LIS SOLUTIONS MONTHLY NEWSLETTER SEPTEMBER 2022

WHAT IS AN INSIDER THREAT?

An Insider Threat is defined by a person utilizing their authorized access or understanding of an organization to do harm to that organization or to their nation. The harm that is caused can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities. An insider can be a person that the organization trusts, including employees, organization members, and those to whom the organization has given sensitive information and access. Also, an insider can be a person who has knowledgeable about the organization's business strategy and goals, entrusted with future plans, or the means to sustain the organization and provide for the welfare of its people.

INSIDER THREAT INDICATORS: WHY DO PEOPLE BECOME INSIDER THREATS?

While some people join organizations or government entities with the intent to gain access to information and do harm, employees or partners can change their allegiance over the course of time and become an Insider Threat.

Some indicators to identify when people become an Insider Threat are:

- **Behavioral Indicators:**
  - A dissatisfied or disgruntled employee, contractor, vendor, or partner.
  - Attempts to circumvent security.
  - Regularly working off-hours.
  - Displays resentment toward co-workers.
- **Digital Indicators:**
  - Signing into enterprise applications and networks at unusual times. For instance, an employee who, without prompting, signs into the network at 3am may be cause for concern.
  - Surge in volume of network traffic. If someone is trying to copy large quantities of data across the network, there will be unusual spikes in network traffic.
  - Accessing resources that they usually don't or that they are not permitted to.
  - Accessing data that is not relevant for their job function.

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com

THE MOTIVES OF AN INSIDER THREAT:

As a trusted employee, you are the first line of defense when it comes to detecting an Insider Threat. The better you understand the people you work with such as: their motivations, or their relationship with your data and networks, the earlier you can detect and contain potential threats. It is important to know that Insider Threats can be created by an absent-minded employee failing to follow basic security protocols or by a malicious insider:

- **Financial Gain:** This is the most common driver for the malicious insider. Employees across all levels are aware that corporate data and sensitive information has value.
- Negligence: Negligence is the most common cause of insider threats, costing organizations an average of $4.58 million per year.
- **Distraction:** Where negligent employees may raise red flags by regularly ignoring security best practices, the distracted insider may be a model employee until the moment they make a mistake.
- **Organizational Damage:** Some malicious insiders have no interest in personal gain. Their sole driver is harming the organization.
- **Espionage and Sabotage:** Malicious insiders do not always work alone. In some cases, they may be passing information to a third-party such as a competitor or a nation-state.

Report all Insider Threat Indicators to your Insider Threat Working Group at LIS Solutions: **security@lissol.com** or **hr@lissol.com**

INSIDER THREAT AWARENESS COURSE CDSE:

This course provides a thorough understanding of how Insider Threat Awareness is an essential component of a comprehensive security program. With a theme of, "If you see something, say something" the course promotes the reporting of suspicious activities observed within the place of duty. Using a few case study scenarios, the course teaches the common indicators which highlight actions and behaviors that can signify an insider threat. The instruction promotes a proactive approach to reporting the suspicious activities. Course: **https://securityawareness.usalearning.gov/itawareness/index.htm**

Please take the time, if you have not already, to review and complete the Insider Threat Awareness Course. Once completed, please provide LIS Security your certificate of completion to **security@lissol.com**

MUST READ ARTICLE

Your biggest cybersecurity threats are inside your enterprise

By: Taryn Plumb • July 6, 2022

"Much is made of the multitude of outside security risks and vulnerabilities faced by enterprises, and rightly so."

"That said, though, many organizations may be overlooking their potentially most harmful threat: their employees and other trusted insiders."

Read the Full Article Here:
https://venturebeat.com/2022/07/06/the-weight-of-insider-threats-in-enterprise-cybersecurity/

REFERENCES:

- https://www.cisa.gov/defining-insider-threats
- https://securityawareness.usalearning.gov/itawareness/index.htm
- https://www.microfocus.com/en-us/what-is/insider-threat
- https://www.helpnetsecurity.com/2020/09/08/mapping-the-motives-of-insider-threats/
- https://venturebeat.com/2022/07/06/the-weight-of-insider-threats-in-enterprise-cybersecurity/