Incident Response Plan

Introduction

Incident response plan presents a list of responses to an intrusion and a series of actions to stop an intrusion before it will cause damage an action plan has to include all possible result of analysis as well as actions it has too to cover critical and informational alerts and it should of course be accessible to all employees in the workplace..

Preparation

Preparation presents how employees should be trained to respond to incidents in the workplace, an employee should contact the IT Help Desk immediately after discovering an incident. The Help Desk will store information about an incident like the name of the employee who calls him, the source of the incident, the time, the location of equipment.Next; he has to contact the responsible employee referring to the contact list of the Incident Response team. He has to log the information received and add information to the report like the name of the attacked systems, IP address.

Identification

The incident response team members contacted will meet to discuss the situation and assure that the event is a security incident, and discuss the response strategy that they will apply for example installation of security information and event management (SIEM), so that even logbooks can be proactively analyzed and acted upon or using a honeypot system to log all the attackers' activities and study their behavior which is nothing but a server that offers any kind of services to the attacker with critical vulnerabilities, the type of incident (high, medium or Low),kind of incident because computer incidents require specific Incident Response Team activation.

Confinement

Here they try to limit the damage and isolate the affected systems to avoid probable damage, so usually, they shut down the systems so they stop the attack and assure preserving evidence.

Eradication

It's time to do a root cause analysis to find out why the incident occurred and how to prevent it from occurring again. Act immediately to get the investigation started before valuable evidence is deleted including reviewing of system logs, reviewing intrusion detection or firewall logs, collection, and revision of log files, Reports from network monitoring programs, Detection of unauthorized services installed, any changes in the password file..

Recovery

In this phase they will restore the affected systems to be sure that all vulnerabilities have been removed, the vulnerability must be analyzed on each system before any correction.

Lessons learned

The IT team will revise the incident response plan they should update it according to what they learn from the incident, and improve future response so the incident doesn’t happen again. They must complete an incident report and outline it. they should make sure that the logs have been configured to be sent to a commercial log collection, and that their analysis product runs various logs summaries like trends to observe the big picture(Most Attacked Ports, Main Event Types) As well as Previously Invisible Events to discover rare but critical events in newspapers..