**Vulnerability Assessment Report**

**20th May 2024**

# **Risk Assessment**

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| **System Administrator** | **Demonstrates ill-willed recon on internal systems over a duration of time via utilizing strategic tools like spyware with the intent to identify potential system vulnerabilities to exploit.** | **2** | **2** | **4** |
| **Hacker** | **Compromises everyday business operations via utilizing malware, to manipulating the integrity of the bank's organizational data within their IT systems.** | **2** | **3** | **6** |
| **Storage** | **128gb storage limitations facilitating banking server leaves the company's IT systems vulnerable to potential server overload via (DdoS) attacks as well as operational or service inefficiencies.** | **3** | **3** | **9** |

# **Risk Analysis**

* The logic driving my decision for choosing these vulnerabilities stems from their relative levels of organizational risk, since the company would face severe regulatory, ethical and legal consequences if they were exploited by potential threats. Specifically, if the organization's DBMS remains available to the public, it is certain that its DBMS would lie helpless to black hat perpetrators seeking to use ransomware as well as any person's that could have potential access to its systems like third party suppliers or business affiliates who would most likely require authenticated data queries. Notably, organizational insiders like disgruntled system admins. may also pose a potential risk to the server's weak security framework via exploiting its underdeveloped security controls via leveraging spyware in order to determine potential system weaknesses over time. Additionally, the other blatant server vulnerability that stuck out to me like a proverbial sore thumb was the miniscule storage capabilities of its server’s DBMS, since a meer 128 GBs of storage would not be enough to satisfy the processes of all of its bank server's network traffic, resource operations, data or system requirements. Thus, the lack of optimal system storage could lead to their employees and customers being faced with poor service performances, dysfunctional system operations as well as complete system or server shutdowns from DDoS or disruptive malware attacks.. Imperatively, the fact that the organization's server's DB has been open to the public for data queries is a cause of concern, since the system is insecurely exposed to an array of different attack vectors via a diversity of surface area exposures. Nevertheless, it's worth noting that my vulnerability assessment was limited to the relative scope and security standards set forth by the NIST SP 800-30 Rev. 1, but I recommend conducting the necessary pen tests to explore these vulnerabilities as well as their risk in more depth in order to respond with informed remediation solutions.
* **Remediation Strategy**

Currently, the company has technical security controls in place like encoded data formats via encryption software, which will deter looming perpetrators and threat actors from eavesdropping on or intercepting their data in transit, at rest and in operation throughout the DAL. However, the company lacks operational security controls such as vital server traffic and network configurations that are necessary for their organization to create additional layers of security protections. These configurations would help their security team with delegating appropriate service authentications as well as file or resource access permissions, to remote personnel based on their job requirements or customers who ought to be deemed rightful access. Mainly, making sure that the company's server and its banking services or systems are conscientiously configured with the right security mechanisms will help the company automate many security functions that help deter potential threat events. Furthermore, I believe the company should implement managerial security controls like regular automations for password updates as well as user permission checks in order to ensure that an employee who have potentially undergone a team transition or role change do not retain the same user permissions attached to their previous responsibilities and are only ever granted the system permissions required to carry out their immediate tasks. Considering the vulnerabilities associated with the risks discussed, I would suggest that the organization's security team still conducts an additional vulnerability check internally, while keeping the guidelines of the NIST SP 800-30 Rev. 1 in mind in order to identify any potentially overlooked security gaps and to further align with their relative industries security standards, DM practices and applicable data privacy regulations to achieve a stronger security posture that complies accordingly. Nevertheless, I would start the remediation process by upgrading the storage capacity of its system's hardware in order to be able to safely scale the heavy volume of user traffic, for which is technically vital in order for the organization's integral server, DB and IT systems to be able to operate correctly as well as function at an optimal performance for both customer and employee interaction. Additionally, I would also recommend conducting regular user permission and operation audits in order to ensure that the company’s security management team is following as well as integrating the principles of least privilege and separation of duties within its security policies, plans or systems in order to deter the possible occurrence of an internal threat event from taking place. Basically, this would allow the e-commerce companies security team to limit what employees have access to what systems, data or services and how exactly they are able to utilize them, so that asset theft, misuse or exploitation would be more difficult to transpire. Moreover, implementing operational security controls like circuit layer proxy firewalls, to filter illegitimate TCP/IP handshake attempts from unknown sources can prevent malicious threat actors or hackers from gaining access to their server or making their way past their security defenses to harm their organizational systems and from potentially compromising their organizational data. Ultimately, making the following adjustments and control additions to their organizational security plan or framework will help the organization drastically strengthen their overall security posture as well as will create a more safely optimal banking environment for all organizational stakeholders.