ACTIVITY_F1
Security Analysis for System Integration

Group 4
Austria, Jonald Kiel
Aliño, Mark
Bialen, Eurika Angela
Carapatan, Jamil Aaron
Dalanon, Harvey Collin
Lacuarin, Vince Given

November 28, 2024

Tasks

Risk Identification:

- **Data Breach:** There is an exposure of sensitive user information during the integration process. It may range from financial damages and losses.

- **Unauthorized Access -** Unauthorized users may gain access to the system in the integration process.

- **Non-compliance with Data Privacy Laws -** There might be possibilities of violating regulations if the data transferring process did not meet the legal requirements of the system.

Impact Analysis:

- In the data breach risk, there may be loss of sensitive customer data, including personal infromation, financial data, and transaction history. It can damage the company in terms of technical issues that could cause downtime and lost productivity that can impact the ability to process payments and conduct business.

- There may be potential data manipulation, theft or misuse, and disruption of business operations and financial losses. Direct financial impacts from fraud, chargebacks, and indirect costs from investigating incidents and improving systems.

- For non-compliance with data privacy laws, there may be legal penalties and fines. Potential legal action from affected parties may happen. Customers' and partners' trust might gone negative and can harm business reputation.

Mitigation Strategies:

- For mitigating the unauthorized access, the company should use Multi-Factor Authentication for all access points and also assign RBAC to limit access to sensitive data. Moreover, encryption of sensitive information, regular security audits, and monitoring of system access logs may help detect and prevent illegal activities. A good practice in cybersecurity may reduce the likelihood of unauthorized access.