Security risk assessment report

Part 1: Incident's documentation
How it happened: A social media company has suffered a data breach which compromised the user's SPII (*Sensitive Personal Identifiable Information*). After the occurrence, the company started to review the cybersecurity policies with the goal of hardening its network security aspect, which was the main vector used by the threat actors to break into the system. **The audit's assessments**: After performing a security audit within the company, four major vulnerabilities were discovered : - The employees make use of shared password to perform their tasks; - The administrative profile, used to access the companies' database, utilizes the default passcode, which is weak; - The firewall used on the network doesn't contain rules to regulate the in and outgoing traffic from the internal network to the internet; - The company does not make use of any MFA (Multi Factor Authentication) framework. The conclusion of the audit assessed that those four points were the major reasons why the company was susceptible to the attack.

Part 2: Hardening tools and methods to be implemented

Some possible security measures and tools which the company can implement to prevent similar attacks from happening again in the future, and also harden the organization's network security, are the following:

1. **Password Policies**: The company should implement a strict password policy amongst the employees. The **NIST** (*National Institute of Standards and Technology*) advises that passwords should be configured with the latest hashing encryption algorithms, using the salting method to generate those hashes. According to *NIST*, this measure is way more effective than requiring employees to make regular changes or use over complicated passcodes. Compliance regulations should also be created and frequently evaluated by security analysts, to be certain that all staff members are following the established guidelines, consequently, meeting the company's security goals.

2. **MFA** (*Multi Factor Authentication*): Together with a strict pass code policy, at least one MFA framework should also be implemented to the security infrastructure. Achieving a more effective reliability objective, regarding the employees' access to the network. It is essential to have ways of authenticating the users without relying on a simple username-password method.

3. **Firewall maintenance**: The organization should have a dedicated analyst or team of analysts, depending on how much network traffic is handled on the daily basis, to properly install and maintain the firewalls. The attributions of this individual, or team of individuals, are: updating the firewall rules according to the network traffic and keeping the firewalls up-to-date with the new security threats. Another important aspect of firewall maintenance is **port filtering**, paramount to control the in and outgoing traffic, thus preventing threat actors from entering the internal network.

4. **Network Log Analysis**: The company should set up a log analysis tool to keep up with the traffic that comes in and out of the internal network. These tools will help prevent further break in attempts into the system, since they can be used not only to analyze traffic, but also to create alerts for possible threats. **SIEM** (*Security Information and Event Management*) tools are often used for this situation, because they are flexible and can be implemented on many security aspects of an organization, not only for the network traffic analysis.

Part 3: Explanation for the recommendations

The tools and methods, suggested to be added to the security infrastructure of this company at section *Part 2*, have a reason for being. In this section all those elements will be discussed in further detail, explaining the need for such measures.

- The first security aspect was **password policies**. Strict key code policies are essential to preserve the users of the company's internal network and the network itself. Weak and easy-to-decrypt passwords are often used as an exploitation vector by threat actors as a way to gain access to the organization's system, causing harm and damaging the company's image. That's why effective hashing algorithms and multi factor authentication (**MFA**) should be implemented to minimize those risks.

- Another topic mentioned was **firewall maintenance**, which is a vital part for the security framework of any establishment. The lack of effectiveness of a firewall works as an open door to threat actors, who can use this vulnerability as a direct gateway to the internal network. That is the reason why firewalls should be properly set up and maintained, using up to date rules and **port filtering** methods to avoid leaving any open backdoor into the company's system.

- The final suggested element used as a protection measure was a **network log analysis** tool. When a company has a lot of traffic coming from the internal network, it's easy to lose track of what is being accessed from the inside out and what kind of data is coming in from the outside. This window of unknown traffic is often used by threat actors as a leverage to perform tasks such as *port scans* or *social engineering* attacks, targeting the employees and trying to gain access to the system. Therefore, **SIEM** tools are used as one possible solution to this problem, since those tools can be used to analyze network traffic logs and display a more visual comprehensive data, which can later be used to respond to incidents in case of a security threat alert is shown on the dashboard, alert provided by the tool itself.

Many security measures can be used to minimize the attack surface of a system, so, using multiple barriers can assure the security of an organization, reduce the risk of attacks, and keep the integrity of the data as well as the company.