BOOK CHAPTER | The Weakest Link

Case Study: Assessment of Insider Data Attack

Akinsanya Seye Emmanuel
Department of Computer Science
Federal University Oye-Ekiti
Ekiti State, Nigeria
E-mail: sedalomo1@gmail.com
Phone: +2348100381619

Introduction

The issues of security and privacy have expanded significantly as a result of the growing use of technology to handle numerous sensitive tasks within an organization. The attack lunch by the Insider is the most deadly and expensive among major security and privacy attacks. Attacks by the insider are hostile actions carried out by persons who have been granted access to the organization details. Threats by an insider are difficult to detect because of the qualities of authorization granted to the person. Nevertheless, ignoring such dangers may result in an organization's assets, reputation as well as business goals being jeopardized. Insiders therefore remains the weakest link in the cybersecurity chain.

Figure 1: Insider Threat driving Information Security System & Infrastructure Failures
Source: https://www.isdecisions.com/blog/it-security/tackling-insider-threat-creating-a-culture-of-security-awareness/

Citation: Akinsanya S.E (2022). Case Study: Assessment of Insider Data Attack.
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

Nature and Types of Insider Threats

An insider threat refers to a cyber security risk that originates from within an organization. It typically occurs when a current or former employee, contractor, vendor or partner with legitimate user credentials misuses their access to the detriment of the organization's networks, systems and data (Homoliak et al., 2019; Greitzer, 2019).

There are two distinct types of Insider Threats:

1. The Malicious Insider: Malicious Insiders knowingly and intentionally steal data. ...
2. The Negligent Insider: Negligent insiders are just your average employees who have made a mistake.

Figure 2: Categories of Insider Threats
Source: ekransystem.com

The threat perpetrated by an insider can be intentional or unintentional

- Intentional threats are perpetrated with the intent to attack an organization for personal gain or to address a personal grievance. Most insiders, for instance, lunches attack just to avenge their right, probably the organization fails to promote them, give them expected incentive or unexpected firing. As a result, they release sensitive organization information, bugging coworkers, damaging equipment, and committing violence. Others have stolen confidential information or intellectual property that belong to the organization with mindset to advance their own career.
- Unintentional threats arise as a result of accident or negligence, these threats cannot be totally controlled but can be alleviate.

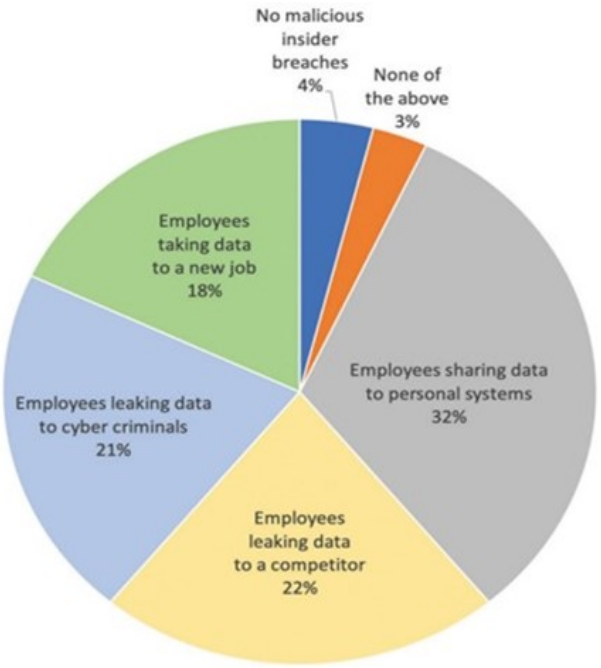

Figure 3: An Intentional Insider Threat Analysis
Source: 'Insider Data Breach Survey 2020', Egress.

Insider Data Theft Attack case study

The Tesla data theft Case indicated how dangerous an insider threat could be. In 2018, Tesler filed a lawsuit against Tripp, who was a former employee of Tesla. Tesla claimed in a complaint filed in Nevada that the employee, Martin Tripp, created code to export gigabytes of Tesla data, which include various secret pictures and video of Tesla's production system. According to the complaint, Tripp admitted he developed the software, but the software was also running on three more computer systems that belongs to Tesla employees. This is to enable him export data while not in office, therefore implicating the parties involved. According to the lawsuit, Tripp "expressed frustration" over his reassignment, and Tesla believes the data theft was all about revenge.

Recommendation

Insider threats can be mitigated by implementing the following measures:

- Conduct risk assessments across the entire organization.
- Policies and regulations should be clearly documented and consistently enforce.
- Create a safe working environment by using physical security measures.
- Installing security software and appliances, establish strong password and account management policies and procedures.
- All endpoints, including mobile devices, are monitored and controlled remotely.
- Increase the security of your network's perimeter, allow for observation, separation of duties and least privilege should be enforced.
- Make sure to properly recycle your equipment and documents.
- To track, monitor, and audit employee activity, use a log correlation engine or a security information and event management system (SIEM).
- Secure backup, archiving, and recovery procedures should be implemented.
- Identify potentially dangerous actors and respond quickly to suspicious conduct.
- Create a comprehensive protocol for terminating employees.

Conclusion

This research focuses on insider data threat using Tesla as a case study, the major categories of insider theft was identified (see Figure 2), it was observed that threat perpetrated by an insider can be intentional or unintentional, finally, possible remedy to mitigate insider attack was highlighted.

References

1. Categories of Insider Threats - ekransystem.com
2. Chris Brook (2021, August 6). Tesla Data Theft Case Illustrates The Danger of the Insider Threat. https://digitalguardian.com/blog/tesla-data-theft-case-illustrates-danger-insider-threat
3. Greitzer, F. L. (2019, April). Insider Threats: It's the HUMAN, Stupid!. In *Proceedings of the Northwest Cybersecurity Symposium* (pp. 1-8).
4. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2), 1-40.
5. https://pages.egress.com/whitepaper-insiderdatabreachsurvey2020-0320
6. Lee, C.; Iesiev, A.; Usher, M.; Harz, D.; McMillen, D. (2021, February). IBM X-Force Threat Intelligence Index. 2020. https: //www.ibm.com/security/data-breach/threat-intelligence
7. https://www.isdecisions.com/blog/it-security/tackling-insider-threat-creating-a-culture-of-security-awareness/