

A Case Study on the Importance of Authorization Controls

How a lack of proper authorization controls led to a data breach at a governmental agency

Introduction

Authorization controls are the mechanisms that determine what actions a user can perform on a system or a resource. They are essential for ensuring sensitive data's confidentiality, integrity, and availability and preventing unauthorized access or misuse. Authorization controls can be implemented at different levels, such as network, application, database, or file system. They can use various methods, such as role-based access control (RBAC), attribute-based access control (ABAC), or mandatory access control (MAC).

This document presents a case study of a data breach that occurred at a governmental agency due to a lack of proper authorization controls. We describe the background of the incident, the root cause of the breach, the impact of the breach, and the lessons learned from the incident. We also provide some recommendations for improving the authorization controls at the agency and preventing similar violations in the future.

Background of the Incident

The governmental agency in this case study is a large department that provides various public services to citizens, such as education, health, welfare, and security. The agency has a complex information system consisting of multiple applications, databases, servers, and devices, which store and process the citizens' personal information (PI) and the agency's classified and confidential data. The agency is subject to the Federal Information Security Management Act (FISMA), which requires the protection of PI from unauthorized access, disclosure, or modification.

The data breach occurred in June 2023, when an unauthorized user accessed the agency's education application and downloaded the records and reports of over 10,000 students. The education application is a web-based system that allows educators and other authorized staff to view, edit, and share the education records and reports of the students. The application is connected to a database that stores the PI of the students, such as their names, dates of birth, social security numbers, grades, and attendance. The application also has a feature that allows users to export records and reports to portable devices, such as USB drives or CDs, for backup or transfer purposes.

Root Cause of the Breach

The root cause of the breach was the lack of proper authorization controls in the education application. The application did not implement any mechanism to verify the identity and role of the users who accessed the system. The application only required a username and password, which the unauthorized user guessed or obtained quickly. The application also did not enforce any restrictions on the users' actions on the system. The application allowed any user to view, edit, and export any record and report of any student, regardless of their role or need-to-know. The application also did not maintain any user activity audit logs, making it difficult to detect and trace the breach.

The lack of proper authorization controls in the education application was the result of several factors, such as:

- The application was developed by a third-party vendor, who did not follow the best practices and standards for information security and privacy.
- The agency did not conduct a thorough security assessment and testing of the application before deploying it in the production environment.
- The agency did not have a clear and comprehensive policy and procedure for managing the access rights and privileges of the users who accessed the application.
- The agency did not adequately train and inform the application's users and administrators about the importance and proper use of the authorization controls.

Impact of the Breach

The breach had a significant impact on the agency and the citizens, such as:

- The breach compromised the confidentiality and integrity of the PI of over 10,000 students, which could expose them to identity theft, fraud, blackmail, discrimination, or other harms.
- The breach violated the FISMA regulations, which could subject the agency to legal actions, fines, penalties, or sanctions from the regulators, the citizens, or other parties.
- The breach damaged the reputation and trust of the agency, which could affect its public service, budget, and performance.
- The breach disrupted the everyday operations and services of the agency, which could affect the quality and efficiency of the public service.

Assignment

Working with others on your team, identify examples of internal controls that could and should be in place to reduce the risk of a similar instance affecting the organization. Additionally, identify examples of controls that might have been effective previously, but may no longer be effective at mitigating authentication risk.