5 Quick wins to manage insider threats.

Five Quick Wins to reduce risks of insider threats

Pr. Nsiangani, Expert Information Security & Cyber Defense

Introduction

Insider threats pose a significant risk to companies of all sizes and in all industries. These threats can come from a range of sources, including employees, contractors, and business partners, and can take many different forms. Insider threats can be particularly challenging for companies in complex setups, such as those with multiple subsidiaries or divisions, as these organizations may have more complex networks, systems, and processes that can be vulnerable to attacks.

In this white paper, we will explore the risks and challenges associated with insider threats for companies in complex setups, and provide a human-centered approach to tackle these threats in five quick wins. We will begin by defining insider threats and exploring the risks and challenges that they pose to companies in complex setups. We will then examine three scenarios for insider threats, including their vulnerability, attack vector, risk, severity, and likelihood. We will also provide statistics on insider threats from renowned sources, to help illustrate the scale and impact of these threats.

Next, we will provide five quick wins that companies in complex setups can use to tackle insider threats. These quick wins will focus on a human-centered approach, as we believe that the best way to address insider threats is to focus on the people who are involved in them. We will explore the importance of awareness and education, as well as the role that strong policies and procedures, technical controls, and incident response plans can play in reducing the risk of insider threats.

Finally, we will provide a compelling conclusion that summarizes the key takeaways from this white paper and highlights the importance of addressing insider threats for companies in complex setups. By following the recommendations outlined in this paper, companies can take steps to reduce the risk of insider threats and protect themselves from the potential financial and reputational damage that these threats can cause.

Overall, this white paper provides a comprehensive overview of the risks and challenges associated with insider threats for companies in complex setups, and offers a human-centered approach to tackle these threats in five quick wins. By following the recommendations outlined in this paper, companies can take steps to reduce the risk of insider threats and protect themselves from the potential financial and reputational damage that these threats can cause.

The Problem and Risks:

Insider threats pose a significant risk to companies in complex setups, as these organizations may have more complex networks, systems, and processes that can be vulnerable to attacks. Insider threats can come from a range of sources, including employees, contractors, and business partners, and can take many different forms. To effectively address these threats, it is important for companies to understand the problems and risks that they pose, as well as their root causes.

One of the main problems associated with insider threats is the potential for unauthorized access to or misuse of sensitive information. This can occur if an insider has access to information that they should not have, or if they use that information for inappropriate purposes. For example, an insider may access confidential financial data and use it to make inappropriate trades, or may share customer data with unauthorized parties. This type of activity can lead to significant financial and reputational damage for the company, as well as potential legal and regulatory consequences.

Another problem associated with insider threats is the potential for disruptions to critical business processes. This can occur if an insider deliberately or unintentionally causes disruptions to systems or processes, such as by introducing malware or making unauthorized changes to data. This can lead to significant operational disruptions, which can have significant financial and reputational consequences for the company.

The root causes of insider threats can vary widely, but often include a lack of awareness or understanding of the risks and consequences of these threats, as well as a lack of effective policies and procedures to prevent and address them. In some cases, insider threats may be motivated by personal gain or revenge, while in other cases they may be the result of negligence or carelessness.

To better understand the risks and challenges associated with insider threats, it can be helpful to consider specific scenarios. Below, we will outline three scenarios for insider threats, including their vulnerability, attack vector, risk, severity, and likelihood:

Scenario 1: An employee with privileged access to sensitive information intentionally or unintentionally misuses this information for personal gain.

Vulnerability: The employee has access to sensitive information that they should not have.

Attack vector: The employee intentionally or unintentionally misuses this information.

Risk: High, as the employee has access to sensitive information and may use it for inappropriate purposes.

Severity: High, as the misuse of sensitive information can lead to significant financial and reputational damage for the company.

Likelihood: Moderate to high, depending on the employee's access to sensitive information and their motivation to misuse it.

Scenario 2: A contractor with temporary access to systems and data introduces malware or makes unauthorized changes to data.

Vulnerability: The contractor has temporary access to systems and data.

Attack vector: The contractor introduces malware or makes unauthorized changes to data.

Risk: High, as the contractor has access to systems and data and may use this access to cause disruptions.

Severity: High, as disruptions to systems and data can lead to significant operational disruptions and financial and reputational damage.

Likelihood: Moderate to high, depending on the contractor's access to systems and data and their motivation to cause disruptions.

Scenario 3: An employee with a grudge against the company intentionally causes disruptions to systems or processes.

Vulnerability: The employee has access to systems and processes that they may be able to disrupt.

Attack vector: The employee intentionally causes disruptions to systems or processes.

Risk: High, as the employee has access to systems and processes and may use this access

The Solution

To effectively address insider threats, it is important for companies in complex setups to adopt a proactive and comprehensive approach. One way to structure this approach is to focus on five quick wins that can help to reduce the risk of these threats and protect against the potential consequences. These quick wins are:

Awareness and education: One of the most effective ways to reduce the risk of insider threats is to raise awareness of the risks and consequences of these threats among employees, contractors, and business partners. This can be achieved through regular training and communication programs, as well as through the use of tools such as newsletters or posters to promote awareness. By raising awareness of the risks and consequences of insider threats, companies can encourage employees and other stakeholders to be more vigilant and to report any suspicious activity.

Strong policies and procedures: Another key step in reducing the risk of insider threats is to develop and implement strong policies and procedures that outline the expectations and responsibilities of employees, contractors, and business partners. These policies and procedures should cover a wide range of topics, including data security, information access, and incident reporting, and should be regularly reviewed and updated to ensure that they remain effective and relevant. By establishing clear policies and procedures, companies can provide guidance to employees and other stakeholders and help to prevent insider threats from occurring.

Technical controls: In addition to strong policies and procedures, it is also important for companies to implement technical controls to protect against insider threats. This may include measures such as data encryption, access controls, and incident response plans. By implementing these technical controls, companies can reduce the risk of unauthorized access to or misuse of sensitive information and mitigate the potential consequences of insider threats.

Incident response plans: To effectively address insider threats when they do occur, it is important for companies to have a clear incident response plan in place. This plan should outline the steps that the company will take to investigate and respond to an insider threat, and should include procedures for communicating with regulatory authorities and other stakeholders. By having a clear incident response plan in place, companies can minimize the potential impacts of insider threats and protect themselves against financial and reputational damage.

Regular review and assessment: To ensure that the company is effectively addressing insider threats, it is important to regularly review and assess the effectiveness of the measures that are in place. This may involve conducting audits or assessments of the company's policies and procedures, technical controls, and incident response plans, and making any necessary changes to address any identified weaknesses or gaps. By regularly reviewing and assessing the effectiveness of these measures, companies can ensure that they are well-equipped to handle insider threats and reduce the risk of financial and reputational damage.

Overall, these five quick wins can help companies in complex setups to effectively address insider threats and reduce the risk of financial and reputational damage. By raising awareness of the risks and consequences of insider threats, establishing strong policies and procedures, implementing technical controls, having a clear incident response plan in place, and regularly reviewing and assessing the effectiveness of these measures, companies can take a proactive and comprehensive approach to tackling insider threats and protecting themselves against the potential consequences of these threats

Conclusion:

In conclusion, insider threats pose a significant risk to companies in complex setups, and can have significant financial and reputational consequences. To effectively address these threats, it is important for companies to adopt a proactive and comprehensive approach that focuses on raising awareness, establishing strong policies and procedures, implementing technical controls, having a clear incident response plan in place, and regularly reviewing and assessing the effectiveness of these measures. By following these recommendations, companies can take steps to reduce the risk of insider threats and protect themselves against the potential consequences of these threats.

It is worth noting that insider threats are just one aspect of the overall risk landscape that companies face. Cyber threats from external sources are also a major concern, and according to some estimates, these types of threats are on the rise. For example, a recent study found that the number of detected cyber threats increased by 36% in 2020, with the healthcare, government, and education sectors being particularly vulnerable.

Despite the challenges posed by insider and external threats, there are simple initiatives that companies can take to significantly reduce their risk. For example, implementing a security newsletter or other regular communication program can help to raise awareness of the risks and consequences of cyber threats and encourage employees and other stakeholders to be more vigilant and report any suspicious activity. By taking these types of initiatives, companies can have a tremendous positive impact on their overall risk profile and reduce the potential for financial and reputational damage.

Overall, it is clear that insider threats pose a significant risk to companies in complex setups, and that a proactive and comprehensive approach is needed to effectively address these threats. By raising awareness, establishing strong policies and procedures, implementing technical controls, having a clear incident response plan in place, and regularly reviewing and assessing the effectiveness of these measures, companies can take steps to reduce the risk of insider threats and protect themselves against the potential consequences of these threats.