Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
To address the critical vulnerabilities identified in our network infrastructure, I recommend the immediate implementation of three fundamental hardening tools. The first is the adoption of an enterprise-grade password management system such as Bitwarden or 1Password, accompanied by a strict corporate policy requiring unique passwords of at least 16 characters with mandatory quarterly rotation. The second intervention concerns the complete configuration of firewall rules implementing both ACLs (Access Control Lists) and zone-based filtering, with particular attention to creating specific rules for inbound and outbound traffic based on the principle of least privilege. As the third essential tool, I propose deploying a multi-factor authentication system using TOTP tokens (Time-based One-Time Password) or hardware solutions like YubiKey for all administrative access and databases containing sensitive data.

Part 2: Explain your recommendations
The selection of these three hardening tools directly addresses the most critical vulnerabilities discovered during our assessment. Implementing an enterprise password manager simultaneously resolves two of our most severe vulnerabilities: it completely eliminates the practice of password sharing by providing each employee with a secure, encrypted personal vault, and prevents the use of default passwords through automatic generation of complex and unique credentials for each system. This approach not only improves security but also increases productivity by eliminating the need to remember multiple complex passwords. Proper configuration of firewall rules creates what the industry calls defense-in-depth, establishing a security perimeter that analyzes and filters all network traffic. By implementing stateful inspection and deep packet inspection rules, we can identify and block unauthorized access attempts before they reach our critical systems. The rules should follow a deny-by-default approach,

allowing only explicitly authorized traffic necessary for business operations, drastically reducing the attack surface available to external aggressors.
Multi-factor authentication represents perhaps the single most effective measure we can implement, considering that according to Microsoft it reduces the risk of account compromise by 99.9%. Even if an employee's credentials are compromised through phishing or other attacks, MFA prevents unauthorized access by requiring a second factor that the attacker does not possess. For our databases containing customers' personal information, this additional layer of security is absolutely critical and should be considered non-negotiable. Implementation should begin with administrative accounts and then gradually extend to all users, accompanied by training sessions to ensure proper adoption by staff.
These interventions, if implemented correctly and in a coordinated manner, will radically transform our security posture, moving from a vulnerable environment to one that follows industry best practices and can effectively resist most common attacks that affect organizations in our sector. The combination of these three tools addresses all four identified vulnerabilities while creating multiple layers of protection that work synergistically to protect our customers' data and maintain the integrity of our social media platform.