Information Security Analysis and Audit

Theory Digital Assignment

Prof – Amutha Prabhakar

Name – Yashraj Agarwal

Reg. no. – 18BCI0183

Slot – G2

Question –

Incident Response - Handling Different Types of Information Security Incidents - Preparation for Incident Response and Handling. Incident Response Team

Solution –

Occurrence reaction is a term used to portray the cycle by which an association handles an information break or cyberattack, including the manner in which the association endeavors to deal with the outcomes of the assault or penetrate (the "episode"). At last, the objective is to successfully deal with the episode so the harm is restricted and both recuperation time and expenses, just as blow-back, for example, brand notoriety, are kept at least.

Associations should, at least, have an unmistakable episode reaction plan set up. This arrangement ought to characterize what establishes an episode for the organization and give an unmistakable, guided cycle to be followed when an occurrence happens. Furthermore, it's prudent to indicate the groups, representatives, or pioneers answerable for both dealing with the general occurrence reaction activity and those entrusted with making each move determined in the episode reaction plan.

Regularly, episode reaction is led by an association's PC occurrence reaction group (CIRT), otherwise called a digital episode reaction group. CIRTs ordinarily are included security and general IT staff, alongside individuals from the legitimate, HR, and advertising offices. As Gartner depicts, a CIRT is a gathering that "is liable for reacting to security penetrates, infections, and other possibly calamitous occurrences in endeavors that face critical security hazards. Notwithstanding specialized pros fit for managing explicit dangers, it ought to incorporate specialists who can control venture chiefs on suitable correspondence in the wake of such episodes."

Why we need incident handling response

Occurrence dealing with administration for IT is a coordinated and organized cycle used to address digital assaults and security breaks. The objective of this security approach is to moderate and perhaps, evade the harm of a potential security robbery and hacking inside an IT structure or office. An occurrence taking care of administration for IT plan offers specialized associations with the opportunity to ensure their standing and decrease the expenses of a potential security break. It permits them to have a lot more secure climate away from network safety dangers and dangers.

If we like it, digital occurrences will keep on being an unavoidable piece of our cutting edge world. These assaults will endeavor to increase undesirable admittance to private frameworks that can at last bring about a significant security penetrate. For that, IT experts ought to have the option to make an adequate episode dealing with administration plan. Thusly, a powerful way to deal with tending to network safety issues and assaults can be made conceivable, as well. In this guide, we'll show you what episode dealing with administration for IT plan is and how significant it is for your association.

WHY INCIDENT HANDLING SERVICE FOR IT IS IMPORTANT

1. Prepares you in times of emergencies - When security issues occur, usually, panic strikes, too. With an effective incident handling service for IT plan, however, you and your team can keep your cool in times of crisis. Since you've already outlined how you'll manage and assess these problems, you'll be able to solve them with a clear mind and a sufficient approach.
2. Mitigates the aftermath of a security incident - The aftermath of a security breach can be disastrous to an organization. This can range from increased downtime to financial and data losses. With a sufficient incident handling service for IT plan, your organization can outline remediation processes that can help you mitigate the damage of a potential security breach.
3. Improves relationships with clients and customers - Security incidents can take a huge toll on your business brand reputation. This means that the consequences and aftermath of a cyber attack can help you lose potential key clients, customers, and business opportunities. Therefore, creating an effective incident handling service for IT plan is crucial in maintaining a good relationship with key clients, business partners, and investors.

SIX STEPS FOR EFFECTIVE INCIDENT RESPONSE

- Planning - The main period of episode reaction is getting ready for an inescapable security break. Readiness assists associations with deciding how well their CIRT will have the option to react to an occurrence and ought to include strategy, reaction plan/system, correspondence, documentation, deciding the CIRT individuals, access control, devices, and preparing.

- Recognizable proof - Identification is the cycle through which occurrences are distinguished, preferably instantly to empower quick reaction and thusly diminish expenses and harms. For this progression of viable episode reaction, IT staff accumulates functions from log records, observing devices, blunder messages, interruption recognition frameworks, and firewalls to distinguish and decide occurrences and their extension.

- Control - Once an occurrence is recognized or distinguished, containing it is a first concern. The primary reason for control is to contain the harm and keep further harm from happening (as noted in sync number two, the previous episodes are recognized, the sooner they can be contained to limit harm). Note that all of SANS' suggested ventures inside the control stage ought to be taken, particularly to "forestall the obliteration of any proof that might be required later for indictment." These means incorporate momentary regulation, framework back-up, and long haul control.

- Destruction - Eradication is the period of compelling occurrence reaction that involves eliminating the danger and reestablishing influenced frameworks to their past state, in a perfect world while limiting information misfortune. Guaranteeing that the correct advances have been taken to this point, including measures that eliminate the malignant substance as -

well as guarantee that the influenced frameworks are totally perfect, are the fundamental activities related with destruction.

- Recuperation - Testing, checking, and approving frameworks while returning them to creation so as to confirm that they are not re-tainted or traded off are the fundamental undertakings related with this progression of occurrence reaction. This stage likewise incorporates dynamic regarding the time and date to reestablish activities, testing and confirming the undermined frameworks, observing for strange practices, and utilizing apparatuses for testing, checking, and approving framework conduct.

- Exercises Learned - Lessons learned is a basic period of occurrence reaction since it assists with instructing and improve future episode reaction endeavors. This is the progression that offers associations the chance to refresh their episode reaction plans with data that may have been missed during the occurrence, in addition to finish documentation to give data to future occurrences. Exercises learned reports give an away from of the whole episode and might be utilized during recap gatherings, preparing materials for new CIRT individuals, or as benchmarks for correlation.

10 types of security incidents and how to handle them

1. Unauthorized attempts to access systems or data

To prevent a threat actor from gaining access to systems or data using an authorized user's account, implement two-factor authentication. This requires a user to provide a second piece of identifying information in addition to a password. Additionally, encrypt sensitive corporate data at rest or as it travels over a network using suitable software or hardware technology. That way, attackers won't be able to access confidential data.

2. Privilege escalation attack

An attacker who attempts to gain unauthorized access to an organization's network may then try to obtain higher-level privileges using what's known as a *privilege escalation exploit*. Successful privilege escalation attacks grant threat actors privileges that normal users don't have.

Typically, privilege escalation occurs when the threat actor takes advantage of a bug, configuration oversight and programming errors, or any vulnerability in an application or system to gain elevated access to protected data.

This usually occurs after a hacker has already compromised a network by gaining access to a low-level user account and is looking to gain higher-level privileges -- i.e., full access to an enterprise's IT system -- either to study the system further or perform an attack.

To decrease the risk of privilege escalation, organizations should look for and remediate security weak spots in their IT environments on a regular basis. They should also follow the principle of least privilege -- that is, limit the access rights for users to the bare minimum permissions they need to do their jobs -- and implement security monitoring. Organizations should also evaluate the risks to their sensitive data and take the necessary steps to secure that data.

3. Insider threat

This is a malicious or accidental threat to an organization's security or data typically attributed to employees, former employees or third parties, including contractors, temporary workers or customers.

To detect and prevent insider threats, implement spyware scanning programs, antivirus programs, firewalls and a rigorous data backup and archiving routine. In addition, train employees and contractors on security awareness before allowing them to access the corporate network. Implement employee monitoring software to reduce the risk of data breaches and the theft of intellectual property by identifying careless, disgruntled or malicious insiders.

4. Phishing attack

In a phishing attack, an attacker masquerades as a reputable entity or person in an email or other communication channel. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including extracting login credentials or account information from victims. A more targeted type of phishing attack known as *spear phishing* occurs when the attacker invests time researching the victim to pull off an even more successful attack.

Effective defense against phishing attacks starts with educating users to identify phishing messages. In addition, a gateway email filter can trap many mass-targeted phishing emails and reduce the number of phishing emails that reach users' inboxes.

5. Malware attack

This is a broad term for different types of malicious software (malware) that are installed on an enterprise's system. Malware includes Trojans, worms, ransomware, adware, spyware and various types of viruses. Some malware is inadvertently installed when an employee clicks on an ad, visits an infected website or installs freeware or other software.

Signs of malware include unusual system activity, such as a sudden loss of disk space; unusually slow speeds; repeated crashes or freezes; an increase in unwanted internet activity; and pop-up advertisements. Installing an antivirus tool can detect and remove malware. These tools can either provide real-time protection or detect and remove malware by executing routine system scans.

6. Denial-of-service (DoS) attack

A threat actor launches a DoS attack to shut down an individual machine or an entire network so that it's unable to respond to service requests. DoS attacks do this by flooding the target with traffic or sending it some information that triggers a crash.

An organization can typically deal with DoS attack that crashes a server by simply rebooting the system. In addition, reconfiguring firewalls, routers and servers can block any bogus traffic. Keep routers and firewalls updated with the latest security patches.

Also, application front-end hardware that's integrated into the network can help analyze and screen data packets -- i.e., classify data as priority, regular or dangerous -- as they enter the system. The hardware can also help block threatening data.

7. Man-in-the-middle (MitM) attack

A man-in-the-middle attack is one in which the attacker secretly intercepts and alters messages between two parties who believe they are communicating directly with each other. In this attack, the attacker manipulates both victims to gain access to data. Examples of MitM attacks include session hijacking, email hijacking and Wi-Fi eavesdropping.

Although it's difficult to detect MitM attacks, there are ways to prevent them. One way is to implement an encryption protocol, such as TLS (Transport Layer Security), that provides authentication, privacy and data integrity between two communicating computer applications. Another encryption protocol is SSH, a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.

Enterprises should also educate employees to the dangers of using open public Wi-Fi, as it's easier for hackers to hack these connections. Organizations should also tell their workers not to pay attention to warnings from browsers that sites or connections may not be legitimate. Companies should also use VPNs to help ensure secure connections.

8. Password attack

This type of attack is aimed specifically at obtaining a user's password or an account's password. To do this, hackers use a variety of methods, including password-cracking programs, dictionary attack, password sniffers or guessing passwords via brute force (trial and error).

A password cracker is an application program used to identify an unknown or forgotten password to a computer or network resources. This helps an attacker obtain unauthorized access to resources. A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password.

To handle passwords attack, organizations should adopt multifactor authentication for user validation. In addition, users should use strong passwords that include at least seven characters as well as a mix of upper and lowercase letters, numbers and symbols. Users should change their passwords regularly and use different passwords for different accounts. In addition, organizations should use encryption on any passwords stored in secure repositories.

9. Web application attack

This is any incident in which a web application is the vector of the attack, including exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms. One example of a web application attack is a cross-site scripting attacks. This is a type of injection security attack in which an attacker injects data, such as a malicious script, into content from otherwise trusted websites.

Enterprises should review code early in the development phase to detect vulnerabilities; static and dynamic code scanners can automatically check for these. Also, implement bot detection functionality to prevent bots from accessing application data. And a web application firewall can monitor a network and block potential attacks.

10. Advanced persistent threat (APT)

An APT is a prolonged and targeted cyberattack typically executed by cybercriminals or nation-states. In this attack, the intruder gains access to a network and remains undetected for an extended period of time. The APT's goal is usually to monitor network activity and steal data rather than cause damage to the network or organization.

Monitoring incoming and outgoing traffic can help organizations prevent hackers from installing backdoors and extracting sensitive data. Enterprises should also install web application firewalls at the edge of their networks to filter traffic coming into their web application servers. This can help filter out application layer attacks, such as SQL injection attacks, often used during the APT infiltration phase. Additionally, a network firewall can monitor internal traffic.

An occurrence reaction group (IRT) or crisis reaction group (ERT) is a gathering of individuals who get ready for and react to any crisis episode, for example, a cataclysmic event or an interference of business tasks. Occurrence reaction groups are regular in broad daylight administration associations just as in different associations, either military or strength. This group is commonly made out of explicit individuals assigned before an episode happens, albeit in specific situations the group might be a specially appointed gathering of willing volunteers.

Occurrence reaction colleagues in a perfect world are prepared and arranged to satisfy the jobs needed by the particular circumstance (for instance, to fill in as episode leader in case of a huge scope public crisis). As the size of an occurrence develops, and as more assets are brought into the function, the order of the circumstance may move through a few stages. In a little scope function, typically just a volunteer or specially appointed group may react. In functions, both huge and little, both explicit part and impromptu groups may work together in a bound together order framework. Singular colleagues can be prepared in different parts of the reaction, either be it clinical help/emergency treatment, unsafe material spills, prisoner circumstances, data frameworks assaults or catastrophe alleviation. Preferably the group has just characterized a convention or set of activities to perform to alleviate the negative impacts of the occurrence.

An episode reaction group (IRT) or crisis reaction group (ERT) is a gathering of individuals who get ready for and react to any crisis occurrence, for example, a catastrophic event or an interference of business tasks. Episode reaction groups are basic in broad daylight administration associations just as in different associations, either military or strength. This group is commonly made out of explicit individuals assigned before an occurrence happens, albeit in specific situations the group might be a specially appointed gathering of willing volunteers.

Who's on the occurrence reaction group?

We've assembled the center elements of an occurrence reaction group in this convenient realistic. Since each organization will have contrastingly estimated and talented staff, we referred to the center capacities versus the possible titles of colleagues. So you may locate that a solitary individual could satisfy two capacities, or you should commit more than one individual to a solitary capacity, contingent upon your group cosmetics. All things considered, here are a couple of other key contemplations to remember: IT leads with solid chief help and between departmental support.

With regards to network protection occurrence reaction, IT should be driving the episode reaction exertion, with chief portrayal from each significant specialty unit, particularly with regards to Legal and HR. While the dynamic individuals from the group will probably not be senior chiefs, plan on requesting that heads partake in significant enlistment and correspondences endeavors. Unmistakably characterize, report, and convey the jobs and duties regarding each colleague.

While we've given general capacities like documentation, correspondence, and examination, you'll need to get more explicit while plotting your colleague jobs. Ensure that you record these jobs and plainly impart them, so your group is very much organized and recognizes what is anticipated from them - before an emergency occurs.

Build up, affirm, and distribute correspondence channels and meeting plans. Viable correspondence is the subtle strategy for any task, and it's particularly valid for episode reaction groups. Print out colleague contact data and circulate it generally (don't simply depend on delicate duplicates of telephone registries. Odds are, you might not approach them during a security episode). Incorporate significant outer contacts also, and try to talk about and report when, how, and who to contact at outside substances, for example, law requirement, the media, or other occurrence reaction associations like an ISAC.