Vulnerability Assessment Report

2nd November 2024

System Description

The information system assessed in this report supports core business functions and includes interconnected servers, databases, and user access points critical for operations. It hosts sensitive data such as customer information, transaction records, and internal communications. The system environment comprises both on-premises and cloud-based components, allowing for flexible access but increasing exposure to various security risks. Due to its central role, the system must prioritize confidentiality, integrity, and availability, with robust security measures to prevent unauthorized access and ensure business continuity.

Scope

The scope of this vulnerability assessment covers the entire networked environment, including servers, databases, and user access controls. Key areas of focus include external threats from hackers, potential software vulnerabilities, and insider threats. This assessment identifies and evaluates risks related to unauthorized access, data breaches, and operational disruptions. Security controls such as least privilege, multi-factor authentication, and defense in depth are evaluated to determine their effectiveness in mitigating identified vulnerabilities. This assessment aims to provide actionable insights to strengthen the security posture and safeguard sensitive data.

Purpose

A database server is a vital asset for any business, serving as the backbone for storing and organizing critical data, from customer profiles and sales records to financial information and inventory logs. This centralized access enhances operational efficiency, decision-making, and responsiveness, which directly support the company's goals and customer service standards. Protecting the server is equally essential, as a breach could expose sensitive information, disrupt trust, and lead to costly legal issues. Securing data prevents unauthorized access and safeguards the integrity of the business, ensuring it complies with regulations and maintains its reputation. If the server were to go offline, the business could experience severe disruptions in daily functions, like processing transactions and supporting customer inquiries. Such downtime not only impacts revenue but can erode client trust and credibility. Implementing reliable security measures and contingency plans is, therefore, crucial to maintaining continuous and trustworthy business operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	• *Threat source sends automated, excessive requests to overwhelm the system's operating capabilities.* • *Threat source comprises a certificate authority to make their connections appear Legitimate.*	*3*	*2*	*6*
Software	*Threat source installs malicious software on organizational systems to locate and acquire sensitive information.*	*2*	*2*	*4*
Software	*Threat source installs software designed to collect (sniff) network traffic over a continued period of time.*	*2*	*2*	*4*

Approach

In this qualitative vulnerability assessment, I selected hackers, software vulnerabilities, and insider threats as the primary sources of risk. Hackers pose a significant risk due to their capability to exploit system weaknesses for unauthorized access, leading to potential data breaches and operational disruptions. Software vulnerabilities are also critical, as outdated or unpatched software can create exploitable entry points in the network, increasing the likelihood of security incidents. Finally, insider threats, whether intentional or accidental, represent a substantial risk, as employees with access to sensitive information can inadvertently or maliciously compromise data integrity. These risks are prioritized to safeguard business continuity and data security.

Remediation Strategy

To address the identified risks, implementing several layered security controls is essential. Applying the principle of least privilege will limit user access to only the resources necessary for their roles, reducing potential misuse or accidental exposure of sensitive data. Multi-factor authentication (MFA) adds an extra layer of security against unauthorized access by hackers, strengthening account protection against common credential attacks. Additionally, a Defense in Depth approach, combining firewalls, intrusion detection systems, and network segmentation, provides multiple barriers to protect against software vulnerabilities and insider threats. Lastly, using an Authentication, Authorization, and Accounting (AAA) framework will enable detailed tracking and control over access and actions, ensuring accountability and enhanced monitoring of user activities.