ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 1, pp: (32-37), Month: January - March 2020, Available at: www.researchpublish.com

Protocols and Standards of Insider Threat: Issues and challenges

[1]Latifa Hussaini, [2]Jamaludin Ibrahim

[1,2] Faculty of Information and Communication Technology, International Islamic University Malaysia

Abstract: **Threat from the insider of corporates is a serious problem since it is very challenging to recognize them from a benign activity. In this paper, we discuss and describing various types of insider threats. Next, we discuss the related work on insider threat mitigation in both technical and non-technical approaches. It is found that tackling insider threat requires both technical, and non-technical approaches to enable qualified detection of threats and seems to lose importance an IT infrastructure is used in performing insider attacks.**

Keywords: **Insider threat, Cyber security, Insider threat Mitigation.**

1. INTRODUCTION

Remotely hosted services on the cloud are being used by 80 percent of the organizations and a greater number of them are depending on the computers in every aspect of their daily operation [1]. Most administrators have begun to centralize citizens' information in large data service centers, while the citizens themselves also rely on cloud computing to store their confidential data. All this makes data theft simpler. Most of the decision-makers in governments and companies are concentrating on external cyber-attacks such as the denial of service, viruses, Trojan horse, Worm, unauthorized access, etc. To hinder networks from external cyber-attacks, 10 percent of the IT budget has been used to protect the organizations from external attacks. However, recent evidence depicts that both external and insider threat is notable [1], while the harm caused by insider threats are harmful than that of outsider attacks [2]. This means that anyone who has the authorization to access an organization's data assets is more serious than any other security threat. The priciest form of attack is insider which costs $8.76 million according to 2018 recent report the Ponemon Institute report [3]. This is because the insider has knowledge of organizations processes, and access to, their employer's assets, this has come about because such an individual has had the trust of the organization causing him or her to be supplied with authorized access so that it is possible to bypass all physical and electronic security measures. However, the number of insider threat incidents has continued to increase to a high extent. According to an insider threat report, 70% of organizations observed that insider attacks have become more frequent over the last 12 months. 60% have experienced one or more insider attacks within the last 12 months [4] but a study shows that more than 70% of these incidents usually go unreported and are handled internally [5].

1.1 What is an Insider Threat?

To understand the definition of an **insider threat**, we must know what an insider is. An **insider** - "Is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure" [6], simply as: an individual who has authorized access to organizations network, system, or data. A **Threat** – refers to anything that has the potential to cause serious harm or damage to an organization's IT systems or assets. An **insider threat** is a malicious **threat** to an organization that comes from people within the organization such as - a) on the part of an employee (privileged users, such as IT team members and superusers) b) knowledge workers and those who have had authorized access to the company's IT assets (analysts, developers, resigned or terminated employees) c) Employees involved in a merger or acquisition e) third parties such as vendors, contractors, partners.

1.2 Factors motivating insiders

According to [7] assumptions, an attacker misuses his/her privilege due to three factors a) insider threat must have the motivating force to attack b) he must identify an opportunity" and c) he must have the capacity to launch an attack. A recent study by Colwill [8] reports that "insider attacks are made with varying degrees of motivation, opportunity, and capability. Motivation will come from internal, personal drivers, whereas opportunity and capability will be given to insiders overtly by your organization to perform their role or maybe attained covertly once they are on the inside".

2. TYPES AND CATEGORIES OF INSIDER THREAT

In general, Insiders are consisting of seven sub-categories based on the ways which have affected the company's security assets and the human factors.

2.1 Insider Social Engineering

An Insider Social Engineering (SE) is when another innocent employee has been manipulated by a psychological act of malicious insider without their knowledge to reveal confidential data or do an action to damage the company's IT network infrastructure, applications or services. However, insider SE occurs when the insider or outsider does not have the full to access part of, or all of, the company's assets. Insider SE, in general, involves an employee or outsider, using psychological manipulation, working inside normal hours, preparing them-selves and planning before the attack, involving a human-based and technology-based attack. This action happens when the SE manipulates the user using a phishing email. They will click on the link which redirects them to fake websites but looks like a legitimate website. Thus, the attacker is able to steal the employee credentials and get access to a firm's confidential data.

2.2 Unintentional Insider threats

This is the type of insider threat is when an employee without the proper security awareness training can inadvertently expose confidential data often as a result of social devices or incorrectly send emails or files. Moreover, they are also called unintentional insider threats who accidentally do an action to harm the company's IT and network infrastructure [13]. They are current employees working within an office and have authorized access to a target system that lead to the inadvertent incident without a malicious motive. An account manager who was working in a pharmacy company in the USA has made a mistake which caused her firm to fire her after performing an accidental security breach. The unintentional insider downloaded a file containing the prescription information of 6,000 patients with full patient details onto a memory stick, which she then lost. This is incident occurred because the victim does not have security awareness training, poorly understanding of the firm security system, poor management systems, work under pressure, or lack proper knowledge in her task or uses drugs [13][9].

2.3 The Insider Theft of Intellectual Property (IP)

It is defined as an insider use of information technology to steal proprietary information from an organization which Intellectual property is defined as intangible assets created and owned by the organization that are critical to achieving its mission for examples software code, business plans and product designs. They are current employees working in their resignation notice period in the office, who has authorized access to IP. They are holding technical positions such as programmers, engineers, scientists, or sales, during normal working hours and do require any tools to initiate and attack. In a case study of September 2013 of intellectual property theft, a data breach occurred in a German mobile telecommunication company by an insider who had knowledge of their IT infrastructure and system, he handle to a copy of more than two million customers information records such as customer names, addresses, dates of birth and account details [12]. Someone who has been part of the process that creates the organization's IP is an IP theft. While other types of IP theft steals IP for financial for the themselves.

2.4 Insider IT Sabotage

The attack is launched by an employee who utilizes his/her IT skills in a company or an individual. Overall, insider IT saboteurs are former employees, working remotely, without authorized access to target systems, working outside normal hours, who make themselves ready and launch the attacks. Their main targets are databases, systems, and network devices. Moreover, malicious users are often the worst enemies of IT and information security professionals because they know exactly where to go to get the goods and don't need to be computer savvy to compromise sensitive information. These users have the access they need, and the management trusts them — often without question. Based on the

information from ***the Software Engineering institute*** database about insiders who commit IT sabotage, 86% held technical positions, and most of the crimes used sophisticated technical means to harm the organization. Of those insiders, 90% had administrator or privileged access at their organization, and 75% of the organizations experienced disruptions in business operations. Organizational reputation was affected by IT sabotage at 28% of the organizations [8].

2.5 IT Fraud

Is an insider's use IT authorization to modification, deletion, or creation of the organization data for personal gain. This type of insider threat will affect the confidentiality, integrity, and availability of the information. Insider threats who are committing insider fraud are generally employees working in an office and has authorized access to the information assets, it is a non-IT position who works under normal business hours. There are case studies of insider IT fraud in the US, which depicts how a malicious insider working for a banking company, having access to sensitive information of the organization could harm the firm's confidentiality and damage its long-term reputation for personal gain. However, the company discovered the breach after a few months they found outsider private capital one data on GitHub. IT fraud is caused by the greed of employees who work to benefit themselves for financial gain. The financial pressure caused by the outside environment is what motivates the fraud crime.

2.6 Insider National Security

Insider national security (NS) threats involve an insider using their authorized access to represent a threat or do harm to a country's NS. This threat can include damage to the country through espionage, sabotage, disclosure of NS information, or through the loss or degradation of departmental resources or capabilities. Their main targets are the NS secret information. The biggest intelligence leak in U.S. history was launched by a malicious insider (a trusted IT contractor) who worked for the NS Agency (NSA). Edward Snowden managed to download millions of documents on classified intelligence collection programs, as he had authorized access to mass electronic surveillance data as part of his job. Then he leaked classified material to media outlets. Since then he has released details of unwarranted NSA hacking of friends and for alike, the fallout damage U.S. relations abroad and putting a spotlight on current security issues facing the U.S. The motivations of national security insider for malicious actions are money, psychology, accident, revenge.

2.7 Insider in Cloud Computing

An insider in cloud computing or insider in service providers is those working inside service provider company environments, who perform malicious insider actions without the client's knowledge to harm their data asset confidentiality. However, there are neither possible ways of detecting such an attack during or even after the breach, as the client has no control over service provider infrastructures or any effective method and tools to prevent such an attack. Insiders in the cloud in generally current employees, working in a technical position, during normal hours, who have fully authorized access to target infrastructure, who are well planned and have a malicious motive. The main insider targets are data assets such as databases, source codes, business plans, and strategic plans [11][14][15]. Malicious threats from inside the cloud computing providers and caused by their employees are increasing. Using their authorized access rights to the environment, they commit security breaches such as file recovery, coping virtual machine files, and removing disks from a RAID.

3. RELATED WORK ON MITIGATING INSIDER THREAT

Insider threats are a complex undertaking that does not test solely on IT's shoulders. Rather, countering the threat requires collaboration between IT, HR, legal, contracting security and data owners. Mitigating the risk of system compromise and intellectual property violations requires a comprehensive risk management process with enterprise-wide policies, procedures, and technologies that enable proper alerting, analysis and reporting. Based on our research on insider threats, it has been found that researchers have mostly focused on three types of insider threats: fraud, intellectual property theft, and IT sabotage, and includes information about the perpetrator, organizations involved, and incident details. This information is derived mainly from public sources (e.g., media reports and court documents) but also includes some data from non-public sources (e.g., law enforcement investigator notes) and past research papers.

3.1 Technical approach to recognize insider

The first area we consider are technical approach. This includes the means for insider to carry out insider threat also means for mitigating and monitoring.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 1, pp: (32-37), Month: January - March 2020, Available at: www.researchpublish.com

3.1.0 Intrusion Detection Systems (IDS)

It is a device or software application that monitors a network or system for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. Stems IDS are used to detect malicious intruders in real-time that drive from outside threats, that is based on monitoring endpoint devices or networks through identifying traffic pattern and activities from any abnormal actions in the network and endpoint, via matching activities and traffic with a database of attack signatures. The IDS displays an alert if it found abnormal behavior. As IDS collects the data over different platforms in real-time, it is a useful tool for detecting a malicious insider by analyzing information any activity that may lead to data breaches or information of any altar of user actions [17]. On the other hand, IDS has its limitations in dealing with insider threats such as a huge database log file size, a high number of false alarms, and requiring an administrator to analyses the traffic and behavior. Moreover, it is not able to monitor encrypted traffic [16].

3.1.1 Data Loss Prevention

Data Loss Prevention (DLP) is a tool used for making sure that end users do not send sensitive or critical information outside the organization network. It can also be described as a software product that helps a network administrator control what data end users can transfer. It is executed in three steps. a**. System discovery involves** watching user behavior, capturing network data flow, and network scanning storage devices. b**. Identification of leaked confidential data** the data that is discovered in the first step could be identified as secret information based in three ways: regular expressions, keyword matching, or hashing fingerprinting. c**. Corporate policy enforcement** - this step hinders any behavior that could cause a security threat in identified confidential data in the previous step [18].

3.2 Non-Technical approach to recognize insider threat:

It is obvious that insider threat is a human problem and they are given the trust, it is a difficult issue to mitigate the threat level of a malicious insider, so, we need to tackle the problem of insider threat from a different perspective, such as awareness, security policy, and prediction training.

3.2.0 Psychological Prediction Model:

User behavior from a psychological point of view, there is a relation between psychology indicators and a malicious insider threat: these are 1) opportunity 2) motive 3) capability [19][20]. Axelrad et al. [21] proposed a model to define 83 psychological variables possibly correlated with the prediction of insider threats. The method was to evaluate each of these variables and assign an estimated score power to each variable. The variables consist of personal characteristics, dynamic environmental stress such as work and file stresses, insider actions such as personal attribute; and degree of interest such as insider threat profile. Moreover, another classification method was proposed for malicious insider threats based on past case studies of insider threat breaches. Greitzer et.al [22][23]. They have used 12 indicators related to insider threats. Greitze's risk indicators classified by the weight of the indicator's risk layers.

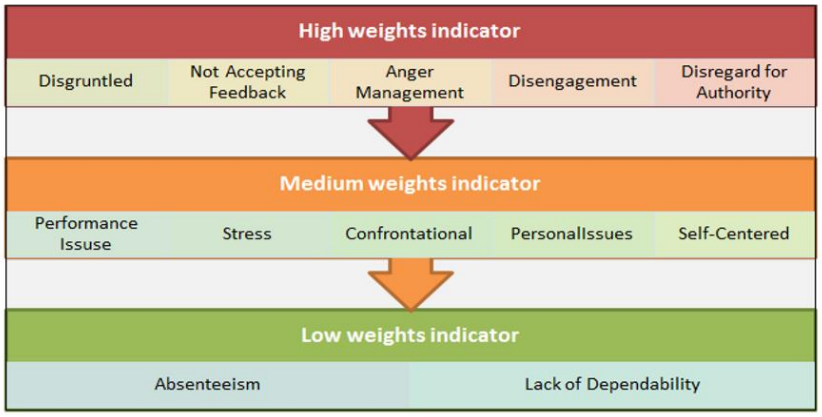

Figure 1: Greitze's risk indicators [22]

This model can assist decision maker so identify the malicious insider threats from a normal user, depending on scoring indicators.

3.2.1 Security awareness and Education

One of the most effective ways to reduce insider threat is my proving the appropriate awareness training, and security education [24], particularly unintentional insider threat. Organizations conduct regular user training programmed as part of their attempts to assure the corporate from insider threats, with 11 percent of IT budget designated to awareness and security education. Awareness and educational training could involve the following fields: a. Online training courses b. Classroom courses c. presentation by outside speakers. The training objective includes a) consequences and sanctions b) incident reporting responsibilities and procedures c) handling of sensitive information d) social engineering scams e) unintentional leaking f) intellectual property protection e) insider threat indicators [3][25][10].

3.2.2 Information security Policy

An organization's information security policies deliver the framework that sets the most critical controllers within the organization once the organization's objectives have been identified. It comes in a detailed statement of employees' expectations of an organization, and what is expected from them in terms of information security, and the acceptable behavior and culture within the organization [25] [27] [28]. An up to date paper by Cyber Security Center at the University of Oxford [10] concentrated on the ability of a company's information security policies to reduce the risk of an unintentional insider threat that is potentially more critical than that posed by other malicious insider categories. Thus, they found that 45 percent of the employees do not follow the information security policies due to two main reasons a) The policy was poorly defined, or b) the staff member was not aware of the security policy. They summed up in their article that if the information security policy is not followed by all authorized users the unintentional insider threat will increase. And that will assist to reduce the insider threat levels.

4. CONCLUSION

In this paper, we have reviewed and presented various characteristics and categories of insider threats, by dividing the insider threat category into seven sub-categories, based on the way they affect the organization's information security goals and the human factors which lead an insider to act maliciously. We have also considered some of the current approaches and controls associated with mitigating the level of insider threat, by classifying them into two main categories: technical mitigation and non-technical mitigation approaches. We have found that there is no solution which can fully eliminate insider threat within organizations. Also, a technical approach itself may not be the most effective way to prevent and/or detect malicious insider threats.

REFERENCES

[1] C. Miller, "Information Security Breaches Survey," Dep. Business, Innov. Ski., 2013.

[2] S. Gorniak, D. Ikonomou, P. Saragiotis, I. Askoxylakis, P. Belimpasakis, B. Bencsath, M. Broda, and C. Vishik, "Priorities for Research on Current and Emerging Network Technologies," Eur. Netw. Inf. Secur. Agency, 2010.

[3] "2018 Cost of Insider threats: Globa Organizations". Available: https://www.observeit.com/ponemon-report-cost-of-insider-threats/

[4] "*Insider threat report*" Available: https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

[5] Online available at: https://www.ieee-security.org/TC/SPW2018/WRIT/ Pdf report: https://www.ieee-security.org/TC/SPW2018/WRIT/WRIT2018Program.pdf

[6] M. Bishop, D. Gollmann, J. Hunker, and C. W. Probst, "Countering insider threats," in Dagstuhl Seminar Proceedings 08302, 2008, pp. 1–18.

[7] W. Bradley, "AN INSIDER THREAT MODEL FOR ADVERSARY SIMULATION," SRI Int. Res. Mitigating Insid. Threat to Inf. Syst. 2, pp. 1–3, 2000.

[8] C. Colwill, "Human factors in information security" Inf. Secur. Tech. Rep., vol. 14, no. 4, pp. 186–196, Nov. 2009.

[9] O. Buckley and J. Nurse, "Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat," Work. Socio, 2013.

[10] CERT Insider Threat Team, "Unintentional Insider Threats: Social Engineering,",Carnegie Mellon Univ, vol. CMU/SEI-20, no. January, 2014.

[11] A. Duncan, S. Creese, and M. Goldsmith, "An overview of insider attacks in cloud computing," Concurr. Comput. Pract. Exp., 2014.

[12] M. Lennon, "Insider Steals Data of 2 Million Vodafone Germany Customers,"2013.[Online].Available: http://www. securityweek.com/attacker-steals-data-2- million-vodafone-germany-customers. [Accessed:30-Apr2015].

[13] F. L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore, and D. Mundie, "Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies," 2014 47th Hawaii Int. Conf. Syst. Sci., pp. 2025–2034, Jan. 2014.

[14] M. T. Khorshed, a. B. M. S. Ali, and S. a. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Futur. Gener. Comput. Syst., vol. 28, no. 6, pp. 833–851, Jun. 2012.

[15] Z. M. Yusop and J. Abawajy, "Analysis of Insiders Attack Mitigation Strategies," Procedia - Soc. Behav. Sci., vol. 129, pp. 581–591, May 2014.

[16] S. Zeadally, B. Yu, D. H. Jeong, and L. Liang, "Detecting Insider Threats: Solutions and Trends," Inf. Secur. J. A Glob. Perspect., vol. 21, no. 4, pp. 183–192, Jan. 2012.

[17] M. Salem, S. Hershkop, and S. Stolfo, "A survey of insider attack detection research," Insid. Attack Cyber Secur., pp. 1–20, 2008.

[18] G. Silowash, D. Cappelli, and A. Moore, "Common Sense Guide to Mitigating Insider Threats 4th Edition,"Dec, 2012.

[19] E. E. Schultz, "A framework for understanding and predicting insider attacks," Comput. Secur., vol. 21, no. 6, pp. 526–531, 2002.

[20] M. Kandias, A. Mylonas, and N. Virvilis, "An Insider Threat Prediction Model," pp. 26–37, 2010.

[21] E. T. Axelrad, P. J. Sticha, O. Brdiczka, and J. Shen, "A Bayesian Network Model for Predicting Insider Threats," 2013 IEEE Secur. Priv. Work., pp. 82–89, May 2013.

[22] F. L. Greitzer and R. E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks," J. Strateg. Secur., vol. 4, no. 2, pp. 25–48, 2011.

[23] F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton, and R. E. Hohimer, "Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats," 2012 45th Hawaii Int. Conf. Syst, pp.2392–240.

[24] E. D. Shaw and L. F. Fischer, "Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations," Sep,2005.

[25] K. Roy Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," Inf. Secur. Tech. Rep., vol. 15, no. 3, pp. 112– 133, Aug. 2010.

[26] G. "Gus" Jabbour and D. a. Menasce, "The Insider Threat Security Architecture: A Framework for an Integrated, Inseparable, and Uninterrupted Self-Protection Mechanism" 2009 Int. Conf. Comput. Sci. Eng., pp. 244–251.

[27] M. E. Palmer, C. Robinson, J. C. Patilla, and E. P. Moser, "Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age," Inf. Syst. Secur., vol. 10, no. 2, pp. 1–15, May 2001.

[28] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," 2011 IEEE/IFIP 41st Int. Conf. Dependable Syst. Networks Work., pp. 129–134.