

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

MFA – require all users to carry either one-time key or authenticator app
Port filtering – close off ports on firewall that are not necessary for function
Encryption – encrypt any sensitive data so even if data's compromised decryption is not practical.

Part 2: Explain your recommendations

MFA (multi-factor authentication) should be implemented ASAP. This, when combined with encryption, would prevent password sharing, and even the use of default password without the other factor would be useless.

Port filtering set on the firewall would reduce attack surface, preventing outside traffic from reaching local servers that shouldn't reach such.

Finally, state of art encryption would ensure that any intruders would not get any plaintext data, esp. When proper salting and hashing were used.

When combined, these three recommendations would reduce the possibility of password compromise, eliminate brute force or dictionary attacks, ability to even reach the database servers, and finally, even if they do reach the servers, they won't be able to do anything with the encrypted data.