Portfolio piece #5. Analyze a vulnerable system for a small business

Purpose

The database server is crucial for the company's ability to analyze customer data and drive sales. However, since it has been open to the public since the company's launch, it's a high-value target for attackers. Unauthorized access or data loss could lead to a loss in reputation, legal issues, and financial losses. This assessment focuses on identifying and prioritizing the key threats to ensure business continuity and maintain customer trust.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	Obtain sensitive information via exfiltration	3	3	9
competitor	Conduct Denial of Service (DoS) attacks	2	2	6
APT	Install persistent and targeted network sniffers	3	2	6

Approach

The chosen threats, hackers, competitors, and APTs, pose realistic and significant risks to a public-facing database. Hackers are driven by the opportunity to steal customer data, while competitors might attempt to disrupt operations with DoS attacks. APTs are capable of sustained, stealthy attacks that could compromise both data integrity and confidentiality. These threats were selected based on their likelihood, and potential to make a negative impact the company's operations.

Remediation

To reduce the risk of unauthorized access, the company should immediately limit public access to the database and make sure only the right people can view data. Setting up multi-factor authentication (MFA) for all remote workers will add extra security. A layered security approach, with things like firewalls, monitoring systems, and regular checks, will help protect against data theft and ongoing threats. These actions will help address the biggest risks found in the assessment.