Incident Response plan

the company

Rev v1.0

- **Md Shifat Uddin – 1147153**
- **Arijit Guha –1186271**
- **Aysha Tul Humaira - 1125896**
- **Bonn Supoch- 1109976**

Table of contents

1. Testing and review Cycle:

1. Incident response plan will be tested **once annually**
2. CSIRT Team will create detailed documentation during the test and identify improvement areas.
3. The imponent measures will be tested and added to the Incident response plan.

2. Purpose:

The purpose of this document is to ensure “TheCompany” is prepare and can manage cyber incidents in most efficient and effective way possible. Having the well documented Incident response plan can greatly minimize the impact of cyber incident on business. Also

3. Scope:

This Incident response plan applies to “TheComany”’s Network, System, Data and stakeholders like employee, contactors and third-party vendors. The member of the Cyber Security Incident Response Team (CSIRT) will lead the Incident response procedure according to this plan. The team should familiarize with plan beforehand.

control has to sufficient to minimize incident. Otherwise higher volumes of incidents may occur, overwhelming the incident response CSIRT team.

4. Authority:

The responsibility of security of information system and data within the system resides to the Managing Director of “TheCompany”. During critical cyber security incident this responsibility will be carried out by CISO/CTO of “TheCompany”

5. Cyber Security Incident Response Team (CSIRT):

5.1 Roles and responsibility of Cyber Security Incident Response Team

CSIRT Role	Responsibility
Executive	Accountable Executive for protecting cyber security within the organization. Responsible for reporting to board directors and other executives. Within the CSIRT, this role is responsible for all issues requiring executive decision.
Incident Handler	This role organizes the team and initiates the Incident Response Plan to investigate and respond to cyber security incidents.
Communications	The Communications Expert is responsible for both public relations and internal communications. They are the messenger to ensure that internal/external stakeholders, customers, and the public are informed in a timely and compliant fashion.
Note-taker	The note-taker records the progress of the CSIRT, including anything from meeting minutes, to post-mortem reports.
Network	The Network Engineer provides technical expertise to the response.
Desktop Technician	The Desktop Support Specialist provides technical expertise to the response.
Server Technical	The Server Support Specialist provides technical expertise to the response.
Legal Technician	Legal Counsel providing legal expertise to the CSIRT.

5.2 CSIRT Contacts

Following tables contains contacts information of CSIRT member along with backup email.

CSIRT Role	Name	Title	Phone	Email
Incident Handler	*Kevin*	*President/Owner*	*437-366-1234* *Backup 437-366-1234*	kevin@thecompany.inc tc_kevin@gmail.com
Incident Handler (Backup)	*Art*	*General Manager*	*437-366-1235* *Backup 437-366-1233*	*art@thecompany.inc* *tc_art@gmail.com*
Executive	*Shifat Uddin*	*Assistant Manager*	*437-366-1235* *Backup 437-366-1233*	*shifat@thecompany.inc* *tc_shifat@gmail.com*
Note-taker	*Shifat Uddin*	*Assistant Manager*	*437-366-1235* *Backup 437-366-1233*	*shifat@thecompany.inc* *tc_shifat@gmail.com*
Communications	*Aysha Tul Humaira*	*Manager - PR*	*437-366-1235* *Backup 437-366-1233*	*aysha@thecompany.inc* *tc_aysha@gmail.com*
Network	*Shifat Uddin*	*Assistant Manager*	*437-366-1235* *Backup 437-366-1233*	*shifat@thecompany.inc* *tc_shifat@gmail.com*
Desktop Technician	*Arijit Guha*	*Manager*	*437-366-1235* *Backup 437-366-1233*	*arijit@thecompany.inc* *tc_arijit@gmail.com*
Server Technician	*Bonn Supoch*	*Manager*	*437-366-1235* *Backup 437-366-1233*	*bonn@thecompany.inc* *tc_bonn@gmail.com*
Legal	*Nanji*	*Legality Corp.*	*437-366-1235* *Backup 437-366-1233*	*nanji@thecompany.inc* *tc_nanji@gmail.com*

5.3 External Contacts

Role	Organization	Name	Title	Phone	Email
Network Security Vendor	*Cybersecurity Vendor Ltd.*	*General Helpdesk*	*Helpdesk*	*1-888-555-0014*	*support@cybersec.com*
Internet Service provider	*Roger*	*Roger NOC*	*Helpdesk*	*1-888-555-0014*	*support@roger.com*
Lawyer	*Legality Corp.*	*Vladimir Putin*	*Lawyer*	*647-345-0025*	*putin@legal.eg*
Hardware Supplier	*Supplier Co*	*Gina Steve*	*SalesManager*	*647-555-0036*	*gina@supplier.eg*
Cyber Insurance Provider	*Insurance Ltd. Policy #123ABC*	*Gurkirat Singh*	*Account Manager*	*647-555-0058*	*gurkirat@insurance.eg*
Ransomware Decryption Service Provider	*Ransomware Decryptor Inc.*	*Rachel D'Agostini*	*Account Manager*	*647-555-0069*	*rachel@decryptor.eg*
Law Enforcement (local)	*London Police Local Precinct*	*London Police*		*647-911-0911*	*report@police.eg*
Law Enforcement (federal)	*RCMP National Cybercrime Coordination Unit*	*Cybercrime Reporting System*			

6.Incident Severity Matrix:

6.1 Severity Matrix

Category	Indicators	Scope	Action
1 Critical	Data loss, Malware, Unauthorized access to server	Widespread and/or with critical servers or data loss, stolen data, unauthorized data access	Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide, Look for all other system for sign of breach.
2 High	Theoretical threat becomes active, DDoS	Widespread and/or with critical servers or data loss, stolen data, unauthorized data access	Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide
3 Medium	Email phishing, User Credential compromise	Widespread	Implement CSIRT, Incident Response Plan, create Security Incident,
4 Low	Malware or phishing, lost mobile device.	Individual host or person	Notify CSIRT, create Cyber Security Incident. Solve it with Desk support

6.2 Escalation & reporting mechanism:

Critical: All, immediate action, report to top management immediately with impact and severity, prepare communication proper for internal and external parties

High: Engage Technical and support team, within 2-3 hour. Engage PR team for announcements with estimated time to solve.

Medium: Engage Technical and support team, within 10-16 hour

Low: Engage Desktop support team to help infected user/device and solve it with in 2 working days and report to CSIRT team

6.3 Incident report link:

Anyone can report any anomaly on following email: help@thecompany.com

Anonymous reporting link: help.thecompany.com

7. Incident Handling Process

7. 1. Preparation:

During normal time “the company” will ensure the following preparation steps:

1. Harding the system, OS ,server
2. Ensure network secure
3. Risk Assessment
4. User training
5. Network monitoring (Security Onion)
6. Profiling normal uses of each system component.
7. Temporary war room : Meeting room 1010

7.1.1 Hardware

- Secure storage
- jump kit
- Spare Laptop and server and network equipment
- Back Removable media (HDD , pendrive)
- Printer
- Accessories : cable

7.1.2 Software

- Packet sniffer
- Digital forensic soft
- Clean OS , images

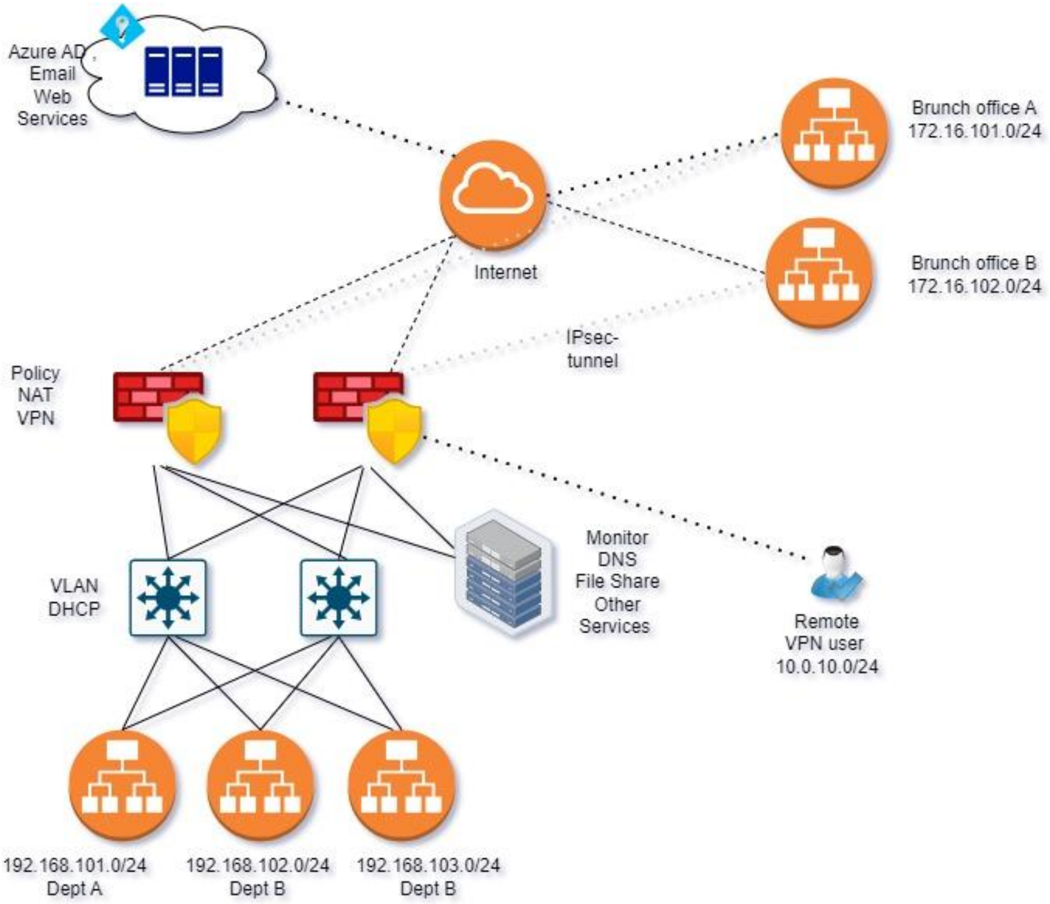
7.1.3 Resource

- 7.1.3.1 Port list

Port Number	Protocol	Service
20, 21	TCP	FTP (File Transfer)
22	TCP	SSH (Secure Shell)
23	TCP	Telnet
25	TCP	SMTP (Email)
53	TCP/UDP	DNS (Domain Name System)
80	TCP	HTTP (Web)
110	TCP	POP3 (Email)
143	TCP	IMAP (Email)
161, 162	UDP	SNMP
443	TCP	HTTPS (Secure Web)
3389	TCP	RDP (Remote Desktop Protocol)
389	TCP/UDP	LDAP (Lightweight Directory Access Protocol)
443	TCP	LDAPS (Secure LDAP)

139, 445	TCP/UDP	NetBIOS
636	TCP/UDP	LDAPS (Secure LDAP)
445	TCP	SMB (Server Message Block)
514	UDP	Syslog
3260	TCP	iSCSI (Internet Small Computer System Interface)
1521	TCP/UDP	Oracle Database
3306	TCP	MySQL Database
5432	TCP/UDP	PostgreSQL Database
5060, 5061	UDP/TCP	SIP (Session Initiation Protocol)
27017-27019	TCP	MongoDB

- 7.1.3.2 Reference Document OS ,app , Protocol , IDS , AV
  - https://ubuntu.com/server/docs
  - https://www.mongodb.com/docs/
  - https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-742893.html
- 7.1.3.3 The Company Network Diagram



- 7.1.3.4 Evidence gather template:

Address / Location	
Manufacturer, Model	
hostname	
media access control (MAC) addresses	
IP addresses of a computer	
Name, title, and phone number of each individual who collected or handled the evidence during the investigation	
Time and date (including time zone)	
Locations where the evidence was stored.	

- 7.1.3.5 PR – framework – and moc interview
  Will be created by PR team

- 7.1.3.6 Lesson learned template

Incident Description	
Time	
How well did staff and management perform in dealing with the incident?	
What information was needed sooner?	
Were any steps or actions taken that might have inhibited the recovery?	
What would the staff and management do differently the next time a similar incident occurs?	
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?	

8.Detection and Analysis

- Bring together those who are aware of the incident

Recognize and assemble the team that will respond to the incident immediately. Team members should include IT, Security, Legal and communication representatives. Team members should be informed briefly about the nature of the incident based on their specific roles and responsibilities.

- Engage Cyber Security Incident Response Team members

CSIRT team should be activated and assigned specific responsibilities among the team members.

The CSIRT team should have access to the necessary resources and tools that will be required to respond to the incident.

- Remind all with responsibility to maintain need-to-know

Separation of duties should be maintained and limiting the access of information to only those who need it. To establish secure communication among the incident response team, protocols need to be implemented that will help in managing misinformation.

- Communicate effectively and efficiently

Clear and concise communication channels must be established between team members for sharing updates of the incident.

- Convene in war room or conference bridges

Set up a centralized location for the CSIRT team to collaborate, make decisions and share information. The war room or conference bridges must be equipped with communication tools and secure physically.

- Utilize multiple location for different needs

Allocate separate locations for the technical team and management team to address their specific requirements. Access to necessary technology and resources need to be ensured.

- CSIRT to investigate and determine whether an incident has occurred

To determine the nature and scope of the incident specific investigation procedures need to be identified. Team members should communicate effectively with each other to understand the nature of the incident and detection processes.

- Perform triage and ensure common understanding

Conduct initial triage to assess the impact and scope of the incident. Routine discussions among team members to ensure understanding of the incident's detection and awareness.

- Analyze the precursors and indicators

To understand the root cause of the incident, precursors and indicators should be identified and analyzed. Threat intelligence and historical data can be considered while doing the analysis.

- Perform research (for example, search engines, knowledge base)

Conduct research to gather information on the incident, potential threats, and relevant vulnerabilities. Utilize external resources like threat intelligence and public databases.

- Document the investigation and evidence gathering

Maintain a detailed record of all research activities and evidence to ensure compliance with all relevant laws and regulations.

- Prioritize handling of incident based on relevant factors (functional impact, information impact, recoverability effort, etc.)

A prioritize framework needs to be developed to help in guiding the response efforts. Relevant factors complied with functional impact, information impact and recoverability effort.

- Determine severity, urgency and initial impact

Evaluate the severity of the incident. Assess its impact on customer trust, data integrity, and business operations.

- Review information and actions taken to date

Review the incident response procedure on a regular basis to find any vulnerabilities or threats. Make sure that every move you take goes in line according to the incident response plan.

- Report incident to appropriate internal personnel and external organizations

Create communication channels for informing stakeholders and executives about the incident. Maintain the legal and regulatory requirements for informing outside authorities about incidents.

9.Containment Eradication & recovery

A thorough strategy is crucial for managing and responding to cybersecurity incidents in an efficient way. We can start by establishing a communications strategy that complies with the required principle and makes sure that data is shared cautiously. We can maintain a stakeholder relationship map to figure out each party's suitable level of involvement. It is important to report information based on actual proof that was at hand and to keep the assigned point of contact always updated on improvements.

Putting an incident response game plan into practice is essential. Firstly, emphasize containing the incident to stop additional harm. After locating the source and exploit, make the required corrections. Confirm the scale of the incident and continue an in-depth impact and damage evaluation. Find out whether changes have been made to any files, connections, accounts, processes, or access. Gather, store, and protect evidence while keeping track of every link of custody.

Take thorough notes and build a comprehensive record of findings and actions. Gradually bring each affected system back to a state where it is ready for use. To make sure the incident is under control and won't happen again, keep a close watch on it. Verify that systems are operating normally after restoring them from reliable sources. If needed, put in extra monitoring measures. Get in touch with the cybersecurity insurance provider to start the claim process if there is a major impact. This systematic approach prevents potential risks and damages while guaranteeing a detailed and efficient response to cybersecurity incidents.

10.Post incident Activity

It is our goal to utilize a detailed and timely evaluation technique when a cybersecurity incident occurs. A meeting will be called to have a thorough discussion on incident structure within two weeks of the incident occurrence. A follow-up report that includes a detailed step-by-step analysis of the incident will then be generated. Besides, according to the incident's degree, this report will specifically examine how the incident was found, who was involved, and when it was found. It will also address the method used for control and removal.

With reference to established frameworks like SANS and NIST Special Publication 800-61 revision 2, the post-incident analysis will be comprehensive and thorough. One goal is to understand the event, another is to find areas where our cybersecurity methods can be stronger. The goal of this introspective process is to improve our capacity to prepare for upcoming events. Most importantly, there will be systems of responsibility in place to ensure that opportunities for development are thoroughly evaluated and exploited of. This agreement illustrates our commitment to endure in the face of cybersecurity threats and continuing improvement.

11. Incident Specific Handling Processes:

11.1 Data breach

- **Secure operations:**

To prevent data breaches, it is crucial to secure systems and fix vulnerabilities. Secure physical areas, lock them, and consult with forensics experts and law enforcement. Mobilize a breach response team to prevent further data loss. Identify a data forensics team and consult with legal counsel for guidance on federal and state laws. Take all affected equipment offline and monitor entry and exit points. Update credentials and passwords of authorized users. Remove improperly posted information from the web, including on your website and other websites. Interview those who discovered the breach and document the investigation. Do not destroy forensic evidence during the investigation and remediation process. This will help prevent multiple data breaches and ensure a secure business environment.

- **Fix vulnerabilities:**

To prevent future breaches, consider examining service providers' access to personal information, ensuring they are taking necessary steps to prevent future breaches, and verifying their remediation of vulnerabilities. Check network segmentation and work with forensics experts to analyze the effectiveness of the segmentation plan. Investigate if encryption measures were enabled during the breach, analyze backup or preserved data, and verify the types of information compromised. Develop a comprehensive communications plan that reaches all affected audiences, avoid misleading statements, and avoid sharing information that could put consumers at risk. Preparing clear, top-tier questions on your website can help limit customer concerns and save time and money.

- **Notify Appropriate Parties**

When a business experiences a data breach, it is crucial to notify law enforcement, affected businesses, and affected individuals. Legal requirements apply to all states, the District of Columbia, Puerto Rico, and the Virgin Islands, and may vary depending on the type of information involved. Law enforcement should contact local police departments immediately to report the situation and potential risk of identity theft. If the breach involves electronic personal health records, the FTC and HHS must be notified. If account access information has been stolen, affected businesses should notify the institution that monitors the accounts for fraudulent activity. If Social Security numbers have been stolen, contact major credit bureaus for additional information or advice. Notifying individuals early can help reduce the chance of misuse and potential damage.

11.2 Ransomware

- **Isolate infected machines**

When ransomware attacks, time is critical. Disabling Wi-Fi, Bluetooth, and any other networking features along with unplugging the Ethernet cable will help you quickly remove your compromised computer from the network. Since ransomware propagates via your network connection, isolating the compromised machine will stop it from propagating and contaminating additional networked devices. Use the same precautions if you think more than one machine has been compromised.

- **Notify IT security team**

Notifying IT staff right away will help them stop the ransomware's spread and set up the appropriate defenses against the attack. An incident response plan is useful in this situation. The implementation of the plan is expected to facilitate the appropriate handling of the incident, the collection, documentation, and preservation of all evidence, and the prompt and effective resolution of the situation.

- **Identify the type of ransomware**

Understanding the kind of ransomware being used in the attack will help better understand how it propagates, what kinds of files it encrypts, and how to get rid of it. Although there are many varieties of ransomware, the two most prevalent ones are those that encrypt files and lock screens. The first is the simplest to fix, and even though it locks down the entire system, files will remain safe until the ransom is paid. It is far harder to recover from the second. Rather than refusing the user access, it locates all the private information, encrypts it, and then requests payment to unlock and restore the data.

- **Inform employees**

  Notify staff members of the breach as soon as possible, along with the implications for the organization and the actions to take to lessen the damage. While investigations into the incident are ongoing, there probably will be some operational downtown, whether or not their computers have been directly infected. Workers will understandably be concerned about how the attack will affect their jobs, so it's critical to be open and provide them with regular updates on the situation as it develops.

- **Change login credentials**

  By collecting credentials and IP addresses, ransomware can propagate quickly. Hackers have the ability to move laterally across networks, encrypt files, and remove backups if they are successful in gaining access to administrative credentials. We should quickly update all admin and user credentials to make sure your system is safe and to stop hackers from impeding your recovery attempts.

- **Never pay the ransom**

  Organizations are strongly advised by the National Crime Agency not to pay a ransom because doing so gives cybercriminals more confidence to carry out more attacks, continuing the vicious cycle. There is no assurance that you will ever get your files back if you decide to pay the ransom, and in fact, it makes you more vulnerable to future attacks.

- **Update security systems**

  WE need to update all systems and conduct a security audit after the incident has ended. Installing updates as soon as they're made available will stop hackers from taking advantage of flaws in earlier software versions. Maintaining machines up to date, stable, and malware-free requires regular patching.

- **Recover from backups**

  To recover from ransomware attacks, follow the 3-2-1 rule, having three copies of data in two different formats, with at least one offsite. Regular cyber security awareness training, regular backups, limiting user permissions, updating software, installing anti-virus software, scanning emails, following good security practices, configuring firewalls, and creating strong passwords are essential. Phishing is the leading cause of cyber-attacks, and MetaPhish can help organizations detect their vulnerability to phishing. These measures can help protect against ransomware attacks and protect businesses.

11.3 DDoS

To mitigate a DDoS attack, distinguish between attack and legitimate traffic. Avoid cutting off all traffic, especially if a website is inundated with customers. DDoS attacks can range from simple single-source attacks to complex multi-vector attacks, which can divert attention from mitigation efforts on any one trajectory.

- **Blackhole routing**

  Almost all network administrators have access to the solution of creating a blackhole route and directing traffic towards it. In its simplest version, network traffic—both malicious and legitimate—is directed to a null route, or blackhole, and removed from the network when blackhole filtering is applied without particular restriction criteria.

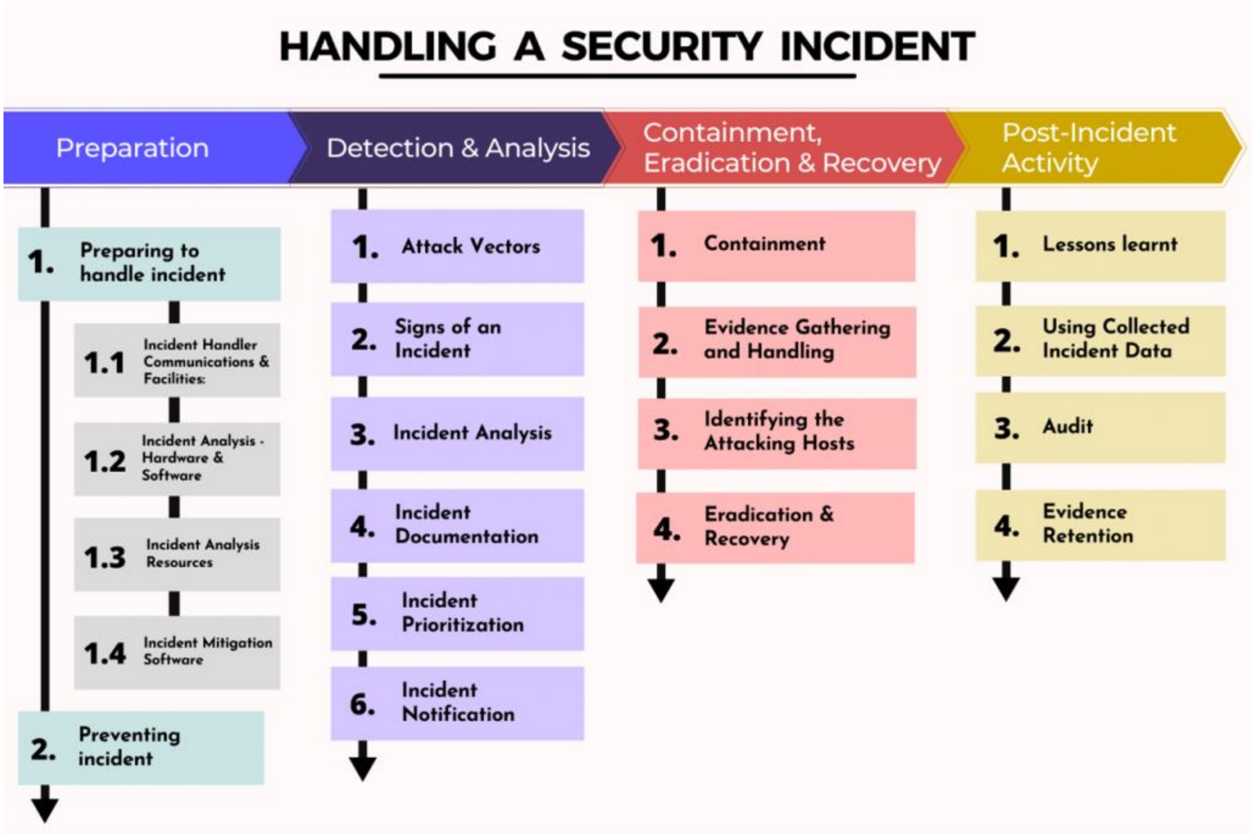
  The Internet service provider (ISP) of a website may, as a defensive measure, direct all site traffic into a blackhole if the website is under a DDoS attack. This is not the best course of action because it essentially grants the attacker their desired outcome, which is to render the network unusable.

- **Rate limiting**

Another method of reducing denial-of-service attacks is to restrict the amount of requests a server will accept in a given amount of time. Rate limitation can be helpful in reducing the speed at which web scrapers steal content and in preventing brute force login attempts, but it probably won't be enough on its own to effectively combat a sophisticated DDoS attack. Rate limiting is nevertheless a helpful part of a successful DDoS mitigation plan.

- **Web application firewall**

One piece of equipment that can help with layer 7 DDoS attack mitigation is a Web Application Firewall (WAF). A WAF may function as a reverse proxy by placing itself in the path of malicious traffic, shielding the targeted server from it. This can be done by placing the WAF between the Internet and the origin server. Layer 7 attacks can be prevented by filtering requests according to a set of rules used to identify DDoS tools. The capability of an efficient WAF to swiftly deploy customized rules in reaction to an attack is one of its main advantages.


HANDLING A SECURITY INCIDENT
Preparation
Detection & Analysis
Containment, Eradication & Recovery
Post-Incident Activity
1. Preparing to handle incident
1.1 Incident Handler Communications & Facilities
1.2 Incident Analysis - Hardware & Software
1.3 Incident Analysis Resources
1.4 Incident Mitigation Software
2. Preventing incident
1. Attack Vectors
2. Signs of an Incident
3. Incident Analysis
4. Incident Documentation
5. Incident Prioritization
6. Incident Notification
1. Containment
2. Evidence Gathering and Handling
3. Identifying the Attacking Hosts
4. Eradication & Recovery
1. Lessons learnt
2. Using Collected Incident Data
3. Audit
4. Evidence Retention

12. Approvals

Responsible Party Responsibility for the security of company and customer information resides with the following responsible party:

Responsible Party Name and Title	Responsible Party Signature	Version	Date
Kevin O' Leary President/Owner		1.0	2024-02-18
Art General Manager		1.0	2024-02-18

The Responsible Party has reviewed the Incident Response Plan and delegates the responsibility for mitigating harm to the organization to the Incident Handler.

13. Case study using – Incident response plan

13.1 Scenario 1

On a Saturday night, network intrusion detection software records an inbound connection originating from a watchlist IP address. The intrusion detection analyst determines that the connection is being made to the organization's VPN server and contacts the incident response team. The team reviews the intrusion detection, firewall, and VPN server logs. It identifies the user ID that was authenticated for the session and the name of the user associated with the user ID.

Phase 1: Preparation

Team Formation: Ensure that members of the IT, security, legal, and management departments are included in the incident response team.

Tool Preparation: Ensure all the tools required for incident identity, analysis, and response are current and readily available.

Communication Plan: Specify routes and procedures for informing parties and arranging the necessary actions to respond.

Phase 2: Detection and Analysis

First Detection: As soon as the incident response team receives an alarm from the intrusion detection analyzer, they should recognize it and investigate.

Examine the logs from the VPN, firewall, and intrusion detection systems to learn more about the occurrence.

Identification: Determine the name of the related user and the user ID that was authenticated during the session.

Phase 3: Containment, Eradication, and Recovery

Isolation: To stop more illegal access, isolate the impacted VPN server from the network.

User Account Management: Remove access rights and deactivate the hacked user account.

System Analysis: Scrutinize the VPN server to find any backdoors or harmful software the hacker may have left behind.

Patch and Remediate: To address vulnerabilities exploited during the incident, apply patches or make configuration modifications.

Restore Services: Return the VPN server to regular operation after it has been determined to be secure.

Phase 4: Post-Incident Activity:

Documentation: Record every move made during the incident response procedure, including conclusions, solutions, and results. Create an incident report that overviews the event, its consequences, and the activities taken in response. Management and all pertinent stakeholders should be given access to this study.

Lessons Learned: Review incident response protocols, security controls, and network architecture after the event to determine what went well and what still needs to be improved.

Continuous Improvement: Make any required adjustments to strengthen incident response capacities and stop such incidents from happening again.

Phase 5: Communication and Coordination

Internal Communication: Keep in constant contact with other incident response team members to make sure everyone is aware of developments and working together.

External Communication: By legal and regulatory obligations surrounding incident reporting and disclosure, notify pertinent stakeholders, such as senior management, legal and regulatory agencies, and law enforcement, as needed.

Phase 6: Legal and Regulatory Compliance:

Legal Counsel: To guarantee adherence to relevant rules and regulations, involve legal counsel in the incident response procedure.

Regulatory Reporting: If necessary, report the occurrence to the appropriate regulatory authorities within the allotted period.

Phase 7 Closure:

Formal Closure: After the incident has been completely contained and eliminated and regular operations have resumed, shut it formally and preserve all pertinent records for future use.

13.2 Scenario 2

On a Tuesday night, a database administrator performs some off-hours maintenance on several production database servers. The administrator notices some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked and calls the incident response team for assistance. The team’s investigation determines that the attacker successfully gained root access to the server six weeks ago.

Response:

According to the Incident response plan it is a Critical Incident. So, it needs to be reported to Higher management and CSIRT and register the incident as Cyber Security Incident.

Just after the detection we need to change the root access. Also, we will check for other unknown accounts, Scan for backdoor and sign of any PII breach. Restore the system from the last backup. After that, the team will look for all other systems for signs of breach. Take logs from all SEIM and monitoring system for last seven weeks and find how attacker gained access. And take preventative measures. Also block attackers IPs for all the system to prevent future attack.

After the incident contain conduct a meeting with all the involved individuals for improvement of both the system control and response method.

13.2 Scenario 3:

On a Wednesday evening, the organization’s physical security team receives a call from a payroll administrator who saw an unknown person leave her office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

Response:

According to the Incident response plan conducted by CSIRT team the severity level of the above incident is moderate. The CSIRT team should identify unauthorized access, isolating the impacted resources and performing a forensic analysis to contain and investigate the incident. Legal authorities of the organization should be informed about the incident and immediate action need to be taken in order to eradicate the incident. Removing malware, changing passwords, and patching vulnerabilities are the primary concerns when dealing with incident containment and eradication. While communication protocols include informing stakeholders about the incident and documenting the incident. The recovery phase entails restoring systems from backups and putting additional security measures in place. To improve overall cybersecurity resilience, the plan must include both ongoing development and corrective measures, like training and incident response plan updates.

14. Reference :

1. National Institute of Standards and Technology. (2012). Title of the Document (NIST Special Publication 800-61r2, Revision 2). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
2. Federal Trade Commission. (n.d.). Data Breach Response Guide for Business. Retrieved from https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business
3. MetaCompliance. (n.d.). How to Deal with Ransomware Attacks. Retrieved from https://www.metacompliance.com/blog/cyber-security-awareness/how-to-deal-with-ransomware-attacks
4. Cloudflare. (n.d.). What Is a DDoS Attack? Retrieved from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/