Security Risk Assessment 2024-05-16 #1

GL Gráfica - San Lorenzo 3176 Eldorado

Report Overview

The situation will be analyzed using the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The CSF is a voluntary framework consisting of standards, guidelines, and best practices for managing cybersecurity risk.

A security risk assessment report will be created to demonstrate a proactive approach to security, improve communication and transparency with stakeholders, and enhance security practices within the organization.

It will identify which security measures should be implemented in response to business needs and determine what are the best options available with regards to network security.

Context

A security risk assessment report was conducted as an external cybersecurity analyst for the company GL Gráfica, which offers web design, graphic design, and social media marketing solutions to small businesses.

The organization has previously suffered a data breach, which has compromised the security of its customers' personal information, such as names and addresses.

The organization wants to implement robust network hardening practices that can be carried out consistently to prevent attacks and breaches in the future.

As an analyst, while inspecting the organization's network, I discovered four major vulnerabilities.

The four vulnerabilities are as follows:

1. Employees within the organization share passwords.
2. The database administrator password is set by default.
3. Firewalls do not have rules in place to filter traffic entering and leaving the network.
4. Multi-factor authentication (MFA) is not used.

If steps are not taken to address these vulnerabilities, the organization is at risk of another data breach or other attacks in the future.

| **Hardening tools and methods to implement** | |
| --- | --- |
| Three hardening tools that the organization can use to address the vulnerabilities found include:   1. Implementing multi-factor authentication (MFA) 2. Establish and enforce strong password policies 3. Perform firewall maintenance periodically   MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, PIN numbers, and passwords.  Password policies can be refined to include rules about password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules surrounding failed login attempts, such as the user losing network access after five failed attempts.  Firewall maintenance involves checking and updating security settings periodically to stay ahead of potential threats. | |
|

| **Recommendations** |
| --- |
| Enforcing multi-factor authentication (MFA) adds an additional layer of security beyond a password. It will reduce the likelihood that a malicious actor can access a network through a brute-force or related attack, as additional effort is required to authenticate in more than one way. MFA can also reduce the likelihood of people sharing passwords. Since the recipient of the shared password would need to possess additional authentication beyond a password, MFA makes it less useful to share passwords, making them less likely to be shared.  Creating and enforcing a password policy within the company will make it increasingly difficult for malicious actors to gain access to the network. Policies such as suspending the account after a certain number of logins can prevent successful brute force attacks. Increasing password complexity, requiring passwords to be updated more frequently, and not allowing password reuse also help prevent malicious actors from infiltrating the network.  Firewall maintenance should be performed regularly. Network administrators should ensure that firewall rules are in place that reflect the most up-to-date standards for allowed and denied traffic. Traffic from suspicious sources should be included in a deny traffic list. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can be used to protect against a variety of DoS and DDoS attacks. |