The Enemy From Within - A Treatise on Insider Threats and Network Security

Adewusi, Michael Adelani
African Centre for Innovative STEM Education (ACEITSE)
Lagos State University
Ojo, Lagos State, Nigeria
E-mail: mikeade3000@yahoo.com
Phone: +2348115800375

Abstract

A security danger that originates within the targeted organisation or firm is known as an insider threat. This is not to say that the actor has to be a current employee or executive of the company. It could be a consultant, a former employee, a business partner, or a member of the board of directors and so on. To safeguard the organisation or firm from insider risks, you must first understand what constitutes an internal danger.This chapter provides insights into types of insider threats, what constitutes insider threats with particular reference to network security as well as mitigating techniques to combat them

Keywords: Cyberspace, Cyber criminals, Cybercrimes, Cyber resilience, Automation, Security

Introduction

Insider threats remains a very present, constant and potent danger to organizationa, institutional, business, corporate, private and public information technology infrastructure. An insider threat is a harmful danger to an organization that arises from insiders, such as employees, former employees, contractors, or business allies, who have inside information about the organization's security processes, data, and computer systems. Fraud, theft of confidential or commercially valuable information, theft of intellectual property, or sabotage of computer systems are all possible threatsTurn-cloaks and pawns, which are evil insiders and unwilling participants, respectively, are the two basic categories of insider threats (Balakkrishman, 2015; Al tabash & Happa, 2018).).

Plans for Defending Against Insider Threats and Responding to Them

To defend against insider threats, the following must be observed:

1. Keep an eye on your main data sources' files, emails, and activity.
2. Find out where your sensitive data are stored and locate them.
3. Determine who has access to the information and who should have access to the information.

Citation Adewusi, M.A. (2022). The Enemy From Within - A Treatise on Insider Threats and Network Security.
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series
Book Chapter on Web of Deceit - African Multistakeholders' Perspective on
Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical
and Design Approaches. Pp 265 -272. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P45

4. Use your infrastructure to implement and maintain a least privilege model.
   a) Get rid of the Global Access Group;
   b) Make data owners responsible for controlling permissions for their data, and make temporary access expire soon.
5. Apply security analytics to alert on abnormal behaviors including:
   a) Attempts to access sensitive data that is not part of normal job function
   b) Attempts to gain access permissions to sensitive data outside of normal processes
   c) Increased file activity in sensitive folders
   d) Attempts to change system logs or delete large volumes of data
   e) Large amounts of data emailed out of the company, outside of normal job function
6. Socialize and train your employees to adopt a data security mindset

Types of Insider Threats

There are three types of insider threats:

a. Malicious insiders, which are people who take advantage of their access to inflict harm on an organization;
b. Negligent insiders, which are people who make errors and disregard policies, which place their organizations at risk; and
c. Infiltrators, who are external actors that obtain legitimate access credentials without authorization.

Xprobe

This is a viable alternative to some programs that rely largely on the TCP protocol to do remote active operating system fingerprinting. When TCP is utilized in the fingerprinting process, this is especially true when trying to identify various Microsoft-based operating systems. Since the TCP implementation with Microsoft Windows XP and Microsoft Windows 2000, fingerprinting processes have been unable to distinguish between various Microsoft-based operating system groups when using the TCP protocol with a remote active operating system (Sourceforge, 2021; Ofirarkin, 2021).

Xprobe probes can be extremely undetectable. Unlike conventional fingerprinting approaches, Xprobe does not send any corrupted datagrams to discover a distant OS type. Xprobe looks for legitimate packets in the remote OS TCP/IP stack answers. On a daily basis, thousands of such packets emerge in the ordinary network, and only a few IDS systems are calibrated to identify them. When people observe the types of datagrams utilized by Xprobe, they usually assume it is just a simple Host Detection attempt, when in fact the responding computers were not only discovered, but their underlying operating systems were also revealed (Sourceforge, 2021; Ofirarkin, 2021).

The practice of footprinting (reconnaissance) is used to obtain information about computer systems and the entities to which they belong. A hacker could utilize a variety of methods and technology to obtain this information. This information is extremely important to a hacker attempting to break into an entire system. "Footprinting" is a term used in the computer security world to describe one of the pre-attack phases, or tasks completed before the actual attack. Sam Spade, nslookup, traceroute, Nmap, and neotrace are some of the Footprinting tools (knowledgeHut, 2020; EC-Council, 2021; Pluralsight, 2021).

It enables a hacker to obtain access to data on the target system or network. This data can be used to launch attacks against the system. Because all of the information is evaluated in order to acquire a comprehensive and successful resolution of the attack, it may be referred to as a Pre-Attack. Ethical hackers and penetration testers employ fingerprinting to uncover security weaknesses and vulnerabilities in their own network before a malevolent hacker does (knowledgeHut, 2020; EC-Council, 2021; Pluralsight, 2021).

The practice of gathering as much knowledge as possible about the target system in order to find ways to break into it. The majority of an ethical hacker's time is spent profiling an organization, acquiring knowledge about the host, network, and people associated with the company. IP addresses, Whois data, DNS information, the OS system utilized, employee email ids, and phone numbers, among other things, are collected (knowledgeHut, 2020; EC-Council, 2021; Pluralsight, 2021).

Footprinting helps to

- Know Security Posture – The data gathered will help us to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications and so on
- Reduce Attack Area – Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems we are focussing on
- Identify vulnerabilities – we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization
- Draw Network map – helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information.

LaBrea – Deterrence

LaBrea is a well-known network scanning deterrence tool that continues to show how active security measures can be used to restrict the spread of wormable malware and frustrate attackers. LaBrea works by scanning the network for ARP queries and creating a new packet with a bogus MAC address for each one that goes unanswered, effectively filling in the unused address space within a switch. When LaBrea is pinged, it will respond to every request on every port with a TCP window size of 0 and will wait for port scans on address space it has filled (which severely slows down the port scan).

LaBrea Demonstration

In risk3sixty's demo, LaBrea was set up in a test network with limited infrastructure and limited nodes all assigned IP addresses via static assignment. Please note that proper planning would need to be completed before setting LaBrea up in an environment using DHCP. They first scanned the network with NMAP using *nmap -sV -n -v -Pn -p- -T4 192.168.1.0/24.* The result was as expected. The scan moved at an unreasonably slow pace. Nmap immediately had difficulty handling the responses and based on the processing speed, it may have taken over a week to scan a /24 network. This type of port scanning is like the behavior you might expect from wormable malware looking for hosts with specific vulnerable ports open to attack.

Advanced Persistent Threat (APT)

This is a sneaky threat actor, usually a nation state or a state-sponsored group, that gains unwanted access to a computer network and goes undiscovered for a long time. In recent years, the phrase has also been used to describe non-state supported groups that carry out large-scale targeted incursions with specified objectives (Wikipedia, 2021). The motivations of such threat actors are either political or economic.

Cyberattacks by advanced actors with explicit purposes of stealing, spying, or disrupting have been documented in every major corporate sector. Government, defense, financial services, legal services, industrial, telecoms, consumer products, and other sectors are among them. Traditional espionage vectors like as social engineering, human intelligence, and infiltration are used by some entities to obtain access to a physical place and enable network attacks. The goal of these attacks is to infect computers with bespoke malware (Wikipedia, 2021). An advanced persistent threat (APT) is a generic term for an attack operation in which an intruder, or a group of intruders, establishes a long-term unlawful presence on a network in order to harvest extremely sensitive data. The targets of these attacks, which are meticulously selected and researched, are usually huge corporations or government networks.

The consequences of such intrusions are vast, and include:

- Intellectual property theft (e.g., trade secrets or patents);
- Compromised sensitive information (e.g., employee and user private data);
- The sabotaging of critical organizational infrastructures (e.g., database deletion);
- Total site takeovers

An APT attack takes more resources to carry out than a normal web application attack. The culprits are usually groups of well-funded cybercriminals with a lot of experience. APT attacks are sometimes supported by the government and employed as cyber warfare weapons.

APT attacks differ from traditional web application threats, in that:

- They are significantly more complex;
- They are not hit and run attacks - once a network is infiltrated, the perpetrator remains in order to attain as much information as possible;
- They are manually executed (not automated) against a specific mark and indiscriminately launched against a large pool of targets;
- They often aim to infiltrate an entire network, as opposed to one specific part.

Perpetrators typically use more conventional techniques like remote file inclusion (RFI), SQL injection, and cross-site scripting (XSS) to gain a foothold in a targeted network. Trojans and backdoor shells are frequently employed to further establish a foothold and establish a persistent presence within the targeted perimeter (Imperva, 2021).

Progression

A successful APT attack can be broken down into three stages: network infiltration, the expansion of the attacker's presence and the extraction of amassed data. All without being detected.

Stage 1 – Infiltration

Web assets, network resources, or authorized human users are the three attack surfaces most commonly used to breach organisations or businesses. This is accomplished by malicious uploads (e.g., RFI, SQL injection) or social engineering assaults (e.g., spear phishing), both of which are common risks to large organisations or businesses. Infiltrators may also launch a DDoS assault on their target at the same time. This can be used as a distraction for network staff as well as a way to undermine a security perimeter, making it easier to infiltrate. After gaining initial access, the attackers swiftly install a backdoor shell, malware that enables network access and allows for stealthy activities from afar. Trojans disguised as legal software can also be used to install backdoors.

Stage 2 – Expansion

Attackers expand their presence within the network once they have secured a foothold. This entails climbing the corporate ladder and compromising employees who have access to the most sensitive information. They can collect vital business information, such as product line information, employee data, and financial records, this way.

The gathered data can be sold to a competitor, manipulated to destroy a company's product line, or utilized to bring down an entire organization, depending on the ultimate attack target. If sabotage is the goal, this phase is used to obtain control of a number of vital functions and modify them in a certain order in order to cause the most damage. For example, in order to prolong the recovery process, attackers could wipe whole databases within a corporation and then impair network connectivity.

Stage 3 – Extraction

While an APT attack is ongoing, stolen data is often stored in a secure area within the network under attack. Once they have gathered enough information, the thieves must extract it without being noticed.

White noise strategies are commonly used to distract security personnel so that the data can be transported out. This could take the shape of a distributed denial-of-service (DDoS) attack, tying up network staff and/or weakening site defenses in order to assist extraction.

Packet sniffer to rescue?

A packet sniffer, also known as a packet analyzer, protocol analyzer, or network analyzer, is a device that monitors network traffic using hardware or software. Sniffers analyze data packet streams that pass between computers on a network, as well as between networked systems and the greater Internet. These packets are intended for and addressed to specific devices, but in "promiscuous mode," a packet sniffer allows IT professionals, end users, or malevolent intruders to study every packet, regardless of destination. Sniffers can be configured in two different ways. The first is "unfiltered," which means they will capture all possible packets and save them to a local hard drive for subsequent analysis. Then there's "filtered" mode, which means analyzers will only record packets with particular data items.

Both wired and wireless networks can benefit from packet sniffers. Their effectiveness is determined by how much "seeing" they can do as a result of network security mechanisms. Sniffers on a wired network may have access to the packets of every connected machine or may be limited by network switch location. Most sniffers can only scan one channel at a time on a wireless network, however using several wireless interfaces can enhance this capabilities.

Prevalence and Risk Factors

It is possible to acquire practically any information using a sniffer. For instance, which websites a user accesses, what is seen on the site, the contents and destination of any communication, as well as information about any downloaded files. Protocol analyzers are commonly used by organisation or businesses to maintain track on employee network usage and are included in many reliable antivirus software packages. Outward-facing sniffers look for specific bits of dangerous code in incoming network traffic, assisting in the prevention of computer virus infections and the spread of malware.

However, it is worth remembering that these analyzers can also be used maliciously. It is feasible for an unauthorized packet sniffer to be installed on a corporate network if a user is persuaded to download malware-laden email attachments or infected files from a website. The packet sniffer, once installed, can record any data sent and relay it to a command and control (C&C) server for further analysis. Hackers might then try packet injection or man-in-the-middle attacks, as well as compromise any data that was not encrypted before being transferred (Kaspersky, 2021). Packet sniffers used correctly can assist clean up network traffic and reduce malware infections; nevertheless, intelligent security software is required to protect against malicious use.

Insider threat detection field case studies

Scenario 1

Following a recent security incident, the company began an internal investigation into an employee's flagrant breach of policies and employment contract. The organization has suspended all access for the employee, who will be taken from the premises immediately, because they believe they cannot accept the risk of providing the employee continuous access to the organization's resources (e.g., workstation, e-mail, files). The company has decided that the employee's services are no longer necessary, and the contract will be terminated as soon as possible. The person in question will receive all of his or her personal stuff. Can the employer immediately revoke all access to resources (to avert any additional possible harm) without giving the employee a grace period to complete any outstanding tasks?

Suggestion

The employer should check the employment contract to verify that it includes a clause stating that if a breach or data misuse is discovered, all access privileges will be promptly revoked after the employment contract is terminated. The requirements for such access may be further detailed in the employment contract depending on the nature of the employee's activities and on having access to relevant systems. For example, the employer may want to declare that all access permissions are revoked as soon as misbehavior is discovered, or even as soon as the first suspicions are raised. This way, even before the official employment contract is terminated, the employee will not be able to access work-related systems.

Scenario 2

An employee has applied for a job with another company and has submitted a resignation letter. In 30 days, the job contract will expire. Meanwhile, the employee will continue to perform his tasks and has been told to turn in any incomplete work to a coworker who has been appointed to replace him. Employees are most likely to steal intellectual property or other important data within the last 30 days before leaving the organization. Employees who are leaving or displaying other non-technical symptoms are being monitored by the security staff. Is it permissible for the organization's security officer to choose users for in-depth data stream monitoring on a case-by-case basis?

Suggestion

The employer must verify that the logic and circumstances for possible ad hoc monitoring are included in the employment contract or internal rule, and that they are legal. If such monitoring is carried out, it must be documented and the person being checked must be identified. When checking the employee's data, a second person (preferably the Data Protection Officer) should be present to avoid any complications.

Scenario 3

In response to an unusually high number of file retrievals from the organization's file server, the automated security monitoring system has produced an alert for a workstation. This was followed by a notification from the organization's e-mail server that an e-mail with multiple large attachments had been sent from the same workstation to an external address. This sequence of events could imply data exfiltration, but the security officer would need to access the work mailbox and view the e-mail to verify the purpose and legality of the contents in order to examine these alarms. There is a chance the alert is a false positive, which is not necessarily a good reason to invade someone's privacy. This type of automated monitoring system frequently necessitates human intervention in data interpretation. Can a security officer intrude on a person's privacy based on suspicions derived from monitoring system alerts?

Suggestion

To take advantage of the broader breadth of monitoring rights, the employer should not allow private use of devices. This prohibition should be monitored on a regular basis to avoid the emergence of contrary but tolerated behavior, which could eventually become a common practice. As a result of this prevalent practice, data control choices are limited, as it is seen as the same as when an employer permits personal usage of the device. As previously stated, the employer must guarantee that the logic and criteria for such monitoring (even if done on an irregular basis as spot checks) are included in the employment contract or internal regulation, and that they are legal. Email must be as transparent as possible if it is to be used for both private and corporate communication. The company could, for example, compel the employee to delete personal emails once they have been sent or received, to clearly identify private emails, or to store them in a separate folder reserved for private use.

'Proportionate controlling' may be implemented if the employer has authorized the private use of gadgets provided by the company. This means that an agreement could be reached allowing limited access to certain service providers such as Gmail or Yahoo!, making it easier for the employee to distinguish between personal and work-related communication. Of course, such restrictions would not prohibit the employee from transmitting corporate data in an unauthorized manner. The four-eye-principle should be used to monitor the content of emails, and the findings should be recorded, detailing why and to what degree emails have been opened and read. The company's Data Protection Officer should be the second person. The company might also consider making it clear that using a personal email account for work-related correspondence is prohibited.

Scenario 4

The Security Officer (SO) must acquire visibility of the encrypted data streams in order to ensure that no sensitive data is leaving the organization's network. This would also enable him to conduct more thorough investigations into security events if any suspicions surface. A man-in-the-middle proxy must be installed and all traffic coming from the organization's network must be routed via it to create a first level of security. However, this technique is ineffective when the sender has already encrypted data (such as a file) before sending it across the network. To remedy this, employees' self-generated private cryptographic keys for storing and transmitting encrypted data would need to be acquired. The SO wants to implement a new internal policy that requires workers to hand over any cryptographic keys they use at work. Is it possible for the SO to demand that employees hand over their private cryptographic keys, which might be used to decrypt any intercepted data?

Suggestion

To avoid problems with accessing the system in general, the employer should make sure that private cryptographic keys are not used for work-related operations, or that cryptographic keys are shared with a trusted person (such as a Data Protection Officer) and stored securely.

Scenario 5

The security team wants to implement new security checks to ensure that staff who work with sensitive data do not save any of it on their mobile devices (phones, tablets, etc.). This would be against company policy, as well as putting data at danger of theft or malware, which is growing more widespread on mobile devices. To ensure that important staff comply with laws and regulations, security checks would compel them to handover their communication devices (both personal and those assigned by their business). Employers frequently allow employees to bring their own gadgets to the office and use them in the workplace. Alternatively, even if the gadget is provided by the employer, it may still contain some personal information due to human factors (e.g., messages, e-mails, etc.). Is it permissible to conduct random security checks to see what kind of data is kept on and transferred via a personal or employer-owned mobile device?

Suggestion

The employer should always supply a company gadget to the employee and expressly ban its personal use (in the employment contract or internal regulations). If the employee has the right to keep the device until the contract is terminated, the employer may prefer to risk being sued for damages rather than risk the employee deleting not just personal but also business data on the device that he or she is meant to return.

Scenario 6

The Security Officer wants to start doing regular (forensic) inspections on equipment that are maintained by third-party vendors. He does not want to tell the contractors about the checks since he does not want to alarm them and cause more problems. Is it permissible for the security team to undertake forensic investigations on any devices provided by contractors (for example, a water cooler or coffee machine in the security area)?

Suggestion

Regular forensic efforts must be agreed upon in advance in the service provider's contract. To avoid eavesdropping, gadgets such as coffee makers, copying machines, and water coolers should be situated in areas where business conversations are not normally held. In the case of other dangers (noise-disturbing mechanisms, automatic email transmission of scanned or copied documents from a high-tech copy machine), particular procedures to inspect the device should be considered prior to finalizing the contract in order to amend the basic contract's general provisions. The gadget should be examined on a regular basis, and this could be agreed upon in the contract, for example, in exchange for the provider's attendance.

Scenario 7

On the organization's network, the security team is interested in setting up decoy targets. Those targets are just simulating scenarios where some ostensibly sensitive and valuable data is actively stored and manipulated, and they are not used or necessary for normal work. These targets' data accesses and transmissions will be watched and logged for further analysis. Is it legal for an employer to set up decoy targets (honeypots) within their company? Can the security team create custom honeypots that would appear more attractive to the suspected individual, and optionally direct the said person to it, if there is a concern that an employee is straying over boundaries?

Suggestion

The employer should always consult with a lawyer about his precise plans, as he could wind up committing a criminal himself if he does not.

Conclusion

Insider threats are a big concern for all organizations, including the government and the military. A recurring study topic has been developing an effective mitigation method to fight the problem. Issues with anomaly detection (AD), such as network intrusion detection (NID), and so on. This study examines insider threat strategies, proposes detection solutions, and provides scenarios with threat detection suggestions. It also proposes a strategy as the way forward for insider threat detection for the benefit of humans.

References

1. K. Al tabash and J. Happa, (2018). "Insider - threat Detection using Gaussian Mixture Models and Sensitivity Profiles," Computer & Security.
2. B. Balakkrishman, (2015). "Insider Threat Mitigation Guidance," The SANS Institute, 2015.
3. Ofirarkin, (2021). https://ofirarkin.wordpress.com/xprobe. Retrieved 23rd March, 2021
4. Sourceforge, (2021). https://sourceforge.net/projects/xprobe. Retrieved 23rd March, 2021.
5. knowledgeHut, (2020). Introduction to Footprinting and Reconnaissance in Ethical Hacking. https://www.knowledgehut.com/blog/security/footprinting-ethical-hacking Retrieved 23rd March, 2021
6. EC-Council, (2021). Footprinting and Reconnaissance. https://ilabs.eccouncil.org/footprinting-reconnaissance. Retrieved on 23rd March, 2021.
7. Pluralsight, (2021). Ethical Hacking: Reconnaissance/ Footprinting.
8. https://www.pluralsight.com/courses/ethical-hacking-reconnaissance. Retrieved on 23rd March, 2021.
9. Imperva, (2021). Remote file inclusion (RFI).
10. https://www.imperva.com/learn/application-security/rfi-remote-file-inclusion. Retrieved on 23rd March, 2021
11. Kaspersky, (2021). Kaspersky Anti-Virus. https://www.kaspersky.co.za/antivirus. Retrieved 23rd March, 2021.