Serianu Cybersecurity Advisory

Overview

One third of all cybersecurity breaches will be caused by an **insider threat**. Insider threats are a prevailing and growing problem both on a regional and global standpoint. An insider threat can be defined as an attack carried out by a user or a malicious code that is already inside a defended perimeter of a system or organization.

Insider threats are some of the most devious attack vectors due to their subtlety and covert nature. They highly go undetected and take longer to contain as attackers compromise valid systems, users and processes in a network or organization, with most recent methods deploying *Living Off the land* tactics and techniques. Recent reports show threat actors can exist in victim networks for as long three years without being detected.

In most cases the threat actors know how the system/network is configured, its crown jewels and its weaknesses. They can easily clear their tracks and take over accounts. Whereas an external attacker has to breach a firewall and learn the system, an internal threat actor already knows how the system is configured.

Additionally, attackers leverage ***supply chain attacks*** to compromise vendor software and products exploiting customers' trust and connectivity to breach their networks. As companies increasingly rely on outside vendors for IT services, cloud computing among other services, they must grapple with the wider pool of potential risky players inside their networks, as essentially, they are outsourcing security trust to these third parties.

Types of Insider Threats

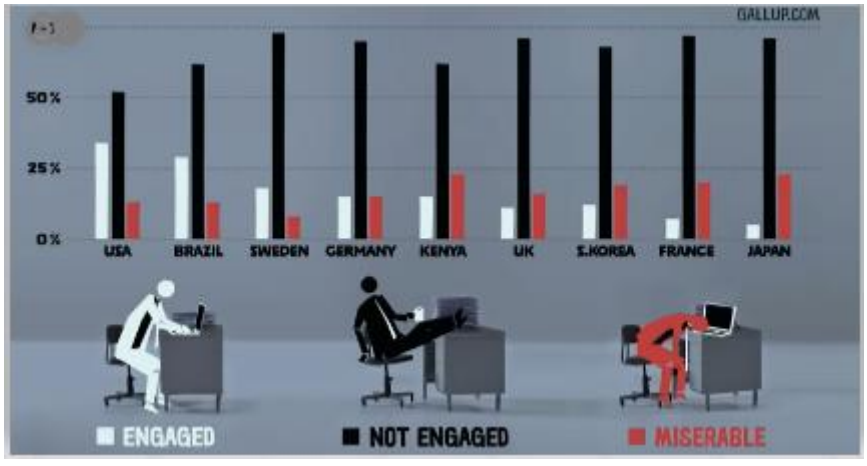
Insider Threats have greatly been exacerbated by increased remote working, supply chain compromise, cloud computing and other emerging technologies like AI and Internet of Things. Remote work and interconnectivity of devices has pushed work-related data and devices beyond offices and onto employees' home and social networks.

Some of the main categories of insider threats include;

1. **Malicious Insiders** – Actors who intentionally cause harm to an organization.
2. **Negligent Insiders** – Individuals within an organization with privileged access that intentionally or unintentionally expose systems and software to outside threats. These mostly fall to security mistakes like falling victim to phishing scams.
3. **Compromised Insiders** – Individuals whose credentials have been compromised by external threat actors.
4. **Third-party Insiders** – Risks to an organization stemming from someone/entity associated with the organization such as product vendor or contractor.
5. **Unintentional Insiders** – Also known as accidental insider threats are employees who pose a risk to an organization without malicious intent but end up compromising organizational security through negligence, errors or a lack of awareness.

Disgruntled employees forming a huge part of insider threat activity can be motivated by various factors such as; Financial gain, revenge, ideology or belief, coercion, ego, notoriety and extortion among others.

According to a Gallup poll, regionally just 13% of the working population endeavor to perform well in their job. However, 64% of employees don't care about their work and aim to get through the day with minimum effort. 25% of workers hate their jobs so much they even work against the company that employs them. Although the numbers vary from country to country, these trends can be observed all over the world.



Detecting Insider Threats

While most companies have adequate processes in place to protect against outside threats, most lack systems that protect the company's assets against its own employees. Through studies carried out on the subject, the best way of approaching this would be trying to understand and focus on the specific intent of the attacker.

Below are some of the detection mechanisms of insider threat activity using security controls deployed on the network.

Incident Detection using Security Information and Event Management (SIEM)

1. **Monitoring Abnormal Authentication Attempts**

Acceptable monitoring should be configured to capture what resources are being accessed by whom and when. Organizations should describe a security policy that addresses threshold limits, user roles, responsibilities and sensitive information.

Any authentication attempt outside the defined policy can be considered abnormal authentication and therefore should be picked as a security alert. SIEM use cases have been implemented to track such login attempts automatically.

2. **Detecting Data Exfiltration Attempts Made through USB or other External Disks**

Data Exfiltration is the unauthorized transfer of data from one host to another host. A malicious actor can use removable storage devices such as USB or Hard disk to transfer sensitive data if they have access to the target system.

To monitor and detect such data exfiltration attempts in a windows environment, you need to configure Windows event logs to record Windows security event ID **4663** on the Event Viewer on the AD (Active Directory) to enable monitoring of Removable Devices.

Companies can also adopt robust protections around restrictions to workstations that allow third party media such as USBs, CDs e.t.c

3. **Detecting Data Exfiltration Attempts Made through FTP (File Transfer Protocol)**

An attacker can infiltrate data over FTP. Various networks do not have firewall rules to restrict outbound connections thereby allowing intruders to get away with critical organization's data. Moreover, most operating systems have inbuilt FTP client so intruders do not have to install additional tools on the compromised host.

SIEMS should be configured to monitor unencrypted channels. However, if the data is encrypted before transmitting over an unencrypted channel, it becomes difficult to detect this data. Therefore, sending encrypted data over unencrypted channels is a strong indicator of

compromise and can be considered as suspicious activity. Organizations are recommended to flag encrypted data transmitted over unencrypted channels to reduce data exfiltration attempts through these means. It is also important to note that attackers can take advantage of valid FTP processes, therefore key focus should be placed on the source, destination, magnitude, frequency and timing (whether during business or off-business hours) of the FTP transmission.

Most appropriate solution for avoiding data exfiltration over FTP would be adopting a whitelist approach to drop FTP packets if they are not listed on the approved whitelist.

4. **Detecting Data Exfiltration Attempts using Personal Web Mail Accounts**

This tries to detect data exfiltration over email. This can be achieved through classification heuristics to identify whether two emails are related to the same person.

Also observing Behavior-based anomalies based on several factors such as;

- Frequency of data transmission between a corporate sender to an external address.
- Direction of data transmission between a corporate sender and an external sender
- Textual content in the email subject fields.

Based on these factors, metrics can be determined to identify if both corporate/external email addresses are related to the same person.

5. **Detecting Data Deletion Attempts**

Disgruntled users with high privileged (rogue administrators) can delete sensitive data from critical servers.

To detect this you can configure windows to detect such attempts by enabling and configuring Windows Event ID **4660** to detect file/folder deletion events. To reduce high rate of false positives every time a File/Folder is deleted emphasis can be put on critical Files and Folders.

6. **Detecting Account Compromise Attempts**

Password modification activity from users other than legitimate users can be an indication of account compromise.

These activities can be detected by enabling Windows Event ID **628/4724** on the Event Viewer on the AD to detect and log password reset attempts by ***administrator*** and Event ID **627/4723** to detect password change attempted by users.

For more critical assets, password changes can be presided by an approval or sign-off forms.

7. Detecting Access or Modification of Unusual Data

Any attempt to access or modify data from an *unauthorized user* can be an indication of account compromise or insider threat. Authorized personnel can be defined by adopting Access Rights control or Zero-trust approach. In the event that any other user other than the intended users attempt to access this data they will be flagged as unauthorized users.

Based on sensitivity of data/file, an organization can enable detection of access of this data/file by enabling Windows Event ID **4656** to detect access of a particular file, and Windows Event ID **4663** to provide details of the operation performed on the said file/document.

From these logs, security personnel can sift through authorized users and those who are not.

8. Detecting Communication over Private Network (TOR Network)

TOR (The Onion Router) Network can be defined as the network used on the *dark web* designed to enable anonymous communication. This forms the biggest part of the internet as we know it as it is untracked, unmanaged and uncensored. Users can use private network such as TOR Network to hide their malicious intent, ex-filtrate data, connect to malicious peer or command 2 servers e.t.c

In case of Outbound TOR network (data from the TOR network into an organization) it could be an indication of an attack or reconnaissance activity.

In case of Inbound TOR Network traffic (data sent into the TOR network from a user's device) it is an indicator of a potential malicious insider.

This can lead to catastrophic problems to the organization such as information theft, malware, botnet attacks, DDoS attacks or bypassing security controls among others.

It is therefore imperative to monitor, detect and block TOR Traffic.

Some prevention actions to prevent the use of TOR in the network include;

- Prevent installing of the TOR application, by restricting user access rights using security controls
- Create a blacklist of TOR nodes; restricting all outbound traffic related to TOR at the border firewalls.
- Block all traffic using self-signed digital certificates

9. Detecting which IPs are connecting to a specific port

Malicious insiders can try to use or establish a connection to a port or service that is not allowed or is suspicious/sensitive like FTP (port 21) or Telnet (port 23). Upon detecting these IPs, you can block or blacklist them from the network.

To achieve this, you have to determine which ports are *listening* on the network, using **netstat** command; which lists all services that are listening on the ports and also provide information related to any connections made to those ports. Feeding netstat data to the SIEM can help detect such anomalies.

10. Detecting Data Exfiltration Attempts over the Cloud

Insider threat actors can leverage private cloud storage to transfer sensitive data.

Organizations can detect attempts of unauthorized upload of data on cloud storage such as Dropbox and look for username and IP address from which this activity is initiated.

Preventing Insider Threats

Below are some of the ways to protect against Insider Threats;

1. **Principle of Least Privilege** – Ensuring that employees only have access to data and systems that they need and nothing more.
2. **Common or shared Administrative Accounts** – As hard as it may be, it is highly advised not to use *Administrator* usernames on systems or networks as this will act as a low hanging fruit for a potential threat actor. Once this account is compromised it will be difficult to identify exactly who performed the action. This is to enhance *non-repudiation.* Where possible implement a decentralized administration module, where no one core employee has access to all your systems.
3. **Visibility –** Maintain full visibility and monitoring on systems and networks to understand where data is coming from, who is accessing that information and how they are using it or changing it. Ensure you are logging the *right* data from the right sources.
4. **Training –** For employees, train them to work with security awareness in mind so that they do not unknowingly expose sensitive data to the public or are unknowingly hijacked into giving away their access. Further train employees and customers on new and emerging social engineering techniques like *vishing, OTP manipulation, deepfakes, voice and video impersonation.*
5. **Adopt Insider Threat Frameworks –** Where possible adopt frameworks that are designed and focused on detecting insider threat activity through collection of enough information and characteristics on “bad” behavior. These ***User and entity behavior analytics (UEBA)*** use algorithms and machine learning to detect anomalies and identify indicators that differentiate good from “bad” employee behavior.
6. **Supply chain compromise –** Vet third parties properly and ensure they are up to date with the latest security protocols and rules for accessing, sharing and storing information and systems. Have a security third-party policy check metric before on-boarding a third-party on your network.

7. **Suspicious Security Events –** Act and respond to suspicious security events indicating a possible insider threat. These could include but not limited to:
    i. Badging into work at unusual times
    ii. Logging in at unusual times
    iii. Logging in from unusual locations
    iv. Accessing systems/applications for the first time
    v. Copying Large amounts of information.
    vi. Unusual Failed logon attempts to an administrative account.

8. **Multi-factor Authentication** – In case of an account take-over multi-factor authentication will make it much more difficult for an unauthorized user to access sensitive data and further leverage the network.

9. **Security Policies** – Implementing security policies like Maker-Checker systems, password expiry policy, disabling/deletion of user access upon termination, monitoring of dormant accounts and insider threat playbooks among others to act as a guideline and security measure for preventing insider misuse.

Cost of Insider Threats

On average organizations will take more than two months to contain an insider threat, whether through malice, negligence or error.

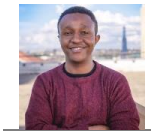
According to Ponemon's study "The Cost of Insider Threats: Global Report" the report shows that insider threats have some of the highest impacts ranging from sensitive government information to long lasting effects on the economy.

- 60% of organizations had more than 30 insider-related incidents per year
- 62% of the insider-related incidents were attributed to negligence
- 23% of the insider-related incidents were attributed to criminal insiders
- 14% of the insider-related incidents were attributed to user credential theft
- Number of insider-related incidents increased by 47% in two years
- Companies spend an average of $755,760 on each insider-related incident

Compromised insiders accounted for 18% of incidents over a 12-month period, while malicious insiders accounted for 26% of incidents, but the majority of incidents related to accidental insiders, at 56%.

Information Sharing

We encourage any organization or individual that has any information related to Insider Threats to share it with us through our email info@serianu.com to further allow us to analyze these cyber threats.



John Kuria
Cybersecurity Researcher, Cyber Threat Intelligence Analyst