Coop. Agricola Mixta Montecarlo Ltda. 2024-09-26 #1 Vulnerability Assessment

Scenery

The coop stores information on a remote database server, as many of the employees work remotely and/or from locations throughout the province. Company employees regularly query, or request, data from the server to find potential customers.

The database has been open to the public since the coop's digitalization fourteen years ago. As a cybersecurity professional, it is recognized that keeping the database server open to the public is a serious vulnerability.

I was tasked with completing a vulnerability assessment of the situation to communicate potential risks to decision makers in the co-op.

A written report will be created explaining how the vulnerable server poses a risk to the coop's operations and how it can be secured.

System Description

The server hardware consists of 4 Dell PowerEdge™ 2950 III 2S rack servers, EA with 8 fully buffered DIMM slots for a total of up to 64GB RAM, two quad-core Intel® Xeon® processors, and a variety of network interface options, plus configurable embedded hypervisors between VMware®, Citrix®, and Microsoft®.

They run on the latest version of the CentOS Linux server operating system and host a MySQL database management system. They are configured with a stable network connection using IPv4 addresses and interact 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 evaluation will cover a three-month period, from July 2024 to September 2024.

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 information system risk analysis.

Purpose

Questions that complement the evaluation decision:

What value does the database server have for the coop?

Why is it important for the coop to protect data on the server?

How would the server affect coop if it was disabled?

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 analytics data that can then be analyzed to track performance and personalize marketing initiatives.

It is essential to protect the system due to its frequent use for marketing operations.

risk assessment

| **Source of the Threat** | **Threat Event** | **Probability** | **Gravity** | **Risk** |
| --- | --- | --- | --- | --- |
| Hacker | Obtaining sensitive information via exfiltration | 3 | 3 | 9 |
| Employee | Disrupt mission-critical operations | 2 | 3 | 6 |
| Customer | Modify/delete critical information | 1 | 3 | 3 |

Approach

The risks were measured considering the coop's data storage and management methods.

Potential threat sources and events were determined using the probability of a security incident given the open access permissions of the information system.

The severity of potential incidents was assessed against the impact on daily operational needs.

Remediation strategy

Implementing authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes the use of strong passwords, role-based access controls, and multi-factor authentication to limit user privileges.

Encryption of data in motion using TLS instead of SSL.

List of allowed IP addresses in the cooperative's offices and other facilities to prevent random Internet users from connecting to the database.