Cybersecurity Incident Report

Summary of the Problem
A major data breach was caused by undetected vulnerabilities. This breach compromised personal information like names and addresses. After inspecting the Organization's network, the following vulnerabilities were found: ● The organization’s employees share passwords ● The admin password for the database is set to the default ● The firewalls do not have rules in place to filter traffic coming in and out of the network ● Multi-Factor authentication (MFA) is not used

Analysis
The following hardening tools should be implemented: ● Configuration checks- These are used to update the encryption standard that is stored. Usually you can use it to see if there are unauthorized changes to the system. ● Password Policies- NIST recommends policies that focus on salt and hash passwords. This is to prevent attackers from easily guessing passwords and brute force attacks. This also goes for admin accounts and not password sharing. ● Multi-Factor Authentication requires a user to verify their identity in two ways. This will help prevent brute force attacks and password sharing. ● Network access privileges- This concept is to provide privileges only to those that need it, limiting the amount of access certain assets have. This will limit unauthorized users from accessing unnecessary data and prevent risk of outside traffic getting to that asset. ● Firewall maintenance- this includes checking and updated security configurations. These rules can be incorporated on a regular basis, or it can be in response to an attack. This will also protect against a DDoS attack, which happens when a source overloads a server with the intention of crashing it. ● Port Filtering- this is a function applied through the firewall that will block certain port numbers to limit communication. This can control network traffic and prevent attackers from entering a network.