Incidence Response Plan

Action Plan – SYBRID

Objectives of Incidence Response Plan

- **Prevention** from attack.
- **Defense** against attack.
- **Mitigate** the threat.
- **Control** and **terminate** the threat or incident as quickly as possible.
- **Preventing** minor incident from becoming a major disaster.
- **Familiarize** all **members** and **staff** with procedures.
- Protect **environment**.
- Protect **department assets**.
- **Minimize** impact on the **department**.

Main Challenges in Cyber Security Incidence Response Plan

1. Identifying a **suspected** cyber security **incident** (e.g., Monitoring evidence of unusual occurrences and assessing one or more trigger points).
2. Establishing the objectives of any **investigation** and **clean-up operation**.
3. **Analyzing** all available information related to the **potential** cyber security incident.
4. **Determining** what has **happened** (e.g., A DDOS, malware attack, system hack, session hijack, data corruption etc.).
5. Identifying what **systems, networks,** and **information** (assets) have been **compromised**.
6. **Determining** what information has been **disclosed** to **unauthorized parties, stolen, deleted** or **corrupted**.
7. Finding out **who did it** (i.e., Which threat agent or agents); and why (e.g., Financial gain, hacktivism, espionage, revenge, or fun).
8. Working out **how it happened** (e.g., How did the attacker gain entry to the system).
9. Determining the **potential department impact** of the cyber security incident.
10. **Conducting** sufficient investigation (e.g., Using deep dive forensic capabilities) to identify (and prosecute, if appropriate) the perpetrator(s).

IDENTIFICATION OF THREATS

The department should make sure the relative defenses are in place to ensure that indicators of compromise are identified. Such identifiers include:

- Unusual outbound network traffic.
- New admin users created.
- Anomalies in privileged user account activity (first logon to a system).
- Geographical irregularities (non-standard login attempts).
- Increased database read volume (database dump).
- Large numbers of request for the same file.
- Suspicious registry or system file changes.
- Unexpected patching.
- Signs of DDoS activity.

CONTAINMENT

Once the department of cyber security - Sybrid is confident that an incident can/will be identified the department should try containing the incident and allocate defined course of action based on the potential impact of the attack and should inform the main IT department of the Sybrid. They need to examine if it has control of aspects such *as the blocking of unauthorized access, blocking of dangerous IP and email addresses or even the isolation of systems on the network amongst others*.

ERADICATION

The aim is to eradicate the cause, actual incident, and the compromise itself. Following are the eradication steps:

- *Removing the attack from the network.*
- *Deleting malware.*
- *Disabling breached user accounts.*
- *Identifying vulnerabilities that were exploited.*
- *Mitigating vulnerabilities that were exploited.*

RESTORATION

After the eradication, the process of recovery or restoration should take place and ensure the restoration of the system as soon as possible such as: restoring the system from *back-up logs, notifying the relevant stakeholders, and addressing similar identified vulnerabilities on the network* etc. The restore phase must also consider validating that systems are back to being fully operational and protected.

Future Measure

Even in today's world it will not be possible to prevent all cyber security incidents. As attackers adapt and change, organizations will need to adapt and change as well. We should therefore prepare for an attack executed by an advanced, sophisticated, organized, well-funded and persistent adversary.

To be better prepared, we should consider how we can:

- *Protect most important data in a compromised environment.*
- *Make it more difficult for attackers to be successful.*
- *Detect that an attack is being planned - or is already underway.*
- *Respond to today's sophisticated attacks.*
- Carrying out regular rehearsals of the cyber security incident management response process, using
  realistic scenarios.
- Continually evaluating how you can respond to cyber security incidents in a faster, more agile, and more
  effective nature.

THE NEED FOR COLLABORATION

There is need to collaborate with the cyber security incidence response, which mainly aims:

- Proactively respond to cyber security attacks (e.g., by closing channels or 'attacking the attacker').
- Prosecute those responsible for the attack.
- Reduce the frequency and impact of future security incidents.