AIG
Agile Intel Group

INSIDER THREAT:
Combating The Enemy Within

Combating Insider Threats Within Organizations

Insider threats presents a considerable risk to the security and integrity of an organization's data and assets.

What is an Insider Threat?

An insider threat is a security risk from people within an organization who misuse their authorized access for malicious reasons. This includes current or former employees, contractors, or partners with knowledge of sensitive operations or data.

Types of insider threats can include:

- Malicious Insiders:
  Individuals who intentionally misuse their access to steal data, sabotage systems, or carry out other harmful activities for personal gain or to harm the organization.

- Careless Insiders:
  Employees who inadvertently compromise security through negligent actions, such as clicking on malicious links, using weak passwords, or mishandling sensitive data.

- Compromised Insiders:
  Individuals whose credentials or access has been compromised by external threats, such as phishing attacks or social engineering, leading to unauthorized access and potential data breaches.

Combatting insider threats requires organizations to implement robust security measures, such as access controls, user monitoring, employee training, and incident response plans. By being vigilant and proactive in addressing insider threats, organizations can better protect their data and assets from internal risks.

The insider threat is significant for several reasons:

1. Access to Sensitive Information:
   Insiders, by virtue of their roles within the organization, often have access to sensitive information, trade secrets, and critical systems. This makes them capable of causing significant damage if they choose to misuse their access.

2. Intimate Knowledge of Systems and Processes:
   Insiders possess intimate knowledge of the organization's systems, processes, and security measures, making it easier for them to circumvent security controls and carry out malicious activities without raising suspicion.

3. Potential for Substantial Damage:
   The actions of an insider can result in severe financial, reputational, and operational damage to the organization. This can include data breaches, theft of intellectual property, sabotage of systems, or disruption of critical operations.

4. Challenges in Detection and Attribution:
   Insider threats can be more challenging to detect than external threats, as the malicious activities may not trigger typical security alerts. Additionally, attributing the source of the threat within the organization can be complex and time-consuming.

5. Impact on Trust and Culture:
   Insider threats can erode trust within the organization and negatively impact its culture. The discovery of an insider threat incident can lead

to decreased employee morale, damaged relationships, and a loss of confidence from customers, partners, and stakeholders.

Given these factors, organizations need to prioritize the identification, mitigation, and prevention of insider threats to protect their assets, maintain trust, and safeguard their operations.

This often involves a combination of technical controls, employee training, incident response planning, and ongoing monitoring to address the specific risks posed by insiders.

How can you Recognize an Insider Threat?

Recognizing an insider threat requires a combination of vigilant monitoring, employee training, and the use of security tools to detect unusual or suspicious behavior. Here are some indicators that may help in recognizing an insider threat:

- Abnormal Access Patterns:
  Watch for employees accessing systems or data outside of their normal duties or beyond their regular working hours, especially if it involves sensitive or confidential information.

- Unauthorized Data Handling:
  Look for signs of employees copying, downloading, or transmitting large amounts of data that are not relevant to their roles, particularly if the data is sensitive or proprietary.

- Repeated Access Attempts:
  Monitor for repeated failed login attempts, especially if they are concentrated on specific systems or sensitive areas of the network, which could indicate unauthorized access attempts.

- Changes in Behavior:
  Identify significant changes in an employee's behavior, such as sudden disgruntlement, financial struggles, or becoming unusually secretive, as these may be signs of potential malicious intent.

- External Connections:
  Keep an eye on employees who are communicating with external entities in ways that are unusual for their roles, as this could indicate unauthorized information sharing or collusion.

- Security Policy Violations:
  Regularly review security policy violations, including unauthorized software installations, attempts to disable security measures, or attempts to bypass access controls.

- Anomalous Network Activity:
  Use network monitoring tools to identify anomalous network traffic, unauthorized data exfiltration, or communication with known malicious entities.

It's important to note that while these indicators may be suggestive of insider threats, they are not definite proof of malicious intent. Therefore, it's essential to approach the detection of insider threats with a balance of vigilance and fairness, ensuring that employees' privacy and rights are respected while safeguarding the organization from potential risks.

Inappropriate Information That May Be Transmittal By Insiders

Inappropriate information transmittal by insiders can pose a significant risk to an organization's data security. Some examples of this behavior include:

- Unauthorized Disclosure of Sensitive Information:
  Employees sharing confidential or proprietary information with unauthorized individuals or external parties without proper authorization.

- Sending Confidential Data via Personal Email:
  Transmitting sensitive data through personal email accounts or unsecured messaging platforms, which can increase the risk of data breaches.

- Use of Unauthorized File-sharing Services:
  Uploading confidential documents or files to unauthorized cloud storage or file-sharing services that may not have adequate security measures in place.

- Data Leakage through Printouts:
  Printing out sensitive information and not properly securing or disposing of the hard copies, potentially leading to data leakage or unauthorized access.

- Data Transfer to External Devices:
  Copying sensitive data to USB drives, external hard drives, or other removable media devices without proper encryption or authorization, increasing the risk of data loss or theft.

- Unapproved Data Backup:
  Creating unauthorized backups of data on personal devices or cloud services without following organizational backup procedures, potentially exposing sensitive information to risks.

- Unauthorized Data Sharing on Collaboration Platforms:
  Sharing confidential data on internal collaboration platforms or messaging apps with unauthorized individuals or groups, compromising data confidentiality.

Organizational Strategies

To prevent inappropriate information transmittal by insiders, organizations should implement measures such as:

1. Data Loss Prevention (DLP) Tools:
   Deploying DLP solutions to monitor, detect, and prevent unauthorized data transfers or sharing of sensitive information.

2. Access Controls and Monitoring:
   Implementing strict access controls, user permissions, and monitoring to track and audit user activities related to data handling.

3. Employee Training and Awareness:
   Providing regular training on data security best practices, policy compliance, and the risks associated with inappropriate information transmittal.

4. Strict Data Handling Policies:
   Establishing clear policies and procedures regarding data handling, sharing, and transmission, and ensuring employees adhere to these guidelines.

5. Encryption and Endpoint Security:
   Enforcing encryption mechanisms for data in transit and at rest, as well as implementing endpoint security measures to safeguard against data leakage.

Observation and Conclusion:

By addressing these risks proactively and promoting a culture of data security and compliance within the organization, businesses can mitigate the threats associated with inappropriate information transmittal by insiders.

The goal is to identify the threat and, equally important, identify the Insider. Both as early as possible.

End