STM JOURNALS

International Journal of
Information Security Engineering

Volume 1, Issue 2, 2023
July—December
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

Designing a Novel Insider Threat Model for Enhanced Cybersecurity

Manas Kumar Yogi*

Abstract

Designing a novel insider threat model is a critical imperative in the realm of cybersecurity. As organizations face an ever-expanding threat landscape, insider threats, whether deliberate or inadvertent, present a formidable challenge to the safeguarding of sensitive data and critical assets. This abstract encapsulates the significance, challenges, and innovations inherent in crafting an effective insider threat model for enhanced cybersecurity. The necessity for novel insider threat models arises from the recognition that traditional security measures often overlook the dangers posed by trusted insiders. This paper explores the multifaceted domain of designing such models, emphasizing their proactive nature and adaptability to evolving security threats. The complexities of this endeavor are magnified by several challenges, ranging from acquiring high-quality data and maintaining compliance with privacy regulations to addressing false positives and combating evolving attack vectors. Additionally, the model's efficacy depends on a deep understanding of contextual information, user behavior profiling, and the ability to differentiate between normal and anomalous activities. It also requires striking a delicate balance between security and privacy, respecting ethical and legal standards while gaining the trust of employees and stakeholders. Innovations in insider threat modeling encompasses a comprehensive approach, integrating advanced machine learning algorithms, user and entity behavior analytics, and adaptive learning to create a dynamic defense against insider threats. This paper underscores the necessity of continuous improvement, collaboration between experts from diverse domains, and awareness of evolving threats and best practices.

Keywords: Insider threat, cybersecurity, privacy, malicious, threat model, safeguard

INTRODUCTION

Insider threats in cybersecurity pose significant and multifaceted adverse effects that can wreak havoc on organizations, ranging from financial losses to damage to reputation, intellectual property theft, and even compromising national security. These threats, which emanate from individuals within an organization, be they employees, contractors, or partners, are often insidious and challenging to detect. Understanding the extensive and detrimental impacts of insider threats is crucial for comprehending the urgency of robust preventive measures [1].

***Author for Correspondence**
Manas Kumar Yogi
E-mail: manas.yogi@gmail.com

Assistant Professor, Department of Computer Science & Engineering, Pragati Engineering College (A), Surampalem, Andhra Pradesh, India

Received Date: October 29, 2023
Accepted Date: November 27, 2023
Published Date: December 06, 2023

Citation: Manas Kumar Yogi. Designing a Novel Insider Threat Model for Enhanced Cybersecurity. International Journal of Information Security Engineering. 2023; 1(2): 24–27p.

One of the most immediate and tangible adverse effects of insider threats is the financial burden they impose on organizations. Malicious insiders, motivated by personal gain or vendettas, can execute fraudulent activities that lead to direct financial losses. These activities may include embezzlement, data theft, or the manipulation of financial records. In addition to these direct financial consequences, insider threats can result in substantial costs related to investigations, legal proceedings, and remediation efforts.

Furthermore, insider threats can inflict severe damage on an organization's reputation and trustworthiness. When data breaches or security incidents occur, public perception and stakeholder confidence in the organization can be eroded. This can lead to a loss of customers, partners, and investors, and it may take years to rebuild the trust that has been shattered. The reputational damage from insider threats can be far more costly and long-lasting than the immediate financial losses.

Intellectual property theft is another insidious consequence of insider threats. Innovations, trade secrets, and proprietary information are at risk when insiders with knowledge of these assets turn against their organization. This intellectual property can be sold to competitors or malicious actors, causing long-term damage to the organization's competitive advantage and profitability. In some cases, it may result in the loss of entire research and development projects, severely undermining an organization's position in the market.

Insider threats can also undermine the confidentiality and privacy of sensitive data, putting individuals and organizations at risk. For instance, healthcare organizations may face breaches of patient records, leading to identity theft and potential harm to patients. Likewise, financial institutions could suffer breaches of customer data, which may result in financial fraud and severe consequences for clients. The exposure of sensitive information can lead to regulatory fines, legal liabilities, and irreparable harm to those affected [2].

In a global context, insider threats can extend to national security concerns. Organizations that deal with classified or sensitive government information are at risk of insider threats jeopardizing critical national interests. Malicious insiders with access to defense or intelligence data can leak classified information, undermining security operations, diplomatic efforts, and international relations. The damage to national security from such insider breaches can be immeasurable.

Insider threats also disrupt day-to-day operations and productivity. When organizations must divert resources to investigate and mitigate insider threats, normal business activities can be significantly hampered. This can lead to missed opportunities, project delays, and a decreased ability to compete effectively in the market. Ultimately, the adverse effects of insider threats extend beyond the immediate financial and operational implications. They encompass a broad spectrum of challenges that affect an organization's long-term viability and sustainability. To mitigate these threats, organizations must adopt a multi-faceted approach that includes robust security measures, employee education, and vigilant monitoring. Combating insider threats is not only a matter of protecting an organization's assets but also safeguarding its integrity, reputation, and the trust of its stakeholders.

NOVEL DESIGN FRAMEWORK

Designing a novel insider threat model for enhanced cybersecurity is a complex and multifaceted task. Such a model should be comprehensive, adaptable, and proactive. Following is a high-level framework for designing such a model [3, 4]:

- *Define objectives and scope:* Clearly define the objectives of the insider threat model, including what types of insider threats you want to detect or prevent. Consider whether you are focused on malicious or unintentional insiders.
- *Data collection and analysis:* Gather relevant data sources, including logs, user activity data, and network traffic. This data will serve as the foundation for your model.
- *Feature engineering:* Extract and engineer meaningful features from the collected data, such as user behavior, access patterns, and anomaly detection features. Feature engineering is critical for model accuracy.
- *Behavior profiling:* Develop a baseline of normal behavior for each user or system. This involves using machine learning techniques to profile and understand typical user actions and system behaviors.

- *Anomaly detection:* Utilize machine learning algorithms, such as clustering, classification, or deep learning, to detect anomalies in user behavior or system activities. Anomalies may indicate insider threats.
- *User and entity behavior analytics (UEBA):* Implement UEBA to continuously monitor user and entity behaviors. UEBA solutions can provide real-time insights into unusual activities that may signify insider threats.
- *Risk scoring:* Assign risk scores to users and entities based on the detected anomalies. A risk score can help prioritize and respond to potential threats.
- *Contextual information:* Integrate contextual information, such as data access patterns, job roles, and external factors, to provide a more accurate understanding of whether an anomaly is truly a threat.
- *Adaptive learning:* Implement machine learning models that can adapt over time as user behavior changes. This ensures that the model remains effective in detecting evolving insider threats.
- *Response mechanisms:* Define response mechanisms for different levels of insider threats, including notification, user education, access restriction, and escalation to incident response teams.

CHALLENGES IN DESIGNING NOVEL INSIDER THREAT MODELS

Designing novel insider threat models for enhanced cybersecurity is a complex and challenging task due to various factors. The key challenges faced are mentioned in the following section:

- *Data availability and quality:* Insider threat models heavily rely on data, and obtaining high-quality, relevant data can be challenging. Many organizations may not have sufficient historical data or may face issues with data silos and data integrity.
- *Data privacy and compliance:* Balancing the need for comprehensive data with privacy regulations and ethical concerns is a significant challenge. Privacy laws like General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) can limit the types of data you can collect and analyze [5].
- *Behavioral changes:* Insiders can change their behavior to avoid detection. Adapting your model to detect evolving insider threats is a constant challenge.
- *Contextual understanding:* Understanding the context of user actions, such as job roles and access privileges, is crucial. However, building an accurate contextual understanding can be complex and dynamic.
- *Insider collaboration:* Insider threats can involve collusion among multiple insiders, making it harder to detect suspicious behavior [6]. Models need to account for group dynamics.
- *Zero-day attacks:* Traditional insider threat models may not be able to detect zero-day attacks or previously unseen attack vectors, which require continuous adaptation and innovation [7].
- *Legal and ethical considerations:* Adhering to legal and ethical standards while monitoring and investigating employee activities poses challenges, particularly regarding privacy and consent.
- *User acceptance and privacy concerns:* Employees may be concerned about their privacy and may resist being monitored. Balancing security needs with user acceptance is an ongoing challenge [8].
- *Interdisciplinary expertise:* Designing insider threat models requires expertise in cybersecurity, data science, psychology, and legal matters. Collaboration among experts from these diverse fields is necessary.
- *Resource constraints:* Smaller organizations may lack the resources, both in terms of technology and personnel, to implement advanced insider threat models effectively.
- *Monitoring remote and hybrid workforces:* The shift to remote and hybrid work environments has made insider threat detection more challenging, as user behavior and network access patterns have changed [9].
- *Model interpretability:* The ability to explain why a model flagged a particular behavior is important for user trust and for investigating incidents. Achieving interpretability in complex models is a challenge.

- *Adversarial attacks:* Insiders may actively try to subvert or trick insider threat models. Defending against adversarial attacks is a growing challenge.

To address these challenges, it is important to regularly assess and adapt your insider threat model, collaborate with experts, and stay informed about evolving threats and best practices in the field of cybersecurity [10]. Additionally, a strong focus on privacy and ethical considerations is crucial to maintaining trust within the organization.

CONCLUSION

The design of novel insider threat models for enhanced cybersecurity is a critical endeavor in our ever-evolving digital landscape. As organizations increasingly recognize that insider threats pose a significant risk, the development of effective models to detect and mitigate such threats becomes imperative. This holistic approach requires a multidisciplinary effort that combines cybersecurity expertise, data analytics, and a profound understanding of human behavior and motivations. The challenges in creating these models are substantial, from acquiring high-quality data and navigating privacy regulations to combating false positives and adapting to rapidly changing attack vectors. Yet, the potential benefits are equally significant. Insider threat models, when well-constructed, have the power to safeguard an organization's sensitive data, intellectual property, and reputation, ultimately bolstering its resilience in the face of both intentional and inadvertent insider threats. Success hinges on the ongoing enhancement and flexibility of these models. They must keep pace with emerging technologies, evolving workforce dynamics, and shifting threat landscapes. Furthermore, striking a balance between security and user privacy is paramount, as well as maintaining transparency and compliance with legal and ethical standards. As insider threats continue to challenge the cybersecurity paradigm, organizations committed to designing novel insider threat models will be better equipped to detect, respond to, and ultimately prevent security breaches from within. By fostering a culture of cybersecurity awareness, implementing state-of-the-art technologies, and learning from past incidents, we can collectively fortify our defenses against insider threats and bolster the security of our digital ecosystems.

REFERENCES

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. New York, NY, USA: John Wiley & Sons; 2020.
2. Swinhoe D. What is an insider threat? 7 warning signs to watch for. CSO Online. December 3, 2018. Available at https://www.csoonline.com/article/566603/what-is-an-insider-threat-7-warning-signs-to-watch-for.html
3. Chan TK, Chin CS, Chen H, Zhong X. A comprehensive review of driver behavior analysis utilizing smartphones. IEEE Trans Intell Transport Syst. 2019; 21 (10): 4444–4475.
4. Keeney M, Kowalski E, Cappelli D, Moore A, Shimeall T, Rogers S. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Washington, DC, USA: United States Secret Service; 2005.
5. Nicolaou A, Shiaeles S, Savage N. Mitigating insider threats using bio-inspired models. Appl Sci. 2020; 10 (15): 5046.
6. Shafiullah M, Refat AM, Haque ME, Chowdhury DM, Hossain MS, Alharbi AG, Alam MS, Ali A, Hossain S. Review of recent developments in microgrid energy management strategies. Sustainability. 2022; 14 (22): 14794.
7. Spitzner L. Honeypots: Tracking Hackers. Reading, MA, USA: Addison-Wesley; 2003.
8. Al-Mhiqani MN, Ahmad R, Abidin ZZ, Abdulkareem KH, Mohammed MA, Gupta D, Shankar K. A new intelligent multilayer framework for insider threat detection. Computers Electric Eng. 2022; 97: 107597.
9. Force JT. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD, USA: National Institute of Standards and Technology; 2017.
10. Verkijika SF, De Wet L. E-government adoption in sub-Saharan Africa. Electron Commerce Res Appl. 2018; 30: 83–93.

