Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are a security analyst working for a social media organization. The organization recently experienced a major data breach, which compromised the safety of their customers’ personal information, such as names and addresses. Your organization wants to implement strong network hardening practices that can be performed consistently to prevent attacks and breaches in the future.

After inspecting the organization’s network, you discover four major vulnerabilities. The four vulnerabilities are as follows:

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.

Multifactor authentication (MFA) is not used.

If no action is taken to address these vulnerabilities, the organization is at risk of experiencing another data breach or other attacks in the future.

In this activity, you will write a security risk assessment to analyze the incident and explain what methods can be used to further secure the network.

Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| The network hardening tools to implement are the SIEM tools, The Intrusion Prevention System and The IDS tools.  Methods to implement are;  1. Multifactor Authentication  2. Penetration Testing  3. Port Filtering |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| The MFA is an effective hardening technique that the organization's employees can use to verify in two or more ways to securely access the network. They include a password, finger print and also an OTP. This can bre implemented at any time and it's mostly a technique that can be set uponce and then maintained.  The security team should carry out pen testing regularly to identify vulnerabilities in the network that could be exploited by a malicious actor in order to protect and prevent against potential attacks.  Port filtering must be implemented by the organization to filter traffic coming in and out of the network and pevent potential attacks from entering a private network. |

|  |  |  |
| --- | --- | --- |
| Security hardening task | Description | Common uses |
| Baseline configurations | A documented set of specifications within a system that is used as a basis for future builds, releases, and updates. | To restore a system to a previous baseline after a network outage, or unauthorized changes on a baseline. |
| Configuration checks | Updating the encryption standards for data that is stored in databases. | To see if there are any unauthorized changes to the system. |
| Disabling unused ports | Ports can be blocked on firewalls, routers, servers, and more to prevent potentially dangerous network traffic from passing through. | Before an incident occurs, to prevent malicious actors from entering the network through the open port. Can be used after an incident to prevent future attacks from happening through unused open ports. |
| Encryption using the latest standards | Rules or methods used to conceal outgoing data and uncover or decrypt the incoming data. | Can be implemented regularly to assess if the current encryption standards are secure and effective for your organization. The encryption standards can also be updated after a data breach. |
| Firewall maintenance | Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. | This can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. |
| Hardware & software disposal | Ensures that all old hardware is properly wiped of all data and disposed of. | Prevent the network from various threats by removing outdated or unused software or hardware that do not have the latest security patches or updates. Unpatched devices can allow malicious actors to easily access the network. |
| Multifactor authentication (MFA) | A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. | Can help protect against brute force attacks and similar security events. MFA can be implemented at any time, and is mostly a technique that is set up once then maintained. |
| Network access privileges | Network access privileges involves permitting, limiting, and/or blocking access privileges to network assets for people, roles, groups, IP addresses, MAC addresses, etc. | Reduces the risk of unauthorized users and outside traffic from accessing the internal network. This can be implemented once, or revisited depending on the likelihood of social engineering or brute force attacks. |
| Network log analysis | The process of examining network logs to identify events of interest. | Can be configured to alert the security team when there is abnormal traffic on the network. This can be used either before an incident occurs, during to track network traffic, and can be configured in the response of a cybersecurity attack. A common tool used for analyzing network logs is a SIEM. |
| Password policies | The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. | Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack). |
| Patch updates | A software and operating system (OS) update that addresses security vulnerabilities within a program or product. | Patch updates often contain fixes to security problems. It is important to keep systems up to date with the latest security patches because attackers will be alerted to the security vulnerability when patches are released. They will be more likely to target that vulnerability before people eventually apply the patches. |
| Penetration test (pen test) | A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. | Pen tests are used to protect and prevent against potential attacks. |
| Port filtering | A firewall function that blocks or allows certain port numbers to limit unwanted communication. | Port filtering is used to control network traffic and can prevent potential attackers from entering a private network. |
| Removing or disabling unused applications and services | Unused applications and services can become a point of vulnerability because they are less likely to be maintained or updated with new security features. | This procedure is used to reduce potential vulnerabilities within a network. |
| Server and data storage backups | Server and data storage backups help protect data assets from being lost. Backups can be recorded and stored in a physical location or uploaded/synced to a cloud repository. | Backups are used to restore lost data from attacks, human error, equipment failures, and other unplanned losses. |