**Vulnerability Assessment Report**

**1st May 2024**

# **System Description**

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version a of red hat Linux operating system as of May 2024 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 will only consider the threat to the confidentiality, integrity, and accessibility of the data, and not any kind of physical threat to the server. The guidelines within NIST SP 800-30 Rev. 1 will be used for the risk analysis below.

# **Purpose**

The database server contains all gathered information from the business employees and other sources about potential customers. That includes PII about a lot of people, as well as campaign and analytical data needed for A/B testing, conversion optimization, and a more targeted marketing campaign needed to boost the bottom line. Without access to an uncorrupted server, it becomes difficult to conduct business operations.

It is important to secure the information stored on that server since as it is PII, the company will become legally liable as data custodian if there is any data breach or exposure – as well as a loss of reputation for the business. There is also the risk that a competitor might try to steal information since it a public database, or otherwise might try to block access to the server for company’s employees. E-commerce is a fast-changing business.

If the server is disabled, the e-commerce company might be put of business since it cannot access valuable data relating to future sales (and future revenue).

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Competitor* | *Denial of service attack* | *2* | *2* | *4* |
| *Business employees* | *Exposure of PII (accidental)* | *2* | *3* | *6* |
| *Customer* | *Access and change information in the database on their own accord* | *1* | *3* | *3* |

# **Approach**

It is a publicly accessible database, and the business world of e-commerce can be fierce. From the looks of it - with employees all over the world - this e-commerce will have some powerful competitors. Some of which might be tempted to use unethical means to “get a leg up” or if not make sure that this business “get it’s leg down”.

Many business employees have a weak understanding of safety measures, and exposures can happen easily - in moments of excitement after many moments of minutiae. The consequences of which can be great.

The attack surface in this case has to do with the data storage and management procedures, and the potential threat actors could come both from outside the business and within. It is accessible to everyone in the world that looks for it, so that could be customers as well. There will be an estimate of the likelihood for that threat event, and the consequence for business operations should that happen.

The limitation of this assessment is that does not include physical threats against the servers such as earthquakes, volcano eruptions etc.

# **Remediation Strategy**

I recommend implementing in no particular order:

* A public key system (PKI) to address the threat of competitors obtaining sensitive information.
* The enforcement of strong passwords and multi-factor authentication to ensure that only authorized user could gain access to the server.
* Role based authorization to the employees according to the principle of least privilege, to minimize the effect of any accidental leakage of data.
* The construction of defense in depth by firewalls and IPS. Set the firewall to only allow specific IP addresses from the specific offices of the relevant employees. That should prevent random users accessing the database.