What is Insider Threat, ways to improve Data Loss Prevention Technique.

Ajinkya Mukherjee
New York Institute of Technology
College of Engineering and Computer Science

Table of Contents Page Number

I. Introduction

An insider Threat can be categorized as an attack carried out by any individual within the organization with an intent to hurt the organization or by accident, causing harm to the organization using vulnerabilities in its own resources(Sensitive Data, Network Vulnerabilities, Operating System Vulnerabilities)[1]. In simple words, the attacker could be either an authorized member of the organization or a random individual or a group that uses an individual to access the organization's resources to harm the organization. This could mean that the attackers could gain instant access to the internal network rather than have to attack the external network and alert the authorities. It could be as simple as a worker unintentionally opening an unsafe email or intentionally putting a virus in the organization's server crashing the firewall and Intrusion systems. Section 2.1 talks about such bad actors in detail.

Insider Threat has always been an issue for organizations and for National Security, which is why the United States Government had to create a National Insider Threat Taskforce[2] in October 2011.

Insider Threat is a simple yet effective attack as it uses human vulnerabilities to attack the organizations network and data instead of technological ones, making it extraordinarily unpredictable and efficacious. Over the past years, the number of Insider Threats has increased by a considerable number; the United States and its organizations alone are victims to 2500 breaches every day, which is a 66% surge in the attack rate in the past two years[17]. Two out of these three attacks are caused due to simple negligence[3][17]. The danger not only lies in the unpredictability of the attack but also the detection rate of the attack as the external network protection system is never triggered, making it difficult for an organization to detect the attack before months have passed[16] and take steps to reverse it, causing financial damage and spoiling the company's image in the market.

II. Actors, Intents, and Challenges

2.1 *Bad Actors leading to Insider Threat*

When dealing with an attack like Insider Threat it is crucial to know what kind of attackers orchestrate such an attack

1. Mischievous Insider Threats (MIT)[3]: MIT's are attackers that are part of the same organization and are well aware of the internal network, prevention systems and sensitive data, and are motivated by different factors, including but not limited to Money, revenge, and so on. For example, A disgruntled employee or an Employee going through severe financial loss.
2. Accidental Insider Threat(AIT)[3]: As the name suggests, AIT's are attackers that are part of the same organization but have no intention of harming the organization and have accidentally leaked information, misplaced information, opened a malicious code, turned off the firewall, cause a firewall anomaly, which allows the intruders to attack the organization easily.
3. Outsider Insider Threat(OIT)[3]: OIT's are attackers that are not part of the same organization and convince an employee or an authorized member of the organization to grant them access to the resources or the internal network which they use to hurt the organization. Example: An Attacker can use Social Engineering to unknowingly get information from the employee, use a phishing scam or an attacker convincing an employee to open or upload his/her malicious code to the server corrupting the data or inserting a trojan or ransomware.

4. External Insider Threat(EIT)[3]: The attackers are individuals or groups that somehow have access to the company's inside confidential data or network policies. It could be due to a company using a third-party company[3] for one of its IoT services or a group using information available on the Internet about the company to hurt them. They could be responsible for manipulating the security policies and can p

2.2. *Intent behind Insider Threats?*

Every attacker has an intention to attack the organization, the intentions differ from individual to individual, some common intentions behind this attack are:

- Money[4]: It is the primary and most popular reason behind Insider Threat. Sometimes Employees or Members are in desperate need of money for personal reasons and are compelled to sell information to the attackers or attack their organization for money. Some of them are merely greedy and want more money.
- Revenge/Making a statement[4]: It is the next most popular reason behind Insider Threat. A disgruntled employee could simply want to take revenge from its organizations for not treating him/her fairly or for not giving him a raise or a promotion and could choose to hurt the organization.
- Competition[4]: In the modern-day world, there is fierce competition amongst organizations and businesses. A competitor could go to any extent to gain an advantage over its rival firm making competition a strong reason for insider threat.
- Carelessness[4]: It is a simple, unintentional, yet a popular reason behind this attack. An employee could be careless while opening a phishing email or while talking to people. They could easily fall for a Social Engineering attack, or a phishing scam.

2.3 *Challenges associated with Insider Threat*

It has become challenging over the years to detect and contain an Insider Threat attacks due to the given reasons.

- Legacy Technology and software: Many organizations rely on their legacy systems since they have been part of their organizations for a long time and comprise a large amount of data. Keeping that in mind getting rid of these systems is not possible both logically and financially while keeping it at the same time is another issue as the modern-day graduates are not very well versed with these systems[7].
- Numerous accounts within the corporate team: Since a large-scale organization have many employees in each team, and there are multiple teams within one branch of an organization, it is difficult for the organization to track the movement of every account or check the access granted and denied for each account[8]. It also makes the attack detection very slow.
- Increase in Number of IoT Devices: With the increase in the use of the Internet and IoT Devices in an organization, it is vital to take care of any kind of breaches. It is easy for any attacker mentioned in section 2.1 to carry out an attack and get away with it.
- Man-Based Attack: This attack is not very complicated and is carried out by a human with access to the data and information without the use of complex technology; hence even though the attacks can be prevented using policies and software, but it cannot be stopped entirely, and it takes months to detect them, making this attack a challenge.

III. Data Loss Prevention(DLP)

3.1 *Technological based techniques*

With the rise in Insider Threat attacks companies have taken drastic steps to reduce the number of attacks taking place by using the following techniques. (1)Data Loss Prevention or Network Data Loss Prevention also referred to as DLP, uses tools and software to ensure no data breaches or no data is compromised[5][6]. (2) Identity and Access Management or (IAAM) tools are used to ensure no member of the organization has access beyond what he/she is supposed to have. For example, in the Software Development department, an Intern cannot have the same access or privilege as his/her manager[9]. (3) User Activity Monitoring or UAM software, as the name suggests, is used to keep a check on what a particular Employee or Member are doing in a given network[10]. UAM software has been extremely popular in companies over the past decade and has helped organizations keep a check on their employee's digital activities while connected to the organization's network.

In this paper, the author focuses on Data Loss Prevention as a technique to contain Insider Threats.

3.2 *Data Loss Prevention(DLP) as a technique*

In this paper, we only talk about Enterprise level DLP's since we are talking about this technique in response to Insider Threats.

Data Loss Prevention(DLP) is a method used to help an organization keep its data safe and prevent it from being accessed by users who do not have access to it. DLP tools use specific parameters and security policies(network included) provided by the service provider and a few parameters and policies developed by the company to ensure its working[11]. Identifying the parameters and the security policies depends on the organization's needs, but the author has set his own parameters & policies for data loss prevention for this paper.

In this paper, to understand the working of a DLP tool, we assume a list of data of an Organization to be Name, Credit Card Info, Social Security Number, Health Records, Rival Companies, Research Information. Out of all this data, the organization is mainly concerned about the Private data which can only be accessed by certain employees in the organization such as Social Security Number, Health Records and Research Information, and these data fields are then marked as protected. Once the organization recognizes what data has to be protected, they make appropriate security policies and use the DLP tool to implement these policies[12] across the server, network or computer and can also set an alert priority depending on how important and sensitive the data is.

Every time someone tries to share the data the organization is notified and in some cases the data is immediately encrypted before being sent out hence the attacker only receives encrypted data and data is not compromised.

3.3 *Disadvantages and Concerns of using Data Loss Prevention(DLP)*

In the field of Cybersecurity, no technique or software is perfect and can help eradicate the problem completely. Even though Data Loss Prevention is an effective technique it has its own concerns such as:

- Expensive: Data Loss Prevention tools and software are expensive since the average cost of getting Data Loss Prevention Services is about $200,000 per annum. The cost only increases with the increase in number of employees for the organization.

- Specific Policies: A lot of Data Loss Prevention tools and software might not recognize or might be not compatible with a lot of policies, which in turn makes the use of the Data Loss Prevention tools meaningless.
- Constant Monitoring and Updates: Even though Data Loss Prevention tools help the organization in implementing the polices it is the job of the organization to keep updating these policies and monitoring the activities in the software.
- Human Based Attack: Insider Threat is not a technological based attack and it sometimes involves attacks by AIT's or OIT's who either make an accident and data is breached or are victims of social engineering attack and give away the information on their own. Data Loss Prevention tools cannot act upon such attackers as these accidents or attacks do not adhere to specific policies set by the organization.
- Known Policies: Most of the policies used by the organizations for Data Loss Prevention are common and are known to the attackers who are within the organizations, hence it is not difficult for the attacker like MIT to formulate an attack and gain information. An example to bypass the system would be, logging in from an authorized user's device and get the information or disable firewall.
- Attack Time identification: The attack time identification using DLP as a tool is very slow, as they can tell which account led to the attack but cannot concretely identify the attacker in all cases.

3.4 *Alternative Solution*

No security tool can guarantee complete eradication of an attack, we can only help lower the number and make it difficult of the attacker to orchestrate the attack as the ultimate goal of any perimeter specialist is to safeguard and protect the sensitive and private data as well as they can. In this section the author is trying to suggest an alternative solution to contain an Insider Threat.

According to the Author a better solution to the problem of Insider Threat would be the use of Biometric Encryption along with Technological based tools such as Data Loss Prevention Tools.

In this solution, the data before being uploaded to the server should be encrypted using the Biometric Encryption technology which uses a Biometric Template as a decryption key unique to an individual, once the data is encrypted and stored on server only people with the decryption key, i.e., people with the biometric key can access the data[14][15]. Each data should be encrypted with two biometrics meaning that it would require two members or biometrics to decrypt it and this biometric linked to the data should be used as a policy in the Data Loss Prevention Tool in order to keep a check on which biometric(which human being) is accessing the data and when. It is similar to requiring two different signatures from an organization to withdraw money from the bank, where the two signatures are the biometrics, the bank checking the two signatures and notifying the organization is the Data Loss Prevention Tool. This encryption method when used with current techniques such as Data Loss Prevention and its policies mentioned in section 3.5 will help the organization detect the Insider Threat and the bad actor associated with it faster than it does now. While this method does not completely eradicate the attack, it helps add an additional layer of security to reduce the number of attacks.

Like every solution this solution has its own advantages and disadvantages, which are as follows:

Advantages of using this solution:

- It makes it difficult for the attacker to steal data and sell it as only people with registered biometrics can access the data, and if a member with a registered biometric is trying to sell it, he or she would require another matching biometric to decrypt the data making it difficult for a single member of the organization to carry out this attack.

- Since this attack is a Human based attack, it monitors human interaction with that data instead of the data alone hence if an attacker tries to use someone else's device to carry out the attack that won't be possible without the authorized individual's biometrics.
- The detection rate and source of the attack would be easier to establish with the copy of the biometric.

Disadvantages of using this solution:

- The encryption is not completely developed and even after it is complete it will take more time to be compatible with the tools such Data Loss Prevention.
- It will be more expensive than the current solutions that the organizations have access to.
- It would still require constant monitoring and update in the policies.

3.5 *Policies that can be used by organizations for Data Loss Prevention*

Every organization has its own needs and wants to protect its sensitive data and therefore the policy could differ for every organizations. Some commons policies the author believes should be a part of the Data Loss Prevention Tool are:

- Data Classification Policy[13]: As the name suggests in this policy the organization can classify its data. Which data should be available to which member/employee of the organization? For example, should a Manager in the Software Development Department have access to the research data in the Health industry or should he have access to the backend code for the API.
- IP Blocking Policy: In this policy Certain IP addresses should not be allowed to view or access the protected data at all.
- BYOD Limit Policy: In this policy the devices that are not issued by the company and belong to the employee should not be given access to the data.
- Employee on leave Blocking: In this policy, the organization must ensure that devices belonging to or authorized to employees who are on temporary leave be it vacation or maternal leave, should not have access to any data.
- Data Encryption Policy: In this policy the organization must ensure that all data being sent out from a device connected to the network is encrypted and can only be viewed from a device connected to the same network to ensure that every time the data is sent or received the organization is notified.
- Specified Network Access: In this policy the organization must ensure that certain members are not given privileges to access certain confidential networks which could have vulnerabilities that could cause a threat to the organization Confidentiality, Integrity and Availability of sensitive data.
- Biometric Policy: In this policy, the organization must ensure that every time a data associated with a certain biometric is accessed or tampered with, it should immediately notify the organization so that the attack can be contained to a certain extent.

IV. Conclusion

Insider Threat attack unlike other attacks is much more unpredictable and the success rate of this attack has only been growing in the last decade. The world has seen a drastic rise in the number of attacks in the past five years alone and the number is only about to rise due to the current COVID-19 Pandemic in the year 2020 and 2021, and therefore it is essential to come up with new solutions.

The reason behind the increase in the number of attacks and the success rate are:

- Digitalization: As organizations are completely dependent on Internet and network due to the current Pandemic, it is easier for attackers to orchestrate an Insider Threat and it is even more difficult for the organization to detect it, as these attacks will take place through remote servers. With the current work from home policy it is difficult to administer each and every account using any of the modern techniques, people could easily find a way to steal data from the company.
- Saturation Point: The current techniques have reached its saturation point as the attackers have been successful so far with attacking companies. The rise in the number of Insider Threats only proves that the modern techniques have also reached its saturation point.
- Attack Sophistication: As mentioned in Section 3.4, attackers always find a way to break the system, be it using brute force method, or using modern algorithms and technologies. Since the attacker only has to be right once while the Cybersecurity team has to be right always the probability that an attacker will succeed once is much higher than the probability that the organization will never fail.
- Poor Economy: As mentioned in section 2.2, Money and Revenge of getting fired from an organization is a strong motive to carry out such an attack. With the current economy on the decline due to the Pandemic, people are not being compensated properly and many are losing jobs, which gives them strong intent to carry out an Insider Attack.

V. References

[1] CDSE, "Potential Risk Indicators: Insider Threat What is the 'something' we should be looking for," *CDSE Insider Threat Job Aid*, p. 1, Aug. 2015.

[2] "National Insider Threat Task Force," *Office of the Director of National Intelligence*, 01-Jan-2012. [Online]. Available: https://www.dni.gov/index.php/ncsc-features/243-how-we-work/1449-national-insider-threat-task-force-nitff. [Accessed: 16-Oct-2020].

[3] Editorial Team, "Creating an insider threat program: Everything you need to know," Virtru.com, 12-Jul-2020. [Online]. Available: https://www.virtru.com/blog/insider-threat-program/. [Accessed: 16-Oct-2020].

[4] A. Cosgrove and S. 8, "Mapping the motives of insider threats," *Help Net Security*, 07-Sep-2020. [Online]. Available: https://www.helpnetsecurity.com/2020/09/08/mapping-the-motives-of-insider-threats/. [Accessed: 15-Nov-2020].

[5] "What is Data Loss Prevention (DLP): Data Leakage Mitigation: Imperva," *Learning Center*, 17-Jun-2020. [Online]. Available: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/. [Accessed: 26-Nov-2020].

[6] "6 reasons why Data Loss Prevention is necessary for business?," *CloudSecureTech*, 17-Jan-2017. [Online]. Available: https://www.cloudsecuretech.com/6-reasons-why-data-loss-prevention-is-necessary-for-business/. [Accessed: 28-Nov-2020].

[7] N. Ismail, "The insider threat – are legacy systems the weakest link?," *Information Age*, 15-May-2018. [Online]. Available: https://www.information-age.com/insider-threat-legacy-systems-weakest-link-123466456/. [Accessed: 28-Nov-2020].

[8] M. Jansen, "Reducing Insider Threat Risk Through IAM," *Delta Risk*, 18-Feb-2020. [Online]. Available: https://deltarisk.com/blog/reducing-insider-threat-risk-through-iam/. [Accessed: 28-Nov-2020].

[9] James A. Martin and John K. Waters, "What is IAM? Identity and access management explained," *CSO Online*, 09-Oct-2018. [Online]. Available: https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html. [Accessed: 28-Nov-2020].

[10] "Insider Threat Indicators in User Activity Monitoring," *Center of Development of Security Excellence*, 28-Nov-2020.[PDF].Available https://www.cdse.edu/documents/cdse/Insider-Threat-Indicators-in-UAM.pdf

[11] J. Fruhlinger, "What is DLP? How data loss prevention software works and why you need it," *CSO Online*, 03-Jul-2020. [Online]. Available: https://www.csoonline.com/article/3564589/what-is-dlp-how-data-loss-prevention-software-works-and-why-you-need-it.html. [Accessed: 30-Nov-2020].

[12] “Creating Data Loss Prevention Policies,” *T-Minus 365*, 22-Jun-2020. [Online]. Available: https://www.youtube.com/watch?v=HFe29NvIxKw. [Accessed: 30-Nov-2020].

[13] K. Flanagan, *YouTube*, 20-Aug-2010. [Online]. Available: https://www.youtube.com/watch?v=lQsoVZOwF1w. [Accessed: 01-Dec-2020].

[14] “What is Biometric Encryption?: Security Encyclopedia,” *HYPR*, 20-Nov-2020. [Online]. Available: https://www.hypr.com/biometric-encryption/. [Accessed: 04-Dec-2020].

[15] A. Cavoukian and A. Stoianov, "Encryption, Biometric," *SpringerLink*, 01-Jan-1970. [Online]. Available: https://link.springer.com/referenceworkentry/10.1007/978-0-387-73003-5_63. [Accessed: 04-Dec-2020].

[16] "Insider Threat Statistics for 2020: Facts and Figures," *Ekran System*, 02-Oct-2020. [Online]. Available: https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures. [Accessed: 05-Dec-2020].

[17] G. Deyan, "20 insider threat statistics to look out for in 2020," Techjury.net, 06-Apr-2020. [Online]. Available: https://techjury.net/blog/insider-threat-statistics/. [Accessed: 16-Oct-2020].