Insider Threat Detection and Prevention Chameleon Report

Chameleon Security Team

Author(s):

Name:	Student ID	Team:
Rewniz Patell	221267802	Chameleon Security

Table of Contents

Summary 3
Introduction 4
Prevalence of Insider Threats 5
Company-Wide Strategy for Chameleon 7
Detection Measures 7
Prevention Measures 8
Conclusion 9
References (IEEE) 10

Summary

This report was written and researched by Rewniz Patell from the Chameleon Security Team. This report involves understanding insider threats, the types of insider threats, the prevalence of these threats, and how Chameleon can develop processes to detect these threats and prevent them from becoming damaging to the organization. This report is aimed at any individual within Chameleon, and is written with to ensure that individuals with a limited knowledge of IT/Cyber security concepts can still understand the report and the measures that can be enacted. The measures recommended within this report should be enacted across the whole of Chameleon, not just one department or team.

Introduction

Insider threats are cyber security threats that originate from authorized users who intentionally misuse their access and authority to damage the infrastructure, or resources, equipment, or objectives within an organization. An insider could be an employee, contractor, volunteer, business partner, or any individual within an organization, that aims to use their access and authority to harm the organization. These threats include disclosing confidential information, deleting company data, sabotaging company infrastructure or security, or enabling malicious attackers through creating opportunities for cyber-attacks, or giving authorization to attackers [1].

As insiders are within the organization, they would have a high level of trust, access and authority within the organization. This is especially the case for senior or upper-level management or individuals with a high level of authority. As a result, detection and prevention measures need to be implemented, to avoid scenarios where an individual within a company intentionally or unintentionally misuses their assigned access to various organization systems [2].

There are many different types of insider threats. The most common is an unintentional threat, that stems from negligence or accidents. Unintentional threats could be caused through accidents, where an insider makes a mistake which causes risk to the organization. This could be a mistake such as engaging with a phishing email, downloading a software that is malicious, or accidentally sending confidential information to a wrong address. Additionally, unintentional threats could occur due to negligence. This is when an insider does not take proper measures, which then leads to threats to the organization. Examples of this include ignoring security policies, ignoring the work devices policy, and logging in to organization infrastructure with a compromised personal device, or not taking proper security measures for account security, leading to attackers gaining account access.

There are also intentional insider threats. This is when the insider intentionally attempts to compromise the security or information of an organization. Reasons for this may include disgruntlement with management or working conditions, falling out with work relationships, being made redundant but still having access to organization infrastructure, or collusion with other malicious parties. These threats can lead to leaking of sensitive information, stealing proprietary data, or creating openings for malicious attackers to exploit. Insider threats could also be outside of the realm of cyber security, with potential insider threats being workplace/organizational violence, espionage, governmental sabotage, or financial theft [3].

Prevalence of Insider Threats

The prevalence of insider threats could vary between organizations. Companies with numerous employees are more prevalent to insider threats as they naturally have more individuals with access and control to company infrastructure. Additionally, if a company gives more than required access to infrastructure, systems, and accounts to employees, then insider threats are more likely. As a result, any organization needs to be aware of insider threats, and how both unintentional insider threats, and intentionally malicious insider threats could cause major damage to any organization.

The Insider Threat Report 2023 by Cybersecurity Insiders showcases that 74% of organizations are at least moderately vulnerable to insider threats, with the three most common insider threat actors being regular employees, third parties, and the privileged users (administrators, and other individuals with high level access) [4].

Furthermore, the motivations of insider threats have become more monetary in recent years, with a 2023 survey of IT professionals reporting that financial motivations are the most concerning threat. These financial motivations include selling company information, and insider trading, with 50% of IT professionals claiming that this was the most concerning motivator. The second most concerning motivator was personal benefit such as personal favors, gaining more job influence, and job advancement being a concerning motivator for insider threats, with 47% of IT professionals being concerned with this motivator. The third most concerning was the motivator of revenge with 45%. Factors for these motivators include targeting the organization for perceived wrongs, such as lay-offs, insider threats feeling that they are not valued, or overall work disgruntlement causing the insider threats.

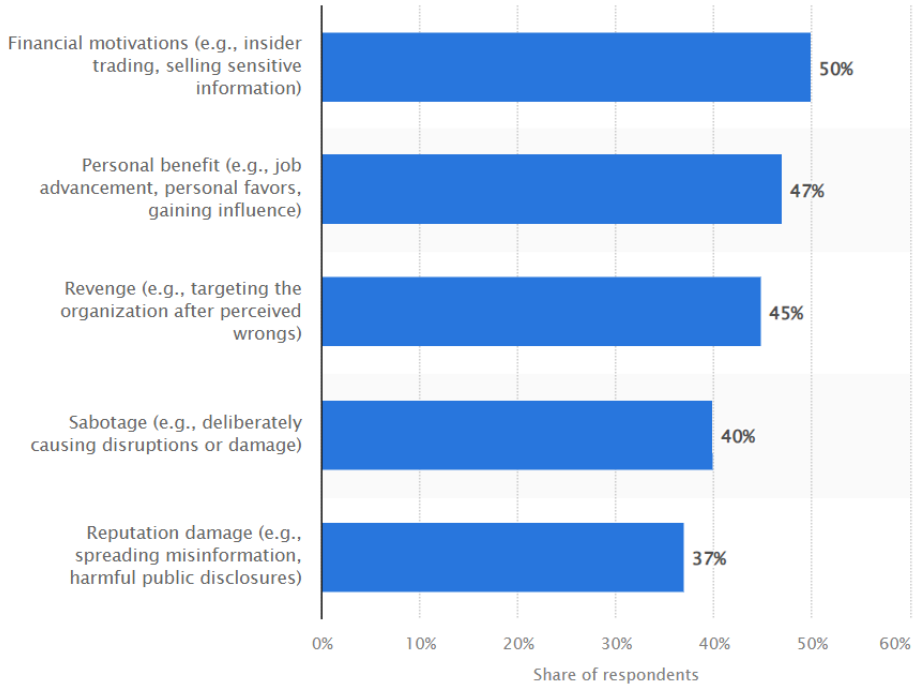

Figure 1: Most concerning insider threat motivations worldwide 2023 [5].

Additionally, the 2023 Cost of Insider Risk Global Report showcases that 21 of 40 surveyed organizations faced insider threat incidents within the years of 2022-2023. There was an 18% increase in insider threats between 2018 and 2023, with 2018 having 53% of companies reporting that they had an insider threat incident, compared to the 71% in 2023 [2]. This showcases a rise in insider threats and its prevalence, and therefore organizations are required to make effective to insider threat detection and prevention systems in order to combat the increased prevalence of insider threats.

Knowing these motivators for malicious insider threats allows organizations to become better equipped to deal with these threats. Financial motivations highlights why insiders have incentive to enable malicious threats, as insiders may be highly motivated to cause harm to an organization for financial benefits.

Company-Wide Strategy for Chameleon

Detection Measures

Detection measures involve having processes in place to detect whenever an insider threat is present within an organization. As Chameleon potentially grows in size during the future, it is important to implement detection strategies for insider threats as the employee count increases. These detection strategies would attempt to detect both malicious and unintentional insider threats, and what the processes enacted to investigate whether an insider threat is intentional or unintentional.

Detecting and identifying insider threats requires both technical and human elements. Attempts should be made by Chameleon to understand insider threats. These includes personal factors such as

- Certain individuals are more likely to pose threats than others within the organization. This is not necessarily negative, for example, new employees may be more susceptible to becoming an unintentional insider threat, as they are not fully trained, aware, or able to perform all the required security access, or have been fully trained about Chameleon policies and awareness programs. As a result, these employees pose more of a risk of being an insider threat and should be monitored whilst in the training process.
- Intentional insider threats occur in a social and workplace culture context. Certain environments, and disgruntlement within departments/teams are more likely to facilitate insider threat behavior.
- The process of a potential intentional insider threat is a process, not an event. Individuals who commit intentional insider threats usually take time before they attempt the threat. This involves a process of them turning malicious, finding resources to perform the insider threat, and then actually performing the threat, which leads to the insider threat event.
- 31% of incidents had others within the organization who had information on the insiders' plans and intentions. Measures should be in place within Chameleon to anonymously report about insider threats.
- 58% of perpetrators communicated their negative feelings, grievances, and or interest in causing harm to the organization. 92% of these were verbally, and 12% had email receipts.

[6]. Understanding the human aspect of insider threats would help to deal with the underlying issues before an intentional or unintentional insider threat event occurs. Furthermore, technological detection measures should be implemented to detect anomalies or insider threat behaviors before they become a larger issue. These include

- Monitoring user activity with tools to track and log user activities, including functions that require high level of administrative privileges, such as accessing confidential files, data transfers, logins from devices, etc.

- Implement data loss prevention (DLP) processes within Chameleon to avoid scenarios of data loss, even if individuals within the organization attempt to delete the data. This could help to limit the damage caused by malicious insiders who aim to erase Chameleon information.
- Utilize anomaly detection systems within Chameleon to detect anomalies, and have processes in place for an individual to investigate the anomaly to find whether an insider threat is present, and if it is intentional.
- Network traffic analysis tools to monitor and analyze for unauthorized logins, communications and data transfers.

A mix of these technological techniques and understanding of the personal factors would help to ensure that Chameleon has measures in place to detect insider threats before they happen or during the process of them happening. This would help to mitigate the chances of large-scale incidents occurring, or intervening before they cause widespread damage to Chameleon.

Prevention Measures

Preventing insider threats would require an approach of mixed technological and personal measures and increasing organizational awareness within Chameleon. Prevention measures include

- Access management: Managing the privileges and access of information for each employee. Employees should only have access to information that they are required to know. This helps to ensure that if a user account is compromised or if a malicious insider threat occurs, the amount of data and information available is limited.
- Employee background checks: Conduct thorough background checks on employees to understand if the employee could potentially become an insider threat.
- Security awareness training: Training employees within Chameleon ensures that each member is aware of security policies, measures, and safe practices. This helps to reduce the chances of unintentional insider threats.
- Incidence response plan: Develop a plan of action if an incident occurs, how to mitigate the damage caused by the incident to Chameleon infrastructure, and how to prevent the incident in the future.
- Access control policies: Creating a access control system that ensures employees only have access to necessary information is vital to ensure that individuals are not given too much access. This limits the ability of an insider to become an unintentional or intentional insider threat to Chameleon.

Conclusion

Insider threats have become more prevalent in recent years. As a result, Chameleon needs to take adequate measures to detect intentional and unintentional insider threats, and then attempt to prevent these threats. Additionally, mechanisms need to be implemented to limit the amount of damage a single incident can create, to avoid widespread or heavy damage to Chameleon infrastructure, security, and services.

References (IEEE)

[1] Cybersecurity & Infrastructure Security Agency (Unknown date) 'Defining Insider Threats' [Website]. Available: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

[2] IBM (Unknown date) 'What are insider threats?' [Website]. Available: https://www.ibm.com/topics/insider-threats#:~:text=IBM-,What%20are%20insider%20threats%3F,their%20accounts%20hijacked%20by%20cybercriminals.

[3] Teramind (Apr 2024) 'Types of Insider Threats Risking Your Company's Security' [Website]. Available: https://www.teramind.co/blog/types-of-insider-threats/

[4] Y. Storchak (Feb 2024) Ekran 'Insider Threat Statistics for 2024: Reports, Facts, Actors, and Costs' [Website]. Available: https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures#:~:text=Any%20company%20can%20have%20a,were%20caused%20by%20user%20negligence.

[5] A. Borgeaud (Apr 2024) Statista 'Most concerning insider threat motivations worldwide 2023' [Website]. Available: https://www.statista.com/statistics/1463588/top-concerning-insider-threat-motivations-worldwide/

[6] Cybersecurity & Infrastructure Security Agency (Nov 2020) 'Insider Threat Mitigation Guide' [Report]. Available: https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf