant teams, including IT, security, legal, and management, about the incident.
        - **External Communication:** Communicate with affected users and external stakeholders, including customers, partners, and regulators, as required by policies and regulations.
        - **Law Enforcement Notification:** Report the incident to law enforcement agencies if necessary, following appropriate protocols and legal requirements.
- **Containment, Eradication, and Recovery:**

- **Choosing a Containment Strategy:**
    - **Isolate the Compromised System:** Disconnect the affected web server from the network to prevent further spread of the attack.
    - **Block Attacker Access:** Implement network access control measures to block the attacker's IP address or other identifying information.
    - **Disable Vulnerable Services:** Temporarily disable vulnerable services or functionalities on the web application to prevent further exploitation.
- **Evidence Gathering and Handling:**
    - **Capture and Preserve Evidence:** Collect digital evidence from affected systems and network devices, maintaining the chain of custody and adhering to legal and ethical guidelines.
    - **Forensic Analysis:** Conduct thorough forensic analysis to identify the attack's origin, scope, and impact, and gather evidence for prosecution if required.
- **Identifying the Attacking Hosts:**
    - **Network Analysis:** Analyze network traffic logs and security tool data to identify the source of the attack.
    - **IP Address Tracking:** Identify the IP addresses involved in the attack, including attacker machines and compromised systems.
    - **Domain Name Resolution:** Determine the domain names used by the attacker and their associated IP addresses.
- **Eradication and Recovery:**
    - **Remove Malware and Backdoors:** Identify and remove any malicious code or backdoors installed by the attacker.
    - **System Restoration:** Restore the web application from a clean backup or

rebuild the system from scratch.

        - **Vulnerability Remediation:** Fix the root cause vulnerabilities that allowed the attack to succeed, patching systems and updating software.

- **Post-Incident Activity:**
    - **Lessons Learned:**
        - **Incident Review:** Conduct a detailed review of the incident to identify the weaknesses in security practices and response processes.
        - **Root Cause Analysis:** Determine the underlying causes of the breach and identify the factors that contributed to the attack's success.
        - **Process Improvements:** Implement improvements to security policies, procedures, and training based on the lessons learned.
    - **Using Collected Incident Data:**
        - **Threat Intelligence:** Analyze the collected data to understand attacker tactics and identify new threat actors or vulnerabilities.
        - **Security Improvements:** Utilize the insights gained from the breach to strengthen security controls and prevent similar incidents in the future.
        - **Future Planning:** Use the data to develop better incident response plans, including improved communication strategies, more effective monitoring, and proactive security measures.
    - **Evidence Retention:**
        - **Legal Requirements:** Retain evidence according to legal requirements and applicable regulations.
        - **Forensic Analysis:** Preserve evidence for potential legal actions, such as prosecution or insurance claims.
        - **Security Improvement:** Utilize the evidence to enhance security controls

and improve incident response capabilities.

4. Coordination and Information Sharing:

- **Coordination:**
  - **Coordination Relationships:** Define roles and responsibilities for various stakeholders involved in incident response, including:
    - **Incident Response Team:** Lead the incident response effort, coordinating with other teams.
    - **IT Security Team:** Provide technical expertise and assist in containment, eradication, and recovery.
    - **Legal Team:** Provide legal guidance and support for evidence handling and reporting.
    - **Communications Team:** Handle communication with stakeholders, including users, management, and external parties.
  - **Sharing Agreements and Reporting Requirements:** Establish clear agreements for information sharing with external parties, such as:
    - **Law Enforcement:** Share relevant information with law enforcement agencies, adhering to legal requirements and protocols.
    - **Security Vendors:** Coordinate with security vendors to obtain technical support, investigate vulnerabilities, and share threat intelligence.
    - **Partners and Customers:** Communicate with partners and customers about the incident, providing updates on the situation and remediation efforts.
- **Information Sharing Techniques:**
  - **Ad Hoc:** Share information through informal communication channels like email, phone calls, and instant messaging.
  - **Partially Automated:** Utilize tools like ticketing systems and collaboration platforms

to facilitate communication and information sharing.

    - **Security Considerations:**
        - **Data Privacy:** Ensure that data sharing practices comply with data privacy regulations, like GDPR and CCPA.
        - **Confidentiality:** Protect sensitive information, including user data and internal details, during communication and information sharing.
        - **Authentication and Authorization:** Implement secure authentication and authorization mechanisms to ensure that only authorized individuals have access to sensitive information.

- **Granular Information Sharing:**
    - **Business Impact Information:** Share information about the impact of the breach on business operations, including downtime, revenue loss, and reputational damage.
    - **Technical Information:** Share technical details about the attack, including attack methods, compromised systems, and vulnerabilities exploited.

Recommendations:

- Regularly review and update the incident response framework to reflect evolving threats, vulnerabilities, and best practices.
- Conduct regular training and simulations to ensure the incident response team is prepared and equipped to handle web application breaches effectively.
- Maintain open communication channels with all stakeholders to ensure timely and accurate information sharing throughout the incident response process.
- Continuously invest in security tools and technologies to enhance the organization's ability to detect, contain, and recover from web application breaches.

By implementing this comprehensive framework, organizations can build a robust incident response capability, mitigate the impact of web application breaches, and protect their systems and data from malicious attacks.

Incident Playbooks for Web Application Breach

1. Introduction

This playbook serves as a guide for all team members involved in responding to web application breaches. It details the actions to be taken at each stage of the response process, including preparation, detection, containment, eradication, recovery, and post-incident analysis.

2. Scope

This playbook is applicable to all web application breaches, regardless of severity or the specific attack vector. It covers breaches affecting:

- Public-facing websites
- Internal web applications
- Mobile applications
- APIs

3. Objectives

The primary objectives of this playbook are:

- **Minimize the impact:** Contain the breach and prevent further damage to systems, data, and reputation.
- **Recover quickly and efficiently:** Restore affected systems and services to operational status.
- **Identify and mitigate root causes:** Analyze the breach to identify vulnerabilities and implement preventative measures.
- **Learn from the experience:** Refine security policies, procedures, and training based on lessons learned.

4. Roles and Responsibilities

4.1 Incident Response Team (IRT)

- **IRT Lead:** Oversees the entire incident response process, coordinates with stakeholders, and ensures effective communication.
- **Security Analyst:** Investigates the breach, analyzes logs and data, and identifies the attack vector and attacker's actions.
- **System Administrator:** Isolates compromised systems, removes malware, and restores affected systems.
- **Network Security Analyst:** Analyzes network traffic, identifies attacker access points, and implements containment measures.
- **Forensics Analyst:** Collects and preserves evidence for analysis and legal purposes.
- **Legal Counsel:** Provides legal guidance on evidence handling, reporting, and communication.
- **Communications Team:** Handles communication with stakeholders, including users, management, and external parties.

4.2 Additional Roles

- **Development Team:** Assists in vulnerability analysis, patching, and code review.
- **Business Operations:** Provides input on business impact and recovery needs.

5. Incident Response Process

5.1 Preparation

5.1.1 Baseline Security Measures

- **Secure Development Practices:** Implement secure development practices throughout the software development lifecycle, such as code review, security testing, and vulnerability scanning. NIST SP 800-53
- **Strong Authentication:** Implement multi-factor authentication (MFA) for all user accounts. NIST SP 800-63B
- **Input Validation and Sanitization:** Validate and sanitize all user input to prevent injection

attacks. OWASP Input Validation Cheat Sheet

- **Secure Configuration:** Configure web servers and application frameworks securely, with unnecessary services disabled. CIS Benchmarks
- **Regular Patching and Updates:** Patch vulnerabilities promptly to mitigate known security weaknesses. NIST SP 800-53
- **Web Application Firewall (WAF):** Implement a WAF to protect against common web application attacks. OWASP Top 10
- **Monitoring and Logging:** Implement robust monitoring systems to detect unusual activity and log all relevant events for later analysis. NIST SP 800-53
- **Regular Vulnerability Assessments:** Conduct regular penetration testing and vulnerability assessments to identify and fix security flaws. OWASP Testing Guide

5.1.2 Incident Response Plan and Procedures

- **Develop a written plan:** Detail the steps to be taken in response to a web application breach. This plan should cover:
    - **Roles and responsibilities:** Clearly define who is responsible for each task.
    - **Communication protocols:** Establish clear communication channels and procedures for notifying stakeholders.
    - **Escalation paths:** Define the process for escalating the incident if needed.
    - **Legal and regulatory considerations:** Address legal requirements and data privacy regulations.
- **Create detailed procedures:** Provide step-by-step instructions for specific tasks, such as:
    - **Evidence collection:** Outline procedures for preserving evidence while maintaining chain of custody.
    - **System isolation:** Detail the steps for isolating compromised systems.
    - **Malware removal:** Provide guidance on identifying and removing malicious code.

    - **Data restoration:** Document the process for restoring data from backups.

5.1.3 Incident Response Team Training

- **Regular training:** Conduct regular training sessions to ensure the IRT is familiar with the playbook and procedures.
- **Simulations:** Conduct realistic incident response simulations to test the team's preparedness and identify areas for improvement.

5.2 Detection

5.2.1 Monitoring and Alerting

- **Log Analysis:** Continuously monitor security logs from web servers, databases, network devices, and security tools for suspicious activity.
- **Security Information and Event Management (SIEM):** Utilize a SIEM to collect and analyze security data from various sources to identify potential breaches.
- **Web Application Firewalls (WAFs):** Configure WAFs to detect and block suspicious activity and generate alerts.
- **Intrusion Detection Systems (IDS):** Deploy an IDS to detect suspicious network traffic patterns and generate alerts.
- **Vulnerability Scanners:** Conduct regular vulnerability scans to identify and patch known vulnerabilities.

5.2.2 Indicators of Compromise (IoCs)

- **Identify common IoCs:** Familiarize the IRT with common IoCs related to web application breaches, such as:
    - **Unexpected database queries:** Unusual or excessive database queries.
    - **Failed login attempts:** Multiple failed login attempts from unknown IP addresses.
    - **Uncommon user agents:** Requests from unusual or unknown user agents.
    - **Unusual traffic patterns:** Spikes in traffic volume, sudden changes in traffic source,

or requests from unexpected geographic locations.

  - **Error messages:** Unexpected errors or unusual error messages from web applications.

- **Establish alert thresholds:** Set thresholds for suspicious activity based on historical data and known attack patterns.

5.3 Containment

5.3.1 Initial Steps

- **Isolate Compromised Systems:** Disconnect the affected web server or application from the network to prevent further spread of the attack.
- **Block Attacker Access:** Implement network access control measures to block the attacker's IP address or other identifying information.
- **Disable Vulnerable Services:** Temporarily disable vulnerable services or functionalities on the web application to prevent further exploitation.

5.3.2 Evidence Collection and Preservation

- **Preserve Evidence:** Capture and preserve evidence from affected systems and network devices, maintaining the chain of custody and adhering to legal and ethical guidelines. NIST SP 800-86
- **Forensic Analysis:** Conduct thorough forensic analysis to identify the attack's origin, scope, and impact, and gather evidence for prosecution if required. NIST SP 800-86

5.4 Eradication

5.4.1 Malware Removal

- **Identify and remove malware:** Use anti-malware tools and forensic analysis to identify and remove any malicious code or backdoors installed by the attacker.
- **System Cleanup:** Thoroughly clean the affected systems to remove any remnants of the malware.

5.4.2 Vulnerability Remediation

- **Patch Systems:** Patch all identified vulnerabilities in the web application, operating systems, and software components.
- **Configure Security Settings:** Re-evaluate and strengthen security settings to prevent similar attacks.
- **Code Review:** Review the application code for potential vulnerabilities and implement fixes.

5.5 Recovery

5.5.1 System Restoration

- **Data Restoration:** Restore data from a clean backup, ensuring data integrity.
- **System Rebuilding:** Rebuild affected systems from scratch if necessary.
- **Service Restoration:** Bring the web application back online after ensuring system stability and data integrity.

5.5.2 Business Impact Mitigation

- **Communication:** Communicate with affected users and stakeholders about the incident, providing updates on the situation and remediation efforts.
- **Business Continuity:** Implement business continuity plans to minimize disruption and ensure operational continuity.

5.6 Post-Incident Analysis

5.6.1 Incident Review

- **Document the Incident:** Create a comprehensive incident report outlining the timeline, events, actions taken, and lessons learned.
- **Analyze Root Causes:** Determine the underlying causes of the breach and identify the vulnerabilities that allowed the attack to succeed.
- **Identify Corrective Actions:** Develop and implement corrective actions to address the identified vulnerabilities and improve security posture.

5.6.2 Continuous Improvement

- **Enhance Security Controls:** Strengthen security controls and implement preventative measures to reduce the risk of future breaches.
- **Update Procedures:** Review and update the incident response playbook based on lessons learned.
- **Improve Training:** Enhance training programs to ensure all team members are equipped to handle future incidents effectively.

6. Communication

6.1 Internal Communication

- **Keep stakeholders informed:** Communicate regularly with internal stakeholders, including IT, security, legal, and management, about the progress of the incident response.
- **Establish communication channels:** Designate clear channels for communication, such as email, instant messaging, or conference calls.

6.2 External Communication

- **Communicate with affected users:** Inform affected users about the incident, the steps taken to address the issue, and any potential impact on their data.
- **Engage with external parties:** Coordinate communication with external stakeholders, such as law enforcement agencies, security vendors, and partners.

7. Legal and Regulatory Considerations

- **Data Privacy Regulations:** Ensure compliance with data privacy regulations, such as GDPR and CCPA, when handling personal data. GDPR, CCPA
- **Incident Reporting Requirements:** Report the incident to relevant authorities, such as law enforcement or data protection agencies, according to legal obligations.
- **Evidence Preservation:** Preserve evidence for potential legal actions, such as prosecution or insurance claims.

8. Ongoing Monitoring and Improvement

- **Regularly monitor for new threats:** Stay up-to-date on the latest threats and vulnerabilities affecting web applications.
- **Conduct vulnerability assessments:** Perform regular penetration testing and vulnerability assessments to identify and mitigate weaknesses.
- **Review and update the playbook:** Periodically review and update the playbook to reflect evolving threats, technologies, and best practices.

Playbook 5: Brute force attack on an authentication service.

A brute force attack is a simple, yet powerful technique used by cybercriminals. It relies on trial-and-error, repeatedly trying different combinations of passwords, PIN numbers, or other credentials until a match is found. While brute force attacks may seem straightforward, they can be highly effective, especially when combined with password lists, automated tools, and access to large computing resources. This playbook outlines a comprehensive approach to prepare for, detect, and respond to such attacks, ensuring the protection of user accounts and the integrity of authentication services.

Incident Response Framework for Brute Force Attack on Authentication Service

1. Introduction:

- **Authority:** This framework is authorized by Management and applies to all individuals and teams involved in handling brute force attacks on authentication services.
- **Purpose and Scope:** This document defines the process for responding to brute force attacks targeting authentication services, encompassing detection, analysis, containment, mitigation, and post-incident review.
- **Audience:** This framework is intended for all employees, IT staff, security personnel, and relevant stakeholders involved in managing authentication service security.

2. Organizing a Computer Security Incident Response Capability:

- **Events and Incidents:**
    - **Event:** Any occurrence that could potentially lead to a brute force attack, including suspicious login attempts, failed login patterns, and increased network traffic.
    - **Incident:** A confirmed brute force attack on the authentication service, characterized by a significant number of failed login attempts targeting multiple user accounts within a short timeframe.
- **Need for Incident Response:**
    - A robust incident response capability is crucial for protecting user accounts,

preventing unauthorized access, and ensuring the continued availability of the authentication service.

- **Incident Response Policy, Plan, and Procedure Creation:**
    - **Policy:** Define clear roles and responsibilities, communication protocols, escalation paths, and legal obligations related to handling brute force attacks.
    - **Plan:** Outline the steps involved in responding to a brute force attack, including detection, analysis, containment, mitigation, and post-incident review.
    - **Procedures:** Provide detailed instructions for performing specific tasks during incident response, such as logging suspicious activity, identifying affected accounts, implementing account lockout, and reviewing security settings.
    - **Sharing Information with Outside Parties:** Establish a clear framework for collaborating with law enforcement, security vendors, and other external parties, ensuring compliance with legal and regulatory requirements.

3. Handling an Incident:

- **Preparation:**
    - **Preparing to Handle Incidents:**
        - **Account Lockout Policies:** Implement account lockout policies to automatically lock accounts after a specified number of failed login attempts.
        - **Rate Limiting:** Implement rate limiting to restrict the number of login attempts per IP address or user account within a defined time window.
        - **Monitoring and Logging:** Implement robust monitoring systems to detect suspicious login activity and log all failed login attempts.
        - **Incident Response Team Training:** Train the incident response team on handling brute force attacks, including technical skills, communication protocols, and legal considerations.

        - **Pre-Incident Communication Plan:** Define communication channels and roles for notifying stakeholders, including users, management, and external parties, about a brute force attack.
    - **Preventing Incidents:**
        - **Strong Password Policies:** Enforce strong password policies, requiring users to use a combination of uppercase, lowercase, numbers, and special characters.
        - **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security by requiring users to provide two or more factors of authentication.
        - **Password Complexity:** Use password complexity requirements to discourage the use of common or easily guessable passwords.
        - **Password Expiration:** Implement password expiration policies to encourage users to update their passwords regularly.
        - **Password Recovery:** Use secure password recovery mechanisms to prevent attackers from guessing or resetting passwords.
- **Detection and Analysis:**
    - **Attack Vectors:** Identify common attack vectors for brute force attacks, such as:
        - **Automated Scripting:** Attackers using automated scripts to try a large number of passwords in a short time.
        - **Credential Stuffing:** Attackers using lists of stolen credentials from other breaches to try against the authentication service.
        - **Dictionary Attacks:** Attackers using lists of common words and phrases to guess passwords.
    - **Signs of an Incident:** Monitor for indicators like:

        - **High Number of Failed Login Attempts:** A significant increase in the number of failed login attempts within a short period.
        - **Unusual Login Patterns:** Failed login attempts from a single IP address or a group of IP addresses.
        - **Login Attempts From Unusual Locations:** Failed login attempts originating from unexpected geographic locations.
        - **Alerts from Security Tools:** Alerts from security tools like intrusion detection systems (IDS) or web application firewalls (WAFs).
    - **Sources of Precursors and Indicators:**
        - **Security Information and Event Management (SIEM):** Collect and analyze security data from various sources to identify potential brute force attacks.
        - **Log Files:** Analyze logs from the authentication service, web servers, and network devices to identify suspicious activity.
        - **Security Tools:** Utilize security tools like intrusion detection systems (IDS) and vulnerability scanners to identify potential threats.
    - **Incident Analysis:**
        - **Determine the Attacker's Target:** Identify the specific user accounts or groups targeted by the attack.
        - **Analyze the Attack Methods:** Identify the specific techniques used by the attacker, such as dictionary attacks, credential stuffing, or automated scripting.
        - **Identify the Source of the Attack:** Determine the IP addresses or systems used by the attacker to launch the attack.
- **Containment, Mitigation, and Recovery:**

- **Choosing a Containment Strategy:**
    - **Account Lockout:** Lock the affected user accounts to prevent further attempts by the attacker.
    - **Rate Limiting:** Implement rate limiting to restrict the number of login attempts per IP address or user account.
    - **IP Address Blocking:** Block the IP addresses identified as the source of the attack.
    - **Traffic Filtering:** Use firewall rules or other network filters to block suspicious traffic patterns.
- **Evidence Gathering and Handling:**
    - **Capture and Preserve Evidence:** Collect digital evidence from affected systems and network devices, maintaining the chain of custody and adhering to legal and ethical guidelines.
    - **Forensic Analysis:** Conduct thorough forensic analysis to identify the attack's origin, scope, and impact, and gather evidence for prosecution if required.
- **Identifying the Attacking Hosts:**
    - **Network Analysis:** Analyze network traffic logs and security tool data to identify the source of the attack.
    - **IP Address Tracking:** Identify the IP addresses involved in the attack, including attacker machines and compromised systems.
    - **Domain Name Resolution:** Determine the domain names used by the attacker and their associated IP addresses.
- **Mitigation:**
    - **Password Reset:** If user accounts have been compromised, require users to

reset their passwords.

        - **Security Awareness Training:** Provide security awareness training to users on best practices for creating and protecting passwords.
        - **Strengthen Authentication:** Consider implementing stronger authentication mechanisms, such as MFA or biometrics.
    - **Recovery:**
        - **Unlock Affected Accounts:** Unlock user accounts that were locked due to the attack.
        - **Restore System Settings:** Restore the authentication service to its normal configuration.
        - **Monitor for Further Attacks:** Continue monitoring for further attack attempts.
- **Post-Incident Activity:**
    - **Lessons Learned:**
        - **Incident Review:** Conduct a detailed review of the incident to identify the weaknesses in security practices and response processes.
        - **Root Cause Analysis:** Determine the underlying causes of the breach and identify the factors that contributed to the attack's success.
        - **Process Improvements:** Implement improvements to security policies, procedures, and training based on the lessons learned.
    - **Using Collected Incident Data:**
        - **Threat Intelligence:** Analyze the collected data to understand attacker tactics and identify new threat actors or vulnerabilities.
        - **Security Improvements:** Utilize the insights gained from the breach to strengthen security controls and prevent similar incidents in the future.

        - **Future Planning:** Use the data to develop better incident response plans, including improved communication strategies, more effective monitoring, and proactive security measures.
    - **Evidence Retention:**
        - **Legal Requirements:** Retain evidence according to legal requirements and applicable regulations.
        - **Forensic Analysis:** Preserve evidence for potential legal actions, such as prosecution or insurance claims.
        - **Security Improvement:** Utilize the evidence to enhance security controls and improve incident response capabilities.

4. Coordination and Information Sharing:

- **Coordination:**
    - **Coordination Relationships:** Define roles and responsibilities for various stakeholders involved in incident response, including:
        - **Incident Response Team:** Lead the incident response effort, coordinating with other teams.
        - **IT Security Team:** Provide technical expertise and assist in containment, mitigation, and recovery.
        - **Legal Team:** Provide legal guidance and support for evidence handling and reporting.
        - **Communications Team:** Handle communication with stakeholders, including users, management, and external parties.
    - **Sharing Agreements and Reporting Requirements:** Establish clear agreements for information sharing with external parties, such as:
        - **Law Enforcement:** Share relevant information with law enforcement

        agencies, adhering to legal requirements and protocols.

        - **Security Vendors:** Coordinate with security vendors to obtain technical support, investigate vulnerabilities, and share threat intelligence.
        - **Partners and Customers:** Communicate with partners and customers about the incident, providing updates on the situation and remediation efforts.

- **Information Sharing Techniques:**
    - **Ad Hoc:** Share information through informal communication channels like email, phone calls, and instant messaging.
    - **Partially Automated:** Utilize tools like ticketing systems and collaboration platforms to facilitate communication and information sharing.
    - **Security Considerations:**
        - **Data Privacy:** Ensure that data sharing practices comply with data privacy regulations, like GDPR and CCPA.
        - **Confidentiality:** Protect sensitive information, including user data and internal details, during communication and information sharing.
        - **Authentication and Authorization:** Implement secure authentication and authorization mechanisms to ensure that only authorized individuals have access to sensitive information.
- **Granular Information Sharing:**
    - **Business Impact Information:** Share information about the impact of the attack on business operations, including downtime, revenue loss, and reputational damage.
    - **Technical Information:** Share technical details about the attack, including attack methods, compromised accounts, and vulnerabilities exploited.

Recommendations:

- Regularly review and update the incident response framework to reflect evolving threats, vulnerabilities, and best practices.

- Conduct regular training and simulations to ensure the incident response team is prepared and equipped to handle brute force attacks effectively.
- Maintain open communication channels with all stakeholders to ensure timely and accurate information sharing throughout the incident response process.
- Continuously invest in security tools and technologies to enhance the organization's ability to detect, contain, and recover from brute force attacks.

Brute Force Attack on Authentication Service Playbook

1. Introduction

This playbook serves as a guide for all team members involved in responding to brute force attacks on authentication services. It details the actions to be taken at each stage of the response process, including preparation, detection, containment, mitigation, and post-incident analysis.

2. Scope

This playbook is applicable to all brute force attacks targeting authentication services, regardless of the specific attack vector or technology used. It covers attacks affecting:

- **Web Applications:** Authentication services embedded in websites.
- **Mobile Applications:** Authentication services used in mobile apps.
- **APIs:** Authentication services used by other applications to access resources.
- **Remote Access Services:** Services like SSH or VPN that require authentication.

3. Objectives

The primary objectives of this playbook are:

- **Minimize impact:** Limit damage to user accounts, sensitive data, and the availability of the authentication service during an attack.

- **Ensure swift recovery:** Restore the authentication service to normal operations quickly and prevent further unauthorized access.
- **Identify and mitigate root causes:** Analyze the attack to identify vulnerabilities and implement preventative measures to reduce future risks.
- **Learn from the experience:** Refine security policies, procedures, and training based on lessons learned.

4. Roles and Responsibilities

4.1 Incident Response Team (IRT)

- **IRT Lead:** Oversees the entire incident response process, coordinates with stakeholders, ensures effective communication, and delegates tasks.
    - **Key Responsibilities:**
        - Overall incident response coordination
        - Communication with stakeholders
        - Escalation management
        - Post-incident review and documentation
- **Security Analyst:** Investigates the attack, analyzes logs and data, identifies the attack vector, and analyzes the attacker's actions.
    - **Key Responsibilities:**
        - Attack investigation
        - Log analysis
        - Threat intelligence gathering
        - Vulnerability assessment
        - Incident reporting
- **System Administrator:** Isolates compromised systems, removes malware, and restores

affected systems to a secure state.

  - **Key Responsibilities:**
    - System isolation
    - Malware removal (if applicable)
    - System restoration
    - Configuration hardening

- **Network Security Analyst:** Analyzes network traffic, identifies attacker access points, implements containment measures, and strengthens network security.
  - **Key Responsibilities:**
    - Network traffic analysis
    - Firewall rule updates
    - Access control implementation
    - Network intrusion detection
- **Forensics Analyst:** Collects and preserves digital evidence from affected systems, maintains the chain of custody, and provides forensic analysis reports.
  - **Key Responsibilities:**
    - Evidence collection and preservation
    - Forensic analysis of system logs, network traffic, and other digital artifacts
    - Evidence reporting
- **Legal Counsel:** Provides legal guidance on evidence handling, reporting, and communication with law enforcement or regulators.
  - **Key Responsibilities:**
    - Data privacy compliance
    - Legal reporting obligations

        - Evidence preservation and disclosure

- **Communications Team:** Handles communication with stakeholders, including users, management, external parties, and the press.
    - **Key Responsibilities:**
        - Public communication
        - Internal communication
        - Crisis management
        - Media relations

4.2 Additional Roles

- **Development Team:** Assists in vulnerability analysis, patching, code review, and implementing secure coding practices.
    - **Key Responsibilities:**
        - Vulnerability assessment and remediation
        - Code review and security audits
        - Implementing secure development practices
- **Business Operations:** Provides input on the business impact of the attack, recovery needs, and operational continuity.
    - **Key Responsibilities:**
        - Business impact assessment
        - Recovery planning and execution
        - Business continuity plan activation

5. Incident Response Process

5.1 Preparation

5.1.1 Baseline Security Measures

- **Account Lockout Policies:** Implement account lockout policies to automatically lock accounts after a specified number of failed login attempts. NIST SP 800-63B
    - **Lockout Threshold:** Define the number of failed login attempts before an account is locked.
    - **Lockout Duration:** Set the duration of the account lockout.
    - **Unlock Mechanism:** Provide a mechanism for unlocking accounts, such as password reset or administrator intervention.
- **Rate Limiting:** Implement rate limiting to restrict the number of login attempts per IP address or user account within a defined time window.
    - **Rate Limit Threshold:** Define the maximum number of requests allowed within a specified timeframe.
    - **Rate Limit Action:** Implement actions to handle rate limit violations, such as temporary blocking or CAPTCHA challenges.
- **Monitoring and Logging:** Implement robust monitoring systems to detect suspicious login activity and log all failed login attempts. NIST SP 800-53
    - **Login Activity Monitoring:** Monitor failed login attempts, user agents, IP addresses, and geographic locations.
    - **Log Retention Policy:** Establish a log retention policy to preserve evidence for investigation.
- **Strong Password Policies:** Enforce strong password policies, requiring users to use a combination of uppercase, lowercase, numbers, and special characters. NIST SP 800-63B
    - **Password Complexity:** Implement password complexity requirements to discourage the use of common or easily guessable passwords.
    - **Password Length:** Enforce a minimum password length.
    - **Password Expiration:** Implement password expiration policies to encourage users to

update their passwords regularly.

- **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security by requiring users to provide two or more factors of authentication. NIST SP 800-63B
    - **MFA Method:** Use robust MFA methods like hardware tokens, biometrics, or one-time passwords.
    - **MFA Enforcement:** Require MFA for critical accounts or sensitive operations.
- **Password Recovery:** Use secure password recovery mechanisms to prevent attackers from guessing or resetting passwords.
    - **Password Reset Process:** Implement a secure process for password resets, including email verification or phone authentication.
    - **Password Recovery Questions:** Use security questions that are difficult for attackers to guess.
- **Security Awareness Training:** Provide security awareness training to users on best practices for creating and protecting passwords, recognizing phishing attempts, and reporting suspicious activity.
    - **Password Security Training:** Educate users on the importance of strong passwords and password hygiene.
    - **Phishing Awareness Training:** Train users to identify and avoid phishing emails and websites.
    - **Suspicious Activity Reporting:** Encourage users to report any suspicious activity they encounter.

5.1.2 Incident Response Plan and Procedures

- **Develop a Written Plan:** Create a documented incident response plan outlining the steps to be taken in response to a brute force attack. Include details on:
    - **Roles and Responsibilities:** Clearly define the responsibilities of each team member

during an incident.

  - **Communication Protocols:** Establish clear communication channels and procedures for notifying stakeholders and coordinating response efforts.
  - **Escalation Paths:** Define the process for escalating the incident to higher authorities if needed.
  - **Legal and Regulatory Considerations:** Address legal requirements related to data privacy, incident reporting, and evidence preservation.

- **Create Detailed Procedures:** Develop step-by-step instructions for specific tasks during an incident, including:
  - **Evidence Collection:** Outline procedures for capturing and preserving evidence from compromised systems while maintaining the chain of custody. NIST SP 800-86
  - **System Isolation:** Detail the steps for isolating compromised systems from the network to prevent further spread of the attack.
  - **Malware Removal (if applicable):** Provide guidance on identifying and removing malicious code from infected systems.
  - **Data Restoration (if applicable):** Document the process for restoring data from backups and verifying data integrity.

5.1.3 Incident Response Team Training

- **Regular Training:** Conduct regular training sessions to ensure the IRT is familiar with the playbook, procedures, and tools.
- **Simulations:** Carry out realistic incident response simulations to test the team's preparedness, communication, and ability to execute the plan effectively.

5.2 Detection

5.2.1 Monitoring and Alerting

- **Log Analysis:** Continuously monitor security logs from the authentication service, web servers, databases, network devices, and security tools for suspicious activity.

  - **Log Collection:** Implement centralized log management to collect logs from different sources.
  - **Log Analysis Tools:** Use tools to analyze logs for patterns, anomalies, and indicators of compromise (IoCs).

- **Security Information and Event Management (SIEM):** Utilize a SIEM to collect, analyze, and correlate security data from various sources to identify potential breaches.
  - **SIEM Configuration:** Configure rules and alerts to detect suspicious activity and correlate events across different systems.
  - **SIEM Reporting:** Generate reports and dashboards to visualize security events and trends.
- **Web Application Firewalls (WAFs):** Configure WAFs to detect and block malicious traffic patterns and generate alerts.
  - **WAF Rules:** Maintain up-to-date WAF rules based on known attack patterns and vulnerabilities.
  - **WAF Logging:** Log WAF activity and generate alerts for suspicious events.
- **Intrusion Detection Systems (IDS):** Deploy an IDS to detect suspicious network traffic patterns and generate alerts.
  - **IDS Signatures:** Maintain up-to-date IDS signatures to identify known attacks.
  - **IDS Alerts:** Configure alerts for suspicious activity and investigate potential intrusions.

5.2.2 Indicators of Compromise (IoCs)

- **Identify Common IoCs:** Familiarize the IRT with common IoCs related to brute force attacks, such as:
  - **High Number of Failed Login Attempts:** A significant increase in the number of

failed login attempts within a short period.

  - **Unusual Login Patterns:** Failed login attempts from a single IP address or a group of IP addresses.
  - **Login Attempts From Unusual Locations:** Failed login attempts originating from unexpected geographic locations.
  - **Alerts from Security Tools:** Alerts from security tools like intrusion detection systems (IDS) or web application firewalls (WAFs) related to suspicious login activity.

- **Establish Alert Thresholds:** Set thresholds for suspicious activity based on historical data and known attack patterns.
  - **Baselining:** Analyze normal login patterns and establish baseline metrics for comparison.
  - **Thresholds:** Define alert thresholds for abnormal deviations in login attempts, IP addresses, or other metrics.

5.3 Containment

5.3.1 Initial Steps

- **Account Lockout:** Lock the affected user accounts to prevent further attempts by the attacker.
  - **Account Lockout Duration:** Set the lockout duration to a reasonable time, such as 30 minutes, or until the user can verify their identity.
  - **Unlock Mechanism:** Provide a secure mechanism for unlocking accounts, such as password reset or administrator intervention.
- **Rate Limiting:** Implement rate limiting to restrict the number of login attempts per IP address or user account.
  - **Rate Limit Threshold:** Adjust the rate limit threshold based on the observed attack

    frequency.

    - **Rate Limit Action:** Implement actions to handle rate limit violations, such as temporary blocking, CAPTCHA challenges, or account lockout.

- **IP Address Blocking:** Block the IP addresses identified as the source of the attack at the firewall or network level.
    - **IP Address Identification:** Use log analysis tools or network monitoring tools to identify the source IP addresses.
    - **Firewall Rules:** Update firewall rules to block identified IP addresses.

5.3.2 Evidence Collection and Preservation

- **Preserve Evidence:** Capture and preserve evidence from affected systems and network devices, maintaining the chain of custody and adhering to legal and ethical guidelines. NIST SP 800-86
    - **Data Acquisition:** Use forensic tools to capture data from hard drives, memory, and network devices.
    - **Chain of Custody:** Document the handling of evidence to maintain its integrity and admissibility in legal proceedings.
- **Forensic Analysis:** Conduct thorough forensic analysis to identify the attack's origin, scope, and impact, and gather evidence for prosecution if required. NIST SP 800-86
    - **Network Traffic Analysis:** Analyze network traffic logs to identify attacker communications and attack patterns.
    - **System Log Analysis:** Analyze system logs for suspicious activity, including file modifications, user actions, and program executions.
    - **Memory Analysis:** Analyze memory dumps for evidence of malicious code or remnants of attacker activity.

5.4 Mitigation

- **Password Reset:** If user accounts have been compromised, require users to reset their passwords.
    - **Password Reset Process:** Implement a secure process for password resets, including email verification or phone authentication.
    - **Password Strength Requirements:** Enforce strong password requirements during password reset.
- **Security Awareness Training:** Provide security awareness training to users on best practices for creating and protecting passwords, recognizing phishing attempts, and reporting suspicious activity.
    - **Password Security Training:** Educate users on the importance of strong passwords and password hygiene.
    - **Phishing Awareness Training:** Train users to identify and avoid phishing emails and websites.
    - **Suspicious Activity Reporting:** Encourage users to report any suspicious activity they encounter.
- **Strengthen Authentication:** Consider implementing stronger authentication mechanisms, such as MFA or biometrics.
    - **MFA Evaluation:** Evaluate different MFA methods, such as hardware tokens, push notifications, or biometrics, to choose the most appropriate solution.
    - **MFA Deployment:** Deploy MFA for critical accounts or sensitive operations.

5.5 Recovery

- **Unlock Affected Accounts:** Unlock user accounts that were locked due to the attack.
- **Restore System Settings:** Restore the authentication service to its normal configuration.
- **Monitor for Further Attacks:** Continue monitoring for further attack attempts.
    - **Alerting Systems:** Maintain active monitoring systems to detect any resurgence of

    the attack.

    - **Log Analysis:** Regularly review logs for any unusual activity.

5.6 Post-Incident Analysis

5.6.1 Incident Review

- **Document the Incident:** Create a comprehensive incident report outlining the timeline, events, actions taken, and lessons learned.
    - **Incident Timeline:** Document the sequence of events, including detection, containment, and recovery actions.
    - **Incident Summary:** Provide a concise summary of the incident, including impact and lessons learned.
- **Analyze Root Causes:** Determine the underlying causes of the attack and identify the vulnerabilities that allowed the attack to succeed.
    - **Vulnerability Analysis:** Identify the specific vulnerabilities that were exploited in the attack.
    - **Attacker Tactics:** Analyze the attacker's techniques and strategies used in the attack.
- **Identify Corrective Actions:** Develop and implement corrective actions to address the identified vulnerabilities and improve security posture.
    - **Vulnerability Remediation:** Patch vulnerabilities, implement secure configurations, and update code to address identified weaknesses.
    - **Process Improvements:** Refine security policies, procedures, and training based on lessons learned.

5.6.2 Continuous Improvement

- **Enhance Security Controls:** Strengthen security controls and implement preventative measures to reduce the risk of future breaches.
    - **Security Audits:** Conduct regular security audits to evaluate the effectiveness of

security controls.

    - **Security Training:** Provide ongoing security training to employees to raise awareness and improve security practices.

- **Update Procedures:** Review and update the incident response playbook based on lessons learned and evolving threats.
    - **Playbook Review:** Periodically review and update the incident response playbook to reflect changes in technology, threats, and regulations.
    - **Best Practice Integration:** Incorporate new security best practices and guidelines into the playbook.
- **Improve Training:** Enhance training programs to ensure all team members are equipped to handle future incidents effectively.
    - **Technical Training:** Provide training on security tools, techniques, and incident response methodologies.
    - **Scenario-Based Training:** Conduct scenario-based training exercises to simulate real-world incident response scenarios.

6. Communication

6.1 Internal Communication

- **Keep stakeholders informed:** Communicate regularly with internal stakeholders, including IT, security, legal, and management, about the progress of the incident response.
    - **Communication Channels:** Use established communication channels, such as email, instant messaging, or conference calls.
    - **Status Updates:** Provide regular updates on the incident status, actions taken, and any potential impact.
- **Establish communication channels:** Designate clear channels for communication, such as email, instant messaging, or conference calls.

    - **Communication Plan:** Develop a communication plan for internal stakeholders to ensure efficient and consistent information sharing.

6.2 External Communication

- **Communicate with affected users:** Inform affected users about the incident, the steps taken to address the issue, and any potential impact on their data.
    - **User Notifications:** Send clear and concise notifications to affected users.
    - **User Support:** Provide user support channels to answer questions and address concerns.
- **Engage with external parties:** Coordinate communication with external stakeholders, such as law enforcement agencies, security vendors, and partners.
    - **Law Enforcement Communication:** Report the incident to law enforcement agencies if necessary, following legal requirements and protocols.
    - **Security Vendor Communication:** Coordinate with security vendors to obtain technical support, investigate vulnerabilities, and share threat intelligence.
    - **Partner Communication:** Communicate with partners about the incident and any potential impact on shared systems or services.

7. Legal and Regulatory Considerations

- **Data Privacy Regulations:** Ensure compliance with data privacy regulations, such as GDPR and CCPA, when handling personal data. GDPR, CCPA
    - **Data Breach Notifications:** Comply with legal requirements for notifying individuals whose data has been compromised.
    - **Data Subject Rights:** Respect data subject rights, such as the right to access, rectification, and erasure.
- **Incident Reporting Requirements:** Report the incident to relevant authorities, such as law enforcement or data protection agencies, according to legal obligations.

    - **Reporting Deadlines:** Meet legal deadlines for reporting data breaches to authorities.
    - **Reporting Procedures:** Follow established procedures for reporting incidents to authorities.
- **Evidence Preservation:** Preserve evidence for potential legal actions, such as prosecution or insurance claims.
    - **Evidence Collection:** Collect and preserve evidence in a forensically sound manner.
    - **Evidence Retention:** Retain evidence according to legal requirements and applicable regulations.

8. Ongoing Monitoring and Improvement

- **Regularly monitor for new threats:** Stay up-to-date on the latest threats and vulnerabilities affecting authentication services.
    - **Threat Intelligence Sources:** Monitor threat intelligence feeds and security blogs to stay informed about emerging threats.
    - **Vulnerability Databases:** Subscribe to vulnerability databases and advisories to identify new vulnerabilities.
- **Conduct vulnerability assessments:** Perform regular penetration testing and vulnerability assessments to identify and mitigate weaknesses.
    - **Penetration Testing:** Engage security experts to conduct penetration tests to identify exploitable vulnerabilities.
    - **Vulnerability Scanning:** Use automated tools to scan for common vulnerabilities.
- **Review and update the playbook:** Periodically review and update the playbook to reflect evolving threats, technologies, and best practices.
    - **Playbook Review:** Conduct periodic reviews of the playbook to ensure its effectiveness and relevance.
    - **Best Practice Integration:** Incorporate new security best practices and guidelines

into the playbook.

- **Improve Training:** Enhance training programs to ensure all team members are equipped to handle future incidents effectively.
    - **Technical Training:** Provide training on security tools, techniques, and incident response methodologies.
    - **Scenario-Based Training:** Conduct scenario-based training exercises to simulate real-world incident response scenarios.

REFERENCES ‘

Kosinski, Matthew. “What Is Phishing?” *IBM*, 17 May 2024

https://www.ibm.com/topics/phishing

"Phishing Investigation." *Microsoft Learn*, Microsoft, 2024

https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-phishing#roles-and-permissions-required

"Phishing Response Playbook." InfoSec Institute, 2023

www.infosecinstitute.com/resources/phishing/the-phishing-response-playbook/

Cichonski, Paul, et al. *Computer Security Incident Handling Guide*. NIST, Aug. 2012

https://csrc.nist.gov/pubs/sp/800/61/r2/final

Secure Development Practices

- OWASP Code Review Guide: https://owasp.org/www-project-code-review-guide/
- OWASP Testing Guide: https://owasp.org/www-project-web-security-testing-guide/

Strong Authentication

- NIST SP 800-63B: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B.pdf

Input Validation and Sanitization

- OWASP Input Validation Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Secure Configuration

- CIS Benchmarks: https://www.cisecurity.org/benchmark/

Regular Patching and Updates

- NIST SP 800-53: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Web Application Firewall (WAF)

- OWASP Top 10: https://owasp.org/Top10/

Monitoring and Logging

- NIST SP 800-53: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Regular Vulnerability Assessments

- OWASP Testing Guide: https://owasp.org/www-project-web-security-testing-guide/

Evidence Collection and Preservation

- NIST SP 800-86: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-86r2.pdf

Data Privacy Regulations

- GDPR: https://gdpr.eu/

- CCPA: https://oag.ca.gov/privacy/ccpa

Account Lockout Policies

- NIST SP 800-63B: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B.pdf

Strong Password Policies

- NIST SP 800-63B: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B.pdf

Multi-Factor Authentication (MFA)

- NIST SP 800-63B: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B.pdf

Evidence Collection and Preservation

- NIST SP 800-86: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-86r2.pdf

Data Privacy Regulations

- GDPR: https://gdpr.eu/

- CCPA: https://oag.ca.gov/privacy/ccpa

Cameron, Dell (13 May 2017)

"Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It". Gizmodo.

Dunn, John E. "Ransom Trojans spreading beyond Russian heartland". TechWorld.

Internet Crime Complaint Center (IC3). 30 November 2012.

"Citadel malware continues to deliver Reveton ransomware..."

Help Net Security. 11 July 2018.

"Ransomware back in big way, 181.5 million attacks since January".

Update: McAfee: Cyber criminals using Android

"Update: McAfee: Cyber criminals using Android malware and ransomware the most". *InfoWorld.*

Cryptolocker victims to get files back for free

Cryptolocker victims to get files back for free". BBC News

FBI says crypto ransomware has raked in >$18 million

"FBI says crypto ransomware has raked in >$18 million for cybercriminals". Ars Technica.

Number of ransomware attacks

"Number of ransomware attacks per year 2022". Statista.

Paul Cichonski (NIST), Thomas Millar (DHS), Tim Grance (NIST), Karen Scarfone (Scarfone Cybersecurity). "Computer Security Incident Handling Guide - SP 800-61 Rev. 2 (Final)" *NIST*, August 2012

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf