Insider Threats

By Caleb Mingle-Taylor,Ramatu Hallie, Omar Elsayyad

What is It ?

An Insider is a person who has/had any authorized access or any knowledge of a company/organization’s resource or assets. That can include their personnel, facilities,information,equipment,networks, and systems. Which could lead to an insider threat where the person could use their authorized access to harm the company/organization

Popular Types/ Variants

Malicious Insiders- These are members of the organization that knowingly abuse their access to data or systems for their own benefit or to cause harm to the company. This can entail stealing private data, undermining systems, or selling private information to rival businesses.

Careless Employee- Employees can inadvertently jeopardize security through incompetence or carelessness. This can entail taking steps like responding to phishing emails, creating weak passwords, or managing private data improperly.

Compromised Accounts- External attackers may use social engineering or phishing techniques to gain access to insiders' accounts. These accounts have the potential to be utilized to get access to private information or company systems once they are compromised.

Insufficient Access Controls- Intrinsic risks might also arise from poorly maintained access control measures. Giving workers more access rights than necessary, neglecting to remove access when workers depart the company, and improperly monitoring access to sensitive data are a few examples of this.

Insider Collusion- Sometimes insiders will work together to get around security measures or steal information. This could entail staff members cooperating to either conceal security vulnerabilities or collect and sell sensitive data.

Disgruntled Employees- Workers that are dissatisfied with their positions or the company could be a serious insider danger. They might try to exact retribution by damaging systems, interfering with operations, or disclosing private information.

How Its Done

- **Access:** The insider gains authorized access to the organization's systems, networks, or data as part of their job responsibilities.
- **Opportunity:** Once inside, the insider identifies an opportunity to misuse their access for personal gain or to cause harm to the organization.
- **Motivation**: The insider may have various motivations for engaging in malicious activities.
- **Execution**: The insider carries out the insider threat by taking actions such as stealing sensitive data, sabotaging systems or networks, installing malware, or leaking confidential information to external parties.
- **Cover-up**: In some cases, insiders may attempt to cover their tracks to avoid detection.
- **Detection:** Insider threats may be detected through various means, including security monitoring tools, anomaly detection algorithms, or reports from other employees.
- **Impact:** The insider threat can have significant consequences for the organization, including financial losses, damage to reputation, regulatory penalties, and loss of customer trust.
- **Response and Mitigation:** Once the insider threat is detected or suspected, the organization must respond promptly to mitigate the damage and prevent further harm.

Notable Occurrences/ Events?

Events that could lead to people being a threat to company is if there is favoritism being played, not proper pay, or even revenge.

Mitigation Techniques

Insider Threats have many different types of mitigation techniques such as

- Sabotage - when a ex employee has a motive to vandalized equipment or compromising confidential information.
- Fraud - when a malicious insider may use company credit card for personal use.
- Espionage - When a ex employee steals trade secrets, confidential information or intellectual property belonging to an organization.