INCIDENT REPORT | 004 | NETWORK HARDENING

DETAILS

Cause: Data Breach

Analysis

The organization's employees' share passwords.

Company policies need to be addressed regarding sharing passwords. This is completely unsafe and creates a vulnerability.

The admin password for the database is set to the default.

The administrative password should not be set to default. A reminder of company policies regarding password security will be mentioned during formal tech training.

Password creativity and combinations will be addressed as well, adding an extra layer so security to account protection.

The firewalls do not have rules in place to filter traffic coming in and out of the network.

Firewall filter rules need to be tailored for heavily monitoring traffic coming in and out of the website service. This creates the ability to manage access to the webpage via targeting specific IPs within admin panels as well.

Multi-factor authentication (MFA) is not used.

Formal training will need to be implemented in order for employees to understand the benefits of Multi-factor authentication (MFA). Instruction will be given on how to access and complete setting up an account's MFA for added security.