A Report on Potential Security Threats Affecting the Smith and Co Second-Hand Bookshop Database

Asala Aljazaery

3 October 2022

University of Sunderland

Contents

1 Introduction

The rapid increase in data volumes requires new solutions to handle it in real time and make it immediately accessible. Thus, data security is critical for building any system to protect the data from unauthorised usage and malicious attacks (Gahlot, Verma and Khandelwal, 2017). This report will shed light on potential database attacks for a bookshop company called Smith and Co Second that keeps records of their customers and book details. This report summarises the classification of database attacks, discussing two types of attacks that may occur in the company, including the system weakness that influences these types of attacks and the type of data that might be targeted.

2 Classification of Database Attacks

The attacks are classified into four categories: direct attacks are when data is the target, while indirect attacks collect information about the data using different methods. Finally, in active attacks, the hacker modifies the actual data values, resulting in misleading data and losing the actual data. In contrast, passive attack hackers observe the data without modifications (Gahlot, Verma and Khandelwal, 2017).

3 Potential Database Attacks

This section will present two possible attacks threatening the Smith and Co Second-Hand bookshop database.

3.1 Brute force

Weak authentication is the main reason behind this type of attack. Allowing the users to use common and easy passwords or storing the system credentials in an insecure database leads to weak security. Weak security makes the database an easy target for attackers and more valuable. The weak authentication can be due to missing requirements while developing the system (Pill Citp, 2019). These attacks seek these types of weaknesses

in the system, break through the login requirements by trying every combination of credentials, and the less complex passwords take less time to be figured (Technology, 2022). Authentication can be achieved by reviewing the time of the day that login has been initiated, the location of this access, and the volume of data that has been reviewed or changed. In authentication, users must be identified before accessing the company resources (Gahlot, Verma and Khandelwal, 2017).

3.2 Privilege escalation

The database has a list of authorised users with different data access levels. A privilege escalation requires someone with a high level of access. It may be a person with high access whose job does not require this level of access to complete it, or the hackers can award themselves access through the internet by taking some low-level user account and using it as an entry point to escalate privileges and gain full system access that credentials are not necessary anymore (Technology, 2022). Privilege escalation can occur due to the system being out of date or misconfiguration. Privilege abuse can be deprived by giving the users the minimum required access to the resources (Gahlot, Verma and Khandelwal, 2017).

4 Data Types

The hackers attack databases that contain sensitive data, for example, Financial Information such as Payment Card Information and Personal Identifying Information such as Customers' full names, physical addresses, and contact numbers (Post, 2019). This information can be used in illegal acts, and the company will lose the customer's trust (Technology, 2022). In addition, the company's competitors may purchase the leaking data to see how it is doing regarding book prices to steal their customers or use it against the company (Gahlot, Verma and Khandelwal, 2017).

5 Conclusion

Authentication and authorisation requirements are essential things in the database. However, this system may contribute to serious privacy concerns that should be considered before using it. Protecting the database is essential from any illegal access or threat because the consequences of destruction and the leaking of customers' confidential information will make the company struggle to recover or compete afterwards (Gahlot,

Verma and Khandelwal, 2017).

References

Gahlot, S., Verma, B. and Khandelwal, A. (2017) 'Database Security: Attacks, Threats and Control Methods', *International Journal of Engineering Research*, 5(10), p. 4.
Pill Citp, M. (2019) *Top ten database attacks | BCS*. BCS, The Chartered Institute for IT. Available at: https://www.bcs.org/articles-opinion-and-research/top-ten-database-attacks/ (Accessed: 20 September 2022).
Post, A. (2019) *Data Breaches 101: Why They Happen and What Data Gets Stolen*. Cybint. Available at: https://www.cybintsolutions.com/data-breaches-101-why-they-happen-and-what-data-gets-stolen/ (Accessed: 25 September 2022).
Technology, S.D. (2022) *6 Types of Database Attacks Hackers Use to Obtain Unauthorized Access - Salvation DATA*. Available at: https://www.salvationdata.com/crime-cases/6-types-of-database-attacks-hackers-use-to-obtain-unauthorized-access/ (Accessed: 20 September 2022).