**Portfolio Activity: Analyze a vulnerable system for a small business**

**Scenario Details:** 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. 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.

Vulnerability Assessment Using NIST SP 800-30

Scenario Snap Shot:

An e-commerce company stores information on a remote database server that has been open to the public since the company's launch three years ago. Employees of the company regularly query the server to find potential customers.

**My Research and Thoughts:**

Assessment:

The fact that the database server is open to the public is a serious vulnerability. This means that anyone with an internet connection can access the server and potentially steal or manipulate the data it contains. This could have a devastating impact on the company's business operations, including:

* Financial losses due to data theft or fraud
* Loss of customer trust and reputation
* Compliance violations and regulatory fines
* Disruption of business operations due to ransomware attacks or other malicious activity

In addition, the server hardware and operating system are relatively powerful, which makes it a more attractive target for attackers.

Recommendations:

To mitigate these risks, the company should take the following steps:

* Close the database server to the public and restrict access to authorized personnel only.
* Implement strong authentication and authorization controls to prevent unauthorized access to the server.
* Regularly patch and update the server hardware and operating system to address known vulnerabilities.
* Implement a firewall and other network security controls to protect the server from unauthorized access and attack.
* Monitor the server for suspicious activity and respond promptly to any incidents that are detected.

Conclusion:

Leaving the database server open to the public is a serious vulnerability that poses a significant risk to the company's business operations. By taking the recommended steps to secure the server, the company can mitigate these risks and protect its data and customers.

Additional Considerations:

The company may also want to consider the following additional recommendations:

* Implement a data loss prevention (DLP) solution to prevent sensitive data from being exfiltrated from the server.
* Conduct regular security audits of the server to identify and address any vulnerabilities.
* Develop a security awareness training program for employees to educate them about cyber threats and best practices for protecting data.

Written Report:

The following is a sample written report that can be used to communicate the potential risks and recommendations to decision makers at the company:

Vulnerability Assessment Report

Date: 2023-10-04

To: Decision Makers

From: Cybersecurity Analyst

Subject: Vulnerability Assessment of Database Server

**Executive Summary:**

This report documents the results of a vulnerability assessment of the database server that stores information on customer leads and other sensitive data. The assessment found that the server is open to the public, which poses a significant risk to the company's business operations.

**The scope of the vulnerability assessment should include the following:**

* Server hardware: The vulnerability assessment should identify any vulnerabilities in the server hardware, such as firmware updates or known security flaws.
* Operating system: The vulnerability assessment should identify any vulnerabilities in the server operating system, such as outdated security patches or known security flaws.
* Database management system: The vulnerability assessment should identify any vulnerabilities in the database management system (DBMS), such as outdated security patches or known security flaws.
* Web applications: If the server hosts any web applications, the vulnerability assessment should also include these applications.
* Network configuration: The vulnerability assessment should also include the server's network configuration to identify any potential security risks.

In addition to these technical areas, the vulnerability assessment should also consider the following:

* Security policies and procedures: The vulnerability assessment should review the company's security policies and procedures to identify any areas where they may be lacking or outdated.
* Employee training: The vulnerability assessment should also assess the level of security awareness among employees and identify any areas where additional training is needed.

By taking a comprehensive approach to the vulnerability assessment, the company can identify and address all of the potential security risks associated with the database server.

Here are some additional things to consider when determining the scope of the vulnerability assessment:

* The company's industry and the type of data that is stored on the server.
* The company's budget and resources.
* The company's risk tolerance.
* The company's regulatory requirements.

Once the scope of the vulnerability assessment has been determined, the company can develop a plan to execute the assessment and address any vulnerabilities that are identified.

**The threat sources for the scenario include:**

* External attackers: These could be cybercriminals, hackers, or nation-states who are motivated by financial gain, espionage, or disruption.
* Malicious insiders: These could be employees, contractors, or other authorized users who abuse their access to the server for malicious purposes.
* Negligent insiders: These could be employees, contractors, or other authorized users who make unintentional mistakes that could lead to a security breach.
* Technical vulnerabilities: These are weaknesses in the server hardware, operating system, or software that could be exploited by attackers.

In addition to these general threat sources, there are some specific threats that could be relevant to the scenario you described, such as:

* SQL injection attacks: These attacks exploit vulnerabilities in database management systems to steal or manipulate data.
* Cross-site scripting (XSS) attacks: These attacks inject malicious code into web pages, which can then be executed by unsuspecting visitors.
* Denial-of-service (DoS) attacks: These attacks overwhelm the server with traffic, making it unavailable to authorized users.
* Ransomware attacks: These attacks encrypt the server's data and demand a ransom payment in exchange for the decryption key.

It is important to note that this is not an exhaustive list of all possible threat sources. New threats are emerging all the time, so it is important to stay informed about the latest cyber security risks and implement appropriate mitigation measures.

To further mitigate the risks, the company should also consider developing a security incident response plan (SIRP). This plan should outline the steps to be taken in the event of a security breach, including how to identify and contain the incident, restore affected systems, and communicate with customers and other stakeholders.

**Possible threat events that could occur if the database server is not properly secured:**

* Data theft: Attackers could steal customer data, such as names, addresses, credit card numbers, and Social Security numbers. This data could then be used for fraudulent purposes, such as identity theft or credit card fraud.
* Data manipulation: Attackers could modify or delete customer data. This could disrupt the company's operations and damage its reputation.
* Ransomware attack: Attackers could encrypt the server's data and demand a ransom payment in exchange for the decryption key. This could cause significant financial losses and disruption to the company's business.
* Denial-of-service attack: Attackers could overwhelm the server with traffic, making it unavailable to authorized users. This could disrupt the company's operations and cost it revenue.
* Malware infection: Attackers could infect the server with malware, such as viruses or trojans. This malware could steal data, damage the server, or disrupt the company's operations.

In addition to these specific threat events, there is also the general risk of reputational damage and financial losses that could result from a security breach. If the company's customers lose trust in its ability to protect their data, they may take their business elsewhere. The company may also face regulatory fines and other legal costs as a result of a security breach.

It is important to note that this is not an exhaustive list of all possible threat events. New threats are emerging all the time, so it is important to stay informed about the latest cyber security risks and implement appropriate mitigation measures.

**The likelihood of the threat events** described in the previous response can vary depending on a number of factors, such as the company's industry, size, and security posture. However, in general, the following can be said:

Qualitative values:

* Data theft: High
* Data manipulation: High
* Ransomware attack: Medium to high
* Denial-of-service attack: Medium
* Malware infection: High

Quantitative values:

* Data theft: According to the IBM Cost of a Data Breach Report 2023, the average cost of a data breach is $4.35 million. This suggests that the likelihood of a data breach is high, as the potential rewards for attackers are significant.
* Data manipulation: The likelihood of data manipulation is also high, as it is a relatively easy attack to carry out. For example, an attacker could simply delete all of the data on the server, causing significant disruption to the company's operations.
* Ransomware attack: The likelihood of a ransomware attack is medium to high, as ransomware is one of the most common types of cyber attack today. In 2022, there were over 300 million ransomware attacks worldwide.
* Denial-of-service attack: The likelihood of a denial-of-service attack is medium, as it is a relatively common type of cyber attack. However, it is important to note that denial-of-service attacks can be very costly for businesses, as they can cause significant disruption to operations.
* Malware infection: The likelihood of a malware infection is high, as there are many different types of malware in circulation and new malware is being developed all the time.

It is important to note that these are just general estimates. The actual likelihood of a particular threat event will vary depending on the specific circumstances of the company.

To reduce the likelihood of these threat events occurring, the company should implement a comprehensive security program that includes measures such as:

* Vulnerability management: Regularly scan the server for vulnerabilities and patch them promptly.
* Access control: Implement strong authentication and authorization controls to restrict access to the server to authorized personnel only.
* Network security: Implement a firewall and other network security controls to protect the server from unauthorized access and attack.
* Security monitoring: Monitor the server for suspicious activity and respond promptly to any incidents that are detected.
* Security awareness training: Educate employees about cyber threats and best practices for protecting data.

By implementing these measures, the company can significantly reduce the likelihood of a security breach and protect its data and customers.

The severity of the threat events described in the previous response can vary depending on a number of factors, such as the company's industry, size, and customer base. However, in general, the following can be said:

Qualitative values:

Data theft: High

Data manipulation: High

Ransomware attack: High

Denial-of-service attack: Medium to high

Malware infection: Medium to high

Quantitative values:

Data theft: The average cost of a data breach is $4.35 million, according to the IBM Cost of a Data Breach Report 2023. This suggests that the severity of a data breach is high, as the potential financial losses for the company can be significant.

Data manipulation: The severity of data manipulation can also be high, as it can disrupt the company's operations, damage its reputation, and lead to financial losses. For example, if an attacker deletes all of the data on the server, the company may need to shut down its operations for an extended period of time to restore the data.

Ransomware attack: The severity of a ransomware attack can also be high, as it can disrupt the company's operations and cause financial losses. The company may need to pay the ransom to get the decryption key, or it may need to invest significant resources to restore its data from backups.

Denial-of-service attack: The severity of a denial-of-service attack can vary depending on the duration and impact of the attack. A short-lived denial-of-service attack may only cause minor disruption to the company's operations, but a prolonged attack can have a significant impact on revenue and customer satisfaction.

Malware infection: The severity of a malware infection can also vary depending on the type of malware and the impact that it has on the company's systems. For example, a virus that encrypts the company's data can have a significant impact on operations, while a worm that spreads to other computers on the network may cause only minor disruption.

**It is important to note** that these are just general estimates. The actual severity of a particular threat event will vary depending on the specific circumstances of the company.

**To mitigate the severity of these threat events,** the company should implement a comprehensive security program that includes measures such as:

1. Data backup and recovery: Implement a robust data backup and recovery plan so that the company can quickly restore its data in the event of a data breach or ransomware attack.

2. Business continuity planning: Develop a business continuity plan so that the company can continue to operate in the event of a major disruption, such as a denial-of-service attack or malware infection.

3. Incident response planning: Develop an incident response plan so that the company can quickly and effectively respond to a security breach or other incident.

4. Security awareness training: Educate employees about cyber threats and best practices for protecting data.

By implementing these measures, the company can reduce the severity of the impact of a security breach or other incident.

Findings:

The database server is open to the public, which means that anyone with an internet connection can access it. This is a serious vulnerability that could allow attackers to steal or manipulate the data on the server. In addition, the server hardware and operating system are relatively powerful, which makes it a more attractive target for attackers.

Recommendations:

To mitigate the risks identified in this assessment, the company should:

* Close the database server to the public and restrict access to authorized personnel only.
* Implement strong authentication and authorization controls to prevent unauthorized access to the server.
* Regularly patch and update the server hardware and operating system to address known vulnerabilities.
* Implement a firewall and other network security controls to protect the server from unauthorized access and attack.
* Monitor the server for suspicious activity and respond promptly to any incidents that are detected.

Conclusion:

By taking the recommended steps to secure the database server, the company can mitigate the risks identified in this assessment and protect its data and customers.

Additional Recommendations:

The company may also want to consider the following additional recommendations:

* Implement a DLP solution to prevent sensitive data from being exfiltrated from the server.
* Conduct regular security audits of the server to identify and address any vulnerabilities.
* Develop a security awareness training program for employees to educate them about cyber threats and best practices for protecting data.

I urge you to take the findings and recommendations in this report seriously. The security of the database server is essential to the company's success.