Server Hardening Checklist

Update the OS

Update 3rd party applications.

Remove unnecessary/insecure 3rd-party apps.

Patch Vulnerabilities.

Minimize unnecessary software on your servers.

Remove unnecessary operating system components.

Unnecessary services should be disabled.

Minimize open network ports.

Use IP Filtering.

Physical server security.

Keep staff aware, informed, and trained.

Manage access to your servers and critical infrastructure.

Restrict critical apps and system files to admins.

Firewall Installation/Configuration.

Monitor and log all access attempts to network devices.

Limit membership to admin users/groups.

Limit user account access to the least privilege needed.

Group user access / permissions by role.

Keep Inventory Updated.

Mirror logs to a separate log server.

Scans/Audits of the server - check for malware/hacks.

Restrict sensitive information to trusted accounts only.

Join Computer to Active Directory if required.

Access should only be on an as needed basis.

Delete/disable unnecessary OS user accounts.

Use the best data encryption Protocols & Cipher Suites for your Communications.

Disable insecure protocols.

Use Security applications, such as Defender Or Defender for Cloud

Choose secure settings recommended by the software vendor.

Keep Security applications updated.

Use Stable versions with latest security patches.

Require Multi-Factor Authentication for sensitive user accounts, systems, or items.

Use regular VM snapshots, or database/application/file backups

Categorize data - which data must remain highly available.

Use Disaster Recovery (DR) and High-Availability (HA) as required.

Establish a periodic archive of your data to a remote site / data storage location.

Have users use very strong passwords or passphrases, especially for administrative passwords.

Change regular account names from 'admin' or 'guest.'

Maintain proper backups.

Keep server clock in-sync.