You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

You are tasked with completing a vulnerability assessment of the situation to communicate the potential risks to decision makers at the company. You must create a written report that explains how the vulnerable server is a risk to business operations and how it can be secured.

Vulnerability Assessment Report

3rd October 2024

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from July 2024 to September 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this assessment is to pinpoint the vulnerabilities related to the database server being used by the e-commerce company. The database server is valuable to the business because many employees work remotely and need the database server to perform their daily tasks. Since the database server has been open to the public for the last three years, from the company’s inception, the sensitive data contained within the server is extremely vulnerable to exploitation by a malicious actor. If the server ended up being disabled it would halt business, prevent employees from doing their daily tasks, and ultimately result in the company accruing financial loss and damage to their reputation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*. Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Advanced Persistent Threat (APT)	*. Perform reconnaissance and surveillance of organization* *. Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Malicious Software	*.Install persistent and targeted network sniffers on organizational information systems*	*3*	*3*	*9*

Approach

The central vulnerability is the fact that the database server is open to the public. This means that theoretically any user can access the database. The first threat source on the risk assessment list is a competitor. A competitor company can easily find useful company and customer data on the server, and use it to gain an advantage over our client company. This is only level 3 risk, just because company competitors are not presumed to be unethical. The second threat source provided is an APT. Now an APT is ethically flexible and will not hesitate to exploit this vulnerability. A database with public access is like heaven for an APT, because it can allow them to exfiltrate data and give them a foothold to gain C2 over the client companies entire system, potentially causing financial and reputational damage to the client company. This is why the risk level is a 9. The third threat source provided is malicious software, and was selected because an APT or hacker can easily install malicious software that will allow them to gain C2 and cause untold damage to the client company.

Remediation Strategy

Limit access to the database server by implementing the Principle of Least Privilege, so that only certain employees who need access to the server to complete their tasks have access to it. Additionally, the Authentication, Authorization, Accounting (AAA) framework should be implemented to ensure that only certain employees are able to access the server. Multi Factor Authentication can be incorporated into this, as well as SSO and password management policies. All of these will significantly decrease the risk of threat actors exploiting the server.