## Activity: Analyze a vulnerable system for a small business

**Activity Overview**

In this activity, you will conduct a vulnerability assessment for a small business. You will  evaluate the risks of a vulnerable information system and outline a remediation plan

A vulnerability assessment is the internal review process of an organization’s security systems. As a cybersecurity analyst, you might help with vulnerability assessments to prevent attacks in an organization. Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

**Scenario**

Review the following scenario. Then complete the step-by-step instructions.

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.

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

**Step-By-Step Instructions**

Follow the instructions to complete each step of the activity. Then, answer the 5 questions at the end of the activity before going to the next course item to compare your work to a completed exemplar.

**Part 1 - Open a report template**

**Step 1: Access the template**

Using a pre-formatted template can be a helpful starting point when constructing a written report. By providing pre-made layouts and headings, templates can provide a professional appearance.

**Vulnerability Assessment Report**

**1st January 20XX**

# 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 June 2023 to August 2023. [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

Consider the following questions to help you write:

* *How is the database server valuable to the business?*
* *Why is it important for the business to secure the data on the server?*
* *How might the server impact the business if it were disabled?*

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
|  |  |  |  |  |
|  |  |  |  |  |

# Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

# Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.

## **Step 2: Access supporting materials**

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps. You will use this resource in Part 2 of this activity.

To use the supporting materials for this course item, click the link and select Use Template.

## NIST SP 800-30 Rev. 1

## 

### **Guide to assessing risk**

NIST SP 800-30 is a publication that provides guidance on performing risk assessments. It outlines strategies for identifying, analyzing, and remediating risks. Organizations use NIST SP 800-30 to gain insights into the potential likelihood and severity of risks—helping them make informed decisions about allocating resources, implementing controls, and prioritizing remediation efforts.

This four page document is adapted from NIST SP 800-30 Rev. 1. The term "Rev. 1" signifies that it is the first updated version of this publication. NIST occasionally revises its documents to incorporate new information, reflect changes in technology and regulatory requirements, or address feedback.

**Note:** NIST's [Computer Security Resources Center](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final) contains more information on SP 800-30 Rev. 1.

### **Threat sources**

NIST SP 800-30 defines and categorizes threat sources as entities or circumstances that can negatively impact an organization's information systems. This information is useful for identifying and assessing potential risks. When referencing it, consider the intent/capabilities of either internal and external threat sources.

**Note:** The following table lists a few possible *threat sources* that could compromise a publicly accessible database server.

|  |  |  |
| --- | --- | --- |
| **Type** | **Examples** | **Description** |
| **Human** | *Standard user*   * Employee * Customer   *Privileged user*   * System administrator   *Group*   * *C*ompetitor * Supplier * Business partner * Nation state   *Outsider*   * Hacker * Hacktivist * Advanced persistent threat (APT) | Threats arising from individuals or groups who might purposefully or accidentally exploit cyber resources. For example, they might alter data in a way that negatively impacts the company. Alternatively, they might intentionally steal data and damage business equipment. |
| **Technological** | *Hardware*   * Storage * Processing * Communications   *Software*   * *O*perating system(s) * Networking * Malicious software | Threats that originate from non-human factors. For example, failures of equipment due to aging, resource depletion, or other circumstances. |
| **Environmental** | *Operational environment*   * Temperature controls * Humidity controls * Faulty power supplies   *Natural hazards*   * Power outages * Extreme weather events | Threats that arise from accidental, non-human factors. For example, equipment failures caused by the operational environment. |

### **Threat events**

NIST SP 800-30 defines and categorizes threat events as actual instances where a threat source exploits a vulnerability and causes damage or harm to an organization's information systems. This information is useful for gaining insights into the types of risks that assets face. More effective controls and countermeasures can be identified by understanding possible threat events,

**Note:** The following table lists just a few possible *threat events* that could compromise a publicly accessible database server.

|  |  |
| --- | --- |
| **Examples** | **Description** |
| Perform reconnaissance and surveillance of organization | Threat source examines and assesses the company's vulnerabilities over time using various tools (e.g., scanning, physical observation). |
| Obtain sensitive information via exfiltration | Threat source installs malicious software on organizational systems to locate and acquire sensitive information. |
| Alter/Delete critical information | Threat source alters or deletes data that is critical to day-to-day business operations. |
| Craft counterfeit certificates. | Threat source compromises a certificate authority to make their connections appear legitimate. |
| Install persistent and targeted network sniffers on organizational information systems. | Threat source installs software designed to collect (sniff) network traffic over a continued period of time. |
| Conduct Denial of Service (DoS) attacks. | Threat source sends automated, excessive requests to overwhelm the system's operating capabilities. |
| Disrupt mission-critical operations. | Threat source compromises the integrity of information in such a way that prevents the business from carrying out critical operations. |
| Obfuscate future attacks. | Threat source takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities at the company. |
| Conduct "man-in-the-middle" attacks. | Threat source eavesdrops on sessions between internal and external systems. Later, they relay messages between organizational and external systems that make them believe they're talking directly to each other over a private connection. |

## Likelihood of a threat event

In general, the *likelihood* of a threat event should be a score based on a combination of factors. For example, any available evidence that you have, prior experience, and your expert judgment.

Consider the intent/capabilities of a threat source and potential threat events when producing a likelihood score.

|  |  |  |
| --- | --- | --- |
| **Qualitative values** | **Quantitative values** | **Description** |
| High | 3 | Threat source is almost certain to initiate a security event. An event could have multiple, severe, or catastrophic effects on business operations and assets. |
| Moderate | 2 | Threat source is somewhat likely to initiate a security event. An event could significantly reduce the functionality of organizational operations and assets. |
| Low | 1 | Threat source is highly unlikely to initiate a security event. An event could have minor, negligible effects on business operations and assets. |

## Severity of a threat event

In general, the *severity* of a threat event is a measure of its potential impact to business operations. For example, would the event cause a business function to stop entirely? Might it temporarily disrupt a business process and go unnoticed?

Consider the business impact of *threat events* when producing a severity score.

|  |  |  |
| --- | --- | --- |
| **Qualitative values** | **Quantitative values** | **Description** |
| High | 3 | Threat source is almost certain to initiate a security event. An event could have multiple, severe, or catastrophic effects on business operations and assets. |
| Moderate | 2 | Threat source is somewhat likely to initiate a security event. An event could significantly reduce the functionality of organizational operations and assets. |
| Low | 1 | Threat source is highly unlikely to initiate a security event. An event could have minor, negligible effects on business operations and assets. |

### **Step 3: Review information about the vulnerable server**

Vulnerability assessments typically include a description of the system being evaluated and the scope of the project.

Review the **System Description** and **Scope** of the Vulnerability assessment report.

The **System Description** highlights the relevant components, architecture, and dependencies of the system being assessed. All of these parts and connections make up the attack surface of the vulnerable information system.

The **Scope** specifies the focus and boundaries of the assessment. For example, you might specify that the scope of this assessment only relates to the confidentiality, availability, and integrity of the data on the server—not the physical security of the server or its related IT systems.

## Part 2 - Perform a risk assessment

### **Step 1: Explain the purpose of the information system**

### **Step 2: Identify potential threat sources**

### **Step 3: Identify potential threat events**

### **Step 4: Calculate the risk of potential threats**

## Part 3 - Propose security recommendations

### **Step 1: Explain your approach**

### **Step 2: Propose a remediation strategy**

3-5 sentences describing the reasons for conducting the security analysis in the **Purpose**

section

A completed **Risk Assessment** section

3-5 sentences explaining your reasoning for the identified risks in the **Approach** section

3-5 sentences summarizing a *remediation* and/or *mitigation* strategy in the **Remediation** section

## Perform a risk assessment

Step 1: The purpose of the information system is critical for the e-commerce company's daily operations. The database server serves as the backbone of their business, housing valuable customer data and transaction records. Securing this system is paramount to ensure the confidentiality, integrity, and availability of this information. Any breach or disruption of the server's functionality could lead to data leaks, financial losses, reputational damage, and ultimately, the inability to serve their customers effectively.

Step 2: Potential threat sources for the publicly accessible database server include standard users, privileged users, and outsiders. Standard users, such as employees and customers, could accidentally or intentionally exploit vulnerabilities. Privileged users, like system administrators, pose risks due to their elevated access levels. Outsiders, including hackers and advanced persistent threats, may purposefully target the system to steal data, disrupt operations, or compromise the integrity of the database.

Step 3: Various potential threat events could compromise the security of the database server. These events encompass actions like reconnaissance and surveillance to identify vulnerabilities, data exfiltration to steal sensitive information, data alteration or deletion that can disrupt business operations, and denial of service (DoS) attacks to overwhelm the system's capabilities. Threat sources might also employ tactics like installing network sniffers, conducting "man-in-the-middle" attacks, crafting counterfeit certificates, and obfuscating future attacks to further their objectives.

Step 4: To calculate the risk of potential threats, we need to consider both the likelihood and severity of each threat event. Likelihood can be rated on a scale of High, Moderate, or Low, based on factors like intent, capability of threat sources, and historical evidence. Similarly, severity can be rated as High, Moderate, or Low based on the potential impact on business operations and assets. By combining these ratings, we can assess the risk associated with each threat event, providing a comprehensive understanding of the security landscape.

## Propose security recommendations

Step 1: The identified risks are based on a thorough assessment of the data storage and management methods of the business. Risks were evaluated by considering the likelihood of threat occurrences and their potential impact on day-to-day operational needs. The risks are significant as they include the compromise of customer data, disruption of operations, financial losses, and damage to the company's reputation. Additionally, the system's public accessibility has made it a prime target for malicious actors, underscoring the urgency of addressing these vulnerabilities.

Step 2: The remediation and mitigation strategy involves implementing several security measures to safeguard the database server. This includes the introduction of authentication, authorization, and auditing mechanisms to restrict access to authorized users, usage of strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. The transition from SSL to TLS encryption for data in motion enhances security. Moreover, IP allow-listing to corporate offices is recommended to prevent random internet users from connecting to the database, reducing the attack surface, and enhancing overall system security. These measures collectively aim to minimize the identified risks and fortify the security posture of the organization.

Top of Form

Bottom of Form