LogicFinder

Consulting, Development and Training

Incident Response Support From LogicFinder

Introduction

Just the past year, businesses have suffered millions of attacks that have exposed 22 billion records, 300 billion passwords, etc. In 2020, ransomware and malware attacks increased by 358% and 435% respectively. These disruptions have caused millions of dollars in loss to various businesses, organizations and institutions. According to the World Economic Forum's 2022 Global Risk Report, the top three risks to global stability over the next five years are cyber attacks, natural disasters and extreme weather. Today, there are estimated cyber attacks every 39 seconds. Numerous security experts believe that a cyber attack or breach of catastrophic proportions is no longer a matter of if, but a matter of when.

To minimize the risks associated with these attacks it's relevant to put measures in place to not just get ahead of attackers and prevent attacks, but to also respond to incidents that may arise. Responding to these incidents in a timely manner is key to lowering the impact of these incidents that organizations face everyday. That is why incident response is the go-to solution for quick responses to help reduce the impact of various malwares and ransome attacks.

Some of the Most Common Security Incidents Include

Social Engineering

Social engineering is when an attacker uses human interaction to obtain or compromise information about a system. Through this process, many attackers have posed as a respectable member of an organization, new employee, researcher, etc to obtain credible information to use in attacking the systems. Social engineering such as phishing, baiting, phishing, tailgating, etc have long evolved into effective methods used by attackers to exploit systems.

Ransomware

Is a type of malicious attack where an attacker denies an organization access to its data by encryption and demanding payment to restore access. A user is tricked into clicking a malicious link that would download a ransomware file from an eternal website. In downloading it is executed and the ransomware takes advantage of the user's device and propagates throughout the organization. Simultaneously, the ransomware encrypts files on all the system and other systems then displays a message on screen demanding a payment in exchange for the decrypting of the files.

Malware Attacks

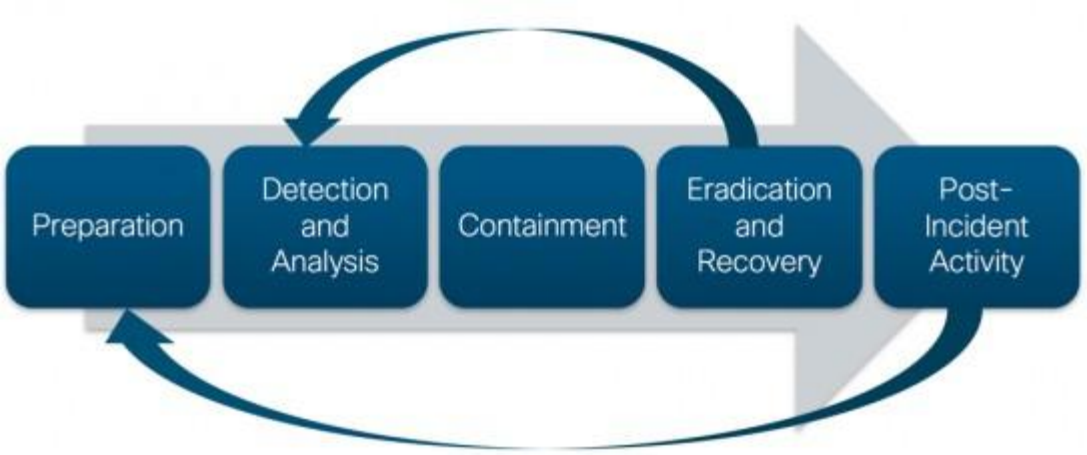
Malware attacks are described as all types of malicious attacks using softwares. These include:
Viruses: a type of malware used to spread malicious codes from one computer to another

Trojan Horses: malicious codes or softwares that pose as legitimate applications tricking users into executing scripts on their devices.
Cryptojacking: One of the malware attacks that are gaining fame. It uses someone's computer to mine cryptocurrency, etc.

DDoS Attacks

A distributed denial-of-service (DDoS) attacks targets websites, servers, systems by disrupting network services. An attacker floods a site or network with errant traffic using botnets, bots and other service requests to overload servers, websites, etc. This compromises an organization's network hence knocking websites, servers, and systems offline. DDoS attacks can last hours or even days.

How Incidents Response Works



As stated before, when these incidents occur in a system, the organization must deploy quick responses to these cyber attacks to deal with them. Most Incident responses follow the same framework based on the National Institute of Standards and Technology (NIST) and SANS Institute. Here are the general procedures on how to go about incidents.

Preparation

The first and most important phase of the incident response process is to make sure the cybersecurity incident response team (CSIRT) has the best procedure and resources in place to identify, eradicate, contain and/or recover from an incident. During this time, the best method of communication is set for the team to securely communicate during this time.

Detections

During this phase, members of the incident response team monitor the system for suspicious activity and potential attacks. The alert or incident is analyzed, and information is gathered from device logs, server logs, and from various security tools (antivirus, vulnerability scanners, endpoint detection and response, firewalls, logs, etc) to help the team understand the incident. During this phase, evidence is collected and stored appropriately for future needs depending on the incident. During this stage, an incident is confirmed to have taken place.

Containment

The steps after indication of an incident is to contain the damage and prevent further influence. The response team now takes meticulous steps to "contain" the threat. This includes, taking networks offline, removing unauthorized access to systems and data, isolating machines, firewalls while preserving other users and devices.

Eradication

Once threats have been contained, the full neutralization or remediation process is started to completely remove threats from the system. This stage involves the elimination of the threat such as destroying malwares, and removing unauthorized users. This often involves secondary monitoring to ensure that affected systems are no longer vulnerable.

Recovery

Security teams upon eradication, restores systems and data as close to previous condition before the attack as possible. This may include restoring backup, restoring compromised users, firewalls, antiviruses, EDRs or XDRs, settings, passwords (if necessary). Some incidents may require rebuilding from scratch. At this stage, systems should be back in production. Once production is determined, the system is continuously monitored for threats.

Lesson Learned

Lastly, another important part of incident response and often overlooked is reviewing the incident that just took place. All information acquired is put together and discussed. Questions such as what happened, where it happened, who was involved, what was the impact? How can the security of the system be improved? What did you learn from this incident? Do we have the best procedure and measures in place? Is there any training necessary? Can the incident response capability be improved?

LogicFinder Incident Response Process

Logic Finder's incident response is a cyclic activity that features ongoing learning and advancement. This cycle discovers how to best protect your organization. The whole process includes four main stages: preparation, detection/ analysis, containment/ eradication and

recovery, and post-incident activities. Specifically, it is a collection of procedures that emphasize on the improvement to discover how to better defend the organization.

1. **Preparation**: to prepare for incidents, our team compiles a list of IT assets including networks, servers, and endpoints. We ensure the baseline of normal activity by monitoring the security events. LogicFinder provides all the core capabilities for perfect incident preparation. This step further includes a centralized visibility interface that shows all configurations, network traffic, and user activities.
2. **Detection/ Analysis:** The phase of detection involves the collection of IT systems, security tools, identifying precursors and indicators. This step is to identify the signs of any incident that may happen in the future. However, the phase of analysis identifies normal activities of affected systems. LogicFinder provides detection capabilities against a wide range of attack vectors.
3. **Containent, Eradication, and Recovery:** To deal with security incidents or stopping malicious processes, LogicFinder helps take remote manual actions. After the incident has been successfully contained, all the elements of the incident are removed by identifying all affected hosts, removing malwares or resetting passwords.
4. **Post-Incident:** This is a central part of the overall incident response activity. In this step, we investigate and document the incident to improve the process. All these findings help to improve the overall process and response policy. Also allows us to add new data into the preparation stage of our incident response process.

Conclusion

Incident response is the process of responding to risks associated with cyberattacks and other malicious activities. It is my hope that hopefully by this point you have enough information to put to an end the incident that has occured.

LogicFinder has an incident response team available to every small, medium, and large organization. The team provides professional security services equipped to carry out fast and effective incident response activities.

Following Documents were used in the preparation of this document:

Paul, C., Scarfone, K., Grance, T., & Millar, T. (2012, August). Computer Security Incident Handling Guide - NIST. Retrieved September 27, 2022, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

McLennan, M., Group, S. K., & Insurance Group, Z. (n.d.). *Global risks report 2022 - 17th Edition*. Retrieved September 27, 2022, from https://www.weforum.org/reports/global-risks-report-2022/digest