Introduction

Whenever an organisation gets hit with a security breach or incident, it needs a plan to get back up again, with the objective to minimize the damage caused by the attack, such that the recovery time and costs should be minimum. Incident Response is a structured approach of managing and handling a security breach, while an Incident Response Plan is a pre prepared consistent response to how to deal with any kind of such security breaches. It is all about responding to problems in real time.

The Incident Response process for the NIST includes four steps:

1. Preparation

The first phase allows an organization and its incident response team to prepare for incident handling and involves creating and designing security policies and strategies, defined in detail, determining roles and responsibilities for when an incident occurs and developing required tools furthermore involves identifying assets critically important, validating that the deployed software/hardware can execute on all endpoints, having the tools and skills allow detection of advanced attacks and threats, accessibility to investigative tools that include malware analysis etc, keeping a record to costs involved in responding to such incidents.

Incident handler Communication and Facilities

Contact information: When an incident occurs, serves as the initial point of contact to reach

On-call information: For other teams within the organisation, to raise escalation.
Incident reporting mechanisms: Means by which people can report incidents(mail, phone, instant messaging), also provisions for submitting reports anonymously.

Issue tracking system: Manages and maintains list of issues and incidents.

War room: Establishing team meeting location for conducting discussions

Secure storage facility: Work unit responsible for safekeeping of evidence and sensitive data.

Incident analysis hardware and software

Digital forensic workstations and/or backup devices: to create disk images, preserve log files, and save other relevant incident data

Packet sniffers and protocol analyzers: to capture and analyze network traffic

Digital forensic software: to analyze disk images

Evidence gathering: Accessories including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions

2. Detection and Analysis

Early and accurate identification of incidents is key to strong and effective incident management. The focus of this phase is to monitor security events to detect and report on potential data incidents. Incident Detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents.

Attack vectors
Loss or Theft of Equipment:The loss or theft of an organisational computing device or media.
Impersonation: Attack involving spoofing, replacing something with malicious
*Web:*Attack carried out through a website or web based application
External/Removable Media: Attack carried out with the help of a removable peripheral
Email: Attack executed with the help of email or mail attachment

Sources of precursors and indicators

IDPSs: Identify suspicious events and record timestamp

Automated network and system logs analysis: Automated Analysis of Network Traffic and system access, helps identify suspicious and unauthorised activity

*Employees:*employee detects an anomaly and reports it

Usage anomaly detection: Machine learning systems to differentiate between safe and anomalous user activity

Internal code review: discovers hidden vulnerabilities, design flaws

Incident Analysis
Determining whether an event is actually an incident or not, requires collaborative work with technical and information security personal to make a decision.

3. Containment, Eradication, and Recovery

Once the threat is identified, IRT should work on containing it, before its exposure to more resources on the production environment, during this phase the infected IT elements should be isolated and measures should be taken in order to backup critical data from the infected systems, a temporary fix should be implemented at that time to avoid further escalation of the threat, objective is to minimise the compromised systems during this phase.
Containment Strategy should be decided, which vary based on the type of incident, such as

Potential damage to and theft of resources
Need for evidence preservation
Service availability (e.g., network connectivity, services provided to external parties)
Time and resources needed to implement the strategy
Effectiveness of the strategy (e.g., partial containment, full containment)
Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

Eradication and Recovery

At Eradication phase, once the threat has been contained, the Incident Response Team should work on a permanent fix such as hardware patches, reconfiguring system and architecture, rebuilding and deploying the system for production use. Objective of this phase is to eliminate the entry point that the attacker used to access to network and data. During this phase, IRT should document all the actions taken in order to eradicate the threat for future purposes.

At Recovery phase, the affected production environment is restored and brought online, includes data recovery and restoration efforts as well. The Incident Response Team will decide when the operations will be fully restored. Testing and verifying the infected systems, continuing to monitor malicious activity and validate recovery.

4. Post-Incident Activity

Finally, the Incident Response Team should work on a document which gives insights and details regarding the incident, investigation and remediation towards the incident. A report should be drafted reviewing the whole Incident Response Plan, its during this phase that the team learns insights and knowledge which is later used to improve the IRP in future
Points discussed during this meeting are well documented and kept for future reference

Benefits of Incident Response Planning

Reduced Investigative Costs

By working on the assumption that occurrences will happen, organisations can minimize company disturbance by simplifying the focus of their investigative workflow specific to analysis and presentation activities.

Confidence of Clients and Investors

A huge deciding factor in public perception is how business responds to a breach, which plays a vital role in building consumer trust, with a ready incident response plan organisation has a better chance of coping with the security breach and simultaneously defending the reputational risk in aftermath

Avoidance of Penalties

Depending on the type of company and nature of incident, external authorities may require involvement, Law enforcement may require immediate release of information regarding the breach, proactive IRP facilitates the organization with such ability to make information readily available in such scenarios.

Data Breach Example

An employee from a manufacturing company falls victim to an iFrame Injection attack by visiting a non-work related (malicious) website from his company provided work laptop, the attacker was able to place his malware on the employee's laptop, which allowed an attacker to gain access to the work network via the employee's (victim) laptop, the attacker then escalated privileges and started making changes to system configurations and research documents, this attack was not detected by the Firewalls and IDPS as it originated from a trusted device, IT team was notified by the research team about the documents being altered and being accessed. The first step that Incident Response Team took was to scan the whole network and user activities on the server, once learnt about the infected work laptop, its connection to the company network was terminated and the critical data on the device was backed up and then the exposure of the threat was analysed, such as what intel and systems were exposed,the systems infected were isolated from the network and were reset and reconfigured while the affected device was then submitted to forensics to study the entry point of the attack. All the client data present on the laptop was analysed and clients were made aware of the breach within 72 hours as per GDPR and a company release was issued to authorities and enforcement agencies. Once the situation was controlled, reports and documents were drafted based on comments and reviews from the people involved in the aversion of the attack, insights generated were used to improve the baseline security and Incident Response Plan.

References

https://securityintelligence.com/creating-an-incident-response-checklist-to-prepare-for-a-data-breach/

https://cloud.google.com/security/incident-response/

https://securityboulevard.com/2018/06/the-core-phases-of-incident-response-remediation/

https://www.valasecure.com/blog/5-benefits-of-having-a-proactive-incident-response-plan

https://www.darkreading.com/operations/a-proactive-approach-to-incident-response-7-benefits-/a/d-id/1324363

https://blog.rapid7.com/2017/01/11/introduction-to-incident-response-life-cycle-of-nist-sp-800-61/

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

https://www.youtube.com/watch?v=GvLnb4YQHh0