Privacy Assessment

Privacy Assessment

Nathan Ketterlinus

March 3, 2024

Towson University, COSC418-102, Steven Evans

Abstract

This paper answers the questions proposed by the Blackboard assignment “From Week 4 Privacy Assessment Due Mar 3, 2024 in Week 5”. It names the 3 types of privacy vulnerability mitigation controls: technical, physical, and administrative. It provides examples of each and looks in-depth at a study that used machine learning to detect insider threats. In addition, it proposes four policies for a fictitious organization that address four different privacy considerations, with sample implementations for each.

Privacy Assessment

1. The three controls used to mitigate privacy vulnerabilities are technical, physical, and administrative. Technical controls are those that are implemented through hardware or software, such as firewalls or regular software updates (Klepper, 2019). Physical controls are those that are implemented physically to secure a site. Examples include "data center perimeter fencing, locks, guards, access control cards, biometric access control systems, surveillance cameras and intrusion detection sensors" (IBM, 2022). Finally, administrative controls are those that deal with selecting and training prospective employees to be properly privacy oriented. They are largely concerned with detecting and preventing insider threats. Manoharan et al. found a promising method to detect insider threats from balanced data sets by utilizing supervised machine learning. Sparing technical details, they found that a "supervised learning with a balanced dataset in RF obtains the best accuracy [discriminating threats vs non-threats] and F1-score of 95.9%" (Manoharan et al., 2023).

2.

a. Password security. All passwords must be a minimum of 12 characters (16-18+ are encouraged), using a mix of numbers, uppercase, lowercase, and symbols. In addition, passwords must be changed every 6 months without reusing old passwords. While this may seem a bit overkill, it provides incredible protection against brute force attacks, requiring 30,000 years to crack with publicly available technology in 2023 (Redzepagic et al., 2023).

b. Employee training. All employee training should include a comprehensive review of best security practices in the workplace, privacy expectations as an employee, how to properly handle and report privacy violations, and the importance of combatting insider threats.

c. Principle of least privilege. All company employees are given system and site access according to the principle of least privilege. This means that the only people that have access to any given resource are those that absolutely need it to do their job. It wouldn’t make sense to give the janitor access to the server room holding millions of dollars in trade secrets, for example.

d. All devices used on site or to do work of any kind must be company issued. BYOD policies, while convenient for the average employee, are an IT nightmare. The variance between devices means that the odds of a novel vulnerability unique to one system are much higher. By unifying used devices to the same security standard, vulnerabilities become much easier to patch out across the entire network.

e. (described in a-d respectively).

References

IBM. (2022). What are security controls? <https://www.ibm.com/topics/security-controls>

Klepper, M. (2019, October 30). Technical controls to mitigate security risk. Infosecurity Magazine. <https://www.infosecurity-magazine.com/blogs/technical-controls-mitigate/>

Manoharan, P., Yin, J., Wang, H., Zhang, Y., & Ye, W. (2023). Insider threat detection using supervised machine learning algorithms. Telecommunication Systems: Modelling, Analysis, Design and Management, 1–17. <https://doi.org/10.1007/s11235-023-01085-3>

Redzepagic, J., Dakic, V., Stanesic, J., & Basic, M. (2023). Analysis of Password Security Policies and Their Implications on Real-Life Security. Annals of DAAAM & Proceedings, 34, 77–81. <https://doi.org/10.2507/34th.daaam.proceedings.011>