(Mock) Vulnerability Assessment Report for Leadership

A person touching a screen with a glowing lock

Description automatically generated

Material & instructions developed by: Google Cybersecurity Professional Certificate Course

Completed by: Alexander Herman on 01/29/24

**Table of Contents:**

Scenario (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Step-By-Step Instructions (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Vulnerability Assessment Report (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Risk Assessment (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**3**

Approach (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**3**

Remediation Strategy (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**3-4**

**Scenario**

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**

1. **Review information about the vulnerable server**
2. **Perform a risk assessment**

* identify potential threat sources
* identify potential threat events
* calculate the risk of potential threats

1. **Propose security recommendations**

* explain your approach
* propose a remediation strategy

**Vulnerability Assessment Report**

**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 20XX to August 20XX. NIST SP

800-30 Rev. 1 is used to guide the risk analysis of the information system.

**Purpose**

The database server is a centralized computer system that stores and manages large amounts

of data. The server is used to store customer, campaign, and analytic data that can later be

analyzed to track performance and personalize marketing efforts. It is critical to secure the

system because of its regular use for marketing operations.

**Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat Source** | **Threat Event** | **Likelihood** | **Severity** | **Risk Grade** |
| Competitor | Gather information using open-source discovery of organizational information | 3 | 3 | 9 |
| Hacker | Obtain sensitive information via exfiltration | 2 | 3 | 6 |
| Hacker | Craft counterfeit certificates | 1 | 3 | 3 |
| Hacker | Conduct "man-in-the-middle" attacks | 2 | 3 | 6 |
| Hacker | Install persistent and targeted network sniffers  on organizational information systems | 1 | 2 | 2 |
| Hacker | Conduct Denial of Service (DoS) attacks | 3 | 3 | 9 |
| Hacker | Obfuscate future attacks | 1 | 3 | 3 |
| Networking | Disrupt mission-critical operations | 2 | 3 | 6 |
| (Accidental) Employee | Alter/Delete critical information | 2 | 2 | 4 |
| (Accidental) Customer | Alter/Delete critical information | 2 | 1 | 2 |
| Malicious Software | Disrupt mission-critical operations | 2 | 3 | 6 |

**Approach**

Because this risk assessment is meant to inform leadership, I took a threat-oriented, qualitative approach when creating this report. The vulnerability identified as a publicly accessible database, is of serious concern and leadership needs to be aware of the threat sources and threat events the vulnerability exposes the company to. Because the database has open access permissions, and it is connected with other servers, devices, and systems on the company network, there are a multitude of threat sources and events to consider. The threat events identified above were weighed based on their likelihood of occurrence and the severity of their potential impact. The two biggest threats identified, that are both highly likely and highly serious, would exploit our current vulnerability are: a competitor getting access to proprietary company information on ‘potential customers’ via open-source discovery, and additionally, a threat actor (hacker) executing a Denial-of-Service Attack on our company network through the externally accessible server that could cause significant disruptions to business-critical operations.

**Remediation Strategy**

1. **Secure the sever storing the ‘potential customer’ database**

* install a properly configured firewall or bring the server behind the company’s network firewall
* employ a VPN service for employees that are connecting to the company network remotely
* ensure law of least privileges regarding who gets access and how much access
* enable MFA for privileged accounts (should enable for all accounts with any access level)
* use TLS encryption for data in transit as opposed to SSL and ensure stored data is encrypted

1. **Establish active and passive monitoring**

* consider installing IDS, IPS, and SIEM services
* establish regular vulnerability assessments, pen-testing, and log audits

1. **Create an employee training & awareness program**

* have regular lessons to keep employees up to date on threats
* train employees how to handle the data and systems they interact with