ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 10, Issue, 08(C), pp. 34175-34178, August, 2019

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

HOW TO RESPOND TO AN INFORMATION SECURITY INCIDENT

Anshuman Awasthi

993 Rincon Ave. Livermore CA-94551

DOI: http://dx.doi.org/10.24327/ijrsr.2019.1008.3836

ARTICLE INFO

Article History:

Received 6th May, 2019
Received in revised form 15th June, 2019
Accepted 12th June, 2019
Published online 28th August, 2019

Key Words:

Information Technology; Information Security; Information Security Incident; Computer Science; Data Security

ABSTRACT

In today's world managing data security is becoming a challenge especially in a Hybrid cloud environment where the critical information is not confined to an organization's secure data center but is spread across multiple environments including one or many private or public clouds. Organizations are spending a good portion of their IT budget in order to build a secure environment so that they can protect their critical data getting into the wrong hands but the fact is we still hear major data security breaches every now and then. It is necessary to have all the tools in place to protect your network and systems but it is equally important to have a documented and working procedure in place on how an organization will act in case a security breach has been detected. The primary objective of this paper is to help the Infrastructure management teams to acknowledge a security incident quickly and what they should do when a data breach is declared with some examples and possible remediation.

INTRODUCTION

Series of Malicious Events

An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of the responsible use policy. If an unauthorized user is able to gain access to the system, it means security has been compromised on multiple layers of communication. This is a violation of computer security policies, acceptable use policies, and standard security practices.

In a number of cases, an attacker may use several methods to gain access to the system: IP spoofing, data modification, and the man-in-the-middle attack. In the beginning an attacker may send a broadcast message and will record the acknowledgment, depending on the information received from the other end, he can select the network which can be compromised and once he gains access he can detect the location of resources where critical information for the organization is stored for example data storage within the Human Resource (HR) record system. Once the location is found, the attacker can modify the information as per his needs. In a lot of scenarios an attacker has to perform various types of attacks or gain access to multiple systems to access the data, some of the type actions are listed below:

- Elevate access to a network administrator to spoof an IP address
- Unauthorized access to critical systems like payroll
- Unauthorized access as an email administrator

Type and Severity of the Attacks

Prioritizing the way an incident is addressed is perhaps the most critical decision of the incident handling process. Incidents should not be handled on a first-come, first served basis due to resource limitations. Instead, incident handling should be prioritized based on relevant factors, such as:

- Functional impact of the incident
- Information impact of the incident
- Recoverability from the incident

Combining the functional impact on the organization's systems and the impact on the organization's information determines the business impact of the incident.

Event Notification

It is extremely important to analyze and prioritize all incidents. When an incident is analyzed and prioritized, the incident response team must notify the appropriate individuals so that all who need to be involved can perform their responsibilities.

Corresponding author:* **Anshuman Awasthi
993 Rincon Ave. Livermore CA-94551

With any crime scene, whether cyber or physical, notification of the incident is crucial. During incident handling, the organization must communicate with outside parties, such as other incident response teams, law enforcement, the media, vendors, and victim organizations. Because these communications often need to occur quickly, organizations should predetermine communication guidelines so that only appropriate information is shared with specific parties.

Efficient and accurate cyber incident reporting is considered key to mitigating the potential damage these attacks can inflict. In general, the auditor should notify the following individuals from the organization based on the type and severity of the incident:

- CIO
- CFO
- Head of Information Security

(Head of information security should decide if this needs to be escalated outside the organization)

- Network Administrator
- Email Administrator
- IT Operations Director
- Human Resource Head
- Payroll and Finance Department
- Legal Department

The incident response team should notify different departments based on the type of incident, few examples are listed below:

- Initial IP Spoofing (Medium Severity) - Network Administrator, IT Operations Director, Head of Information Security
- Privacy Breach (High Severity)- CIO, CFO, Head of Information Security, Network Administrator, IT Operations Director, Human Resource Head, Payroll Department, Legal Department, Employee's Manager
- Unauthorized/Elevated Network Access (High Severity)- CIO, Head of Information Security, Network Administrator, IT Operations Director, Legal Department, Employee's Manager
- Man-in-the-Middle Attack (High Severity) - CIO, Head of Information Security, Network Administrator, Email Administrator, IT Operations Director, Legal Department, Employee's Manager

Incident Containment

Containment is critical to prevent an incident from overwhelming resources or increasing damage. Most incidents require containment, so it is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential component of containment is decision-making (e.g., shut down a system, disconnect it from a network, and disable certain functions).

An incident can only be contained, or rather a decision to contain an incident can only be made when an incident is detected quickly and a response mechanism is in place. Organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing incident response capabilities. All organizations require a plan that meets their unique requirements, which relates to the organization's mission, size, structure, and functions.

If the data breach has occurred on a system which is inside our corporate firewall, that means the incident was not detected in time, and thus the attacker was able to gain unauthorized access on multiple levels. Let use evaluate valuate the steps that an organization should take to avoid unauthorized access.

Identification

First of all, at the network layer, we should identify and categorize all the traffic to determine whether it poses a threat to the network. If we deploy Intrusion Detection System (IDS), firewall, event logging, etc., we can use them to uncover an issue and to analyze the information to determine whether it is accurate and if it has the potential to disrupt or deny network services. If we only have limited visibility to our network we may not be able to correlate events happening on different devices and eventually come to a conclusion that unauthorized network access has happened.

Once the analysis is complete and the information is determined to be credible and includes the potential for harm, the event should be classified as an incident, which is any adverse event that compromises some aspect of computer or network security.

Containment

Once a security incident is identified, the next step is to contain the damage and to prevent harm from spreading further throughout the network and even throughout networks outside the security boundary. The most immediate means of containment is either to disconnect the infected machine and to isolate it from the network or to stop the service that is causing the incident.

In a lot of cases if we can identify a security incident quickly we can take the following steps to contain the incident:

- IP spoofing can be reported by IDS based on a pre-configured policy that allows for blocking an employee's machine MAC address from the organization network.
- When an attacker is using an employee's account to elevate access to a network administrator, we can create a policy to detect and to block unauthorized access to network devices.
- If a user is able to gain system access, we can create alerts for unauthorized access to servers and stop the user when the alert is reported.
- Email messages should be secured, and responses from unauthorized machines should be reported/blocked.
- If feasible, we can disconnect the compromised system like for example the HR/payroll system in the incident discussed earlier, from the network (during the attack) and continue to its operations as stand-alone operations to prevent further damage. This helps to protect the integrity of data.
- If feasible, we can shutdown network devices or the system.

Eradication

After taking steps to contain the incident and its effects, eradication is the next step. The goal is to permanently remove any evidence of the incident from the network. Eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated.

In a lot of cases, we can consider the following factors for eradication if an end user account/system is compromised:

- Disable the employee's user account and reimage the employee's laptop/desktop (reformat hard drives).
- Do a fresh installation of the operating system and immediately apply the latest security patches tothe servers.
- Apply the latest security updates forthe network infrastructure.

System Recovery

The next step is recovery. The extent of the damage and the chosen method for eradication helps dictate recovery. For some incidents, eradication is either not necessary or is performed during recovery. During recovery, administrators restore systems to normal operations, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve actions such as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets and boundary router access control lists). Higher levels of system logging or network monitoring are often part of the recovery process.

In case the security incident involves unauthorized access and if attacker has compromised one of the administrator accounts, after eradication, the following steps of the recovery process can be taken:

- Change administrative passwords for the network appliances, critical applications, and email systems.
- Restore the affected system from the last successful backup to revert to the original data.
- Restore email system to last-known good configuration.
- Change firewall rule sets to secure access for critical servers and network devices access list.
- Installation of a local root certificate authority to implement a public key infrastructure in which all communication to the affected system will require a certificate.
- Install an incident detection appliance, such as IDS, and establish an incident response process.

Eradication and recovery should be performed using a phased approach so that remediation steps are prioritized.

System Verification

System verification or validation is an important step after the recovery process. Pre-checks should be performed before declaring that the system is operational again.

In a lot of cases an IT department can take the following steps for system verification:

- Compare network configuration with last-known good configuration to ensure there are no discrepancies.
- Run a vulnerability scan on all network devices and ensure there are no applicable vulnerabilities.
- Enable network logging to log blocked connection attempts.
- Compare the server configuration with the last-known good configuration and perform a file consistency check.
- Run a vulnerability scan on all servers and ensure there are no applicable vulnerabilities.
- Ensure the system is not accessible using old administrative accounts.
- Validate database records with the last-known good configuration.
- Ensure the affected system is only accessible using the new certificates installed by the PKI infrastructure.
- Perform a test run on the affected system on selected processes and ensure they are executed successfully.

Incident Prevention

Keeping the number of incidents reasonably low is crucial to protect the business processes of an organization. If security controls are insufficient, higher volumes of incidents may occur, overwhelming the incident response team. This can lead to slow and incomplete responses, which translate to a larger negative business impact (e.g., more extensive damage and longer periods of service and data unavailability).

Preventing problems is often less costly and more effective than reacting to them after they occur. Thus, incident prevention is an important component of incident response capabilities. If security controls are insufficient, high volumes of incidents may occur. This could overwhelm the resources and capacity for response, which would result in delayed or incomplete recovery and possibly more extensive damage and longer periods of service and data unavailability.

In general, an organization should take the following steps to protect their critical data:

- Acquire tools (IDS, network firewall) and resources (information security analyst, incident response team) that may be of value during incident handling.
- Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure.
- Identify precursors and indicators through alerts generated by several types of security software.
- Require a baseline level of logging and auditing for all systems and a higher baseline level for all critical systems.

- Profile networks and systems. Profiling measures the characteristics of expected activity levels so that changes in patterns can be more easily identified.
- Understand the normal behaviors of networks, systems, and applications. Team members who understand normal behaviors should be able to recognize abnormal behaviors more easily.
- Prioritize incident handling based on relevant factors.
- Include provisions regarding incident reporting in the organization’s incident response policy.
- Establish strategies and procedures for containing incidents.

After a major incident has been handled, the organization should hold a lessons-learned meeting to review the effectiveness of the incident handling process and to identify the necessary improvements to existing security controls and practices. Lessons-learned meetings can also be held periodically for minor incidents as time and resources permit.

CONCLUSION

This paper has provided a few guidelines on how to prepare an organization to respond to a security incident. Incident handling can be performed more effectively if organizations complement their incident response capabilities with adequate resources to actively maintain the security of networks, systems, and applications. It is critical to respond quickly and effectively when security breaches occur. In the absence of required network and security tools and a security response process, the attacker may get access to an organization’s critical data which usually means that security was compromised on multiple levels of the communication network.

References

- Computer Security Incident Handling Guide-NIST
- The Definitive Handbook of Business Continuity Management
- http://spg.umich.edu
- http://www.govtech.com
- https://www.techrepublic.com
- https://phoenixts.com
- https://learnaboutgmp.com
- https://www.alienvault.com

How to cite this article:

Anshuman Awasthi.2019, How to Respond to Aninformation Security Incident. *Int J Recent Sci Res.* 10(08), pp. 34175-34178. DOI: http://dx.doi.org/10.24327/ijrsr.2019.1008.3836

****