

RAPPORT D'AUDIT IT

Réf : AUDIT-SERVER-2025
Date : 22/12/2025

Périmètre : Audit Serveurs & Virtualisation



Synthèse

Niveau de maturité détecté : Initial

Détail des risques identifiés

Niveau	Risque Identifié	Impact Métier	Action Recommandée
Critique	Conserver les sauvegardes uniquement sur le site de production rend l'entreprise vulnérable aux sinistres physiques (incendie, inondation, vol) et aux ransomwares qui chiffrent souvent les backups locaux accessibles.	Perte totale sur sinistre majeur	Ajouter une copie Cloud ou disque dur externe rotatif
Critique	Le Contrôleur de Domaine unique est un SPOF critique. Sa perte entraîne l'arrêt immédiat de toutes les authentifications : plus d'ouverture de session, plus d'accès aux fichiers, plus de messagerie. L'activité s'arrête totalement.	Arrêt complet du SI	Installer un second DC (même en VM)
Critique	L'absence de redondance disque (RAID) signifie qu'une simple panne de disque dur entraîne la perte immédiate de toutes les données du serveur et l'arrêt du service. C'est une configuration inacceptable en production.	Perte de données sur panne disque	Migrer vers RAID sécurisé
Critique	Utiliser un compte Administrateur de Domaine pour des tâches bureautiques quotidiennes est une faute grave. Si ce compte est compromis (phishing),	Compromission totale du domaine	Créer comptes nominatifs dédiés

Niveau	Risque Identifié	Impact Métier	Action Recommandée
	l'attaquant obtient instantanément le contrôle total de toute l'infrastructure.		
Critique	Une sauvegarde jamais testée est une sauvegarde inexistante. En l'absence de tests réguliers, il est probable que les données soient corrompues ou incomplètes, ce qui ne sera découvert qu'au moment du sinistre, trop tard.	Fausse sécurité	Organiser un test de restauration
Majeur	Un contrat de support standard (J+5) ou partiel est incompatible avec les exigences de production. En cas de panne critique (Carte mère, Alimentation), l'entreprise subira un arrêt d'activité de plusieurs jours en attendant les pièces.	Arrêt de production prolongé	Upgrade garantie ou stock pièces critiques
Majeur	L'architecture basée sur des serveurs autonomes constitue un point de défaillance unique (SPOF). En cas de panne de l'hôte physique, l'ensemble des services hébergés subit une interruption totale jusqu'à réparation manuelle.	Disponibilité non garantie	Étudier passage en cluster (HCI ou SAN)
Majeur	Un environnement physique inadapté (chaleur, poussière, accès libre) réduit drastiquement la durée de vie du matériel et augmente les risques de pannes aléatoires et d'actes de malveillance interne.	Fiabilité réduite	Mettre en baie fermée ventilée
Majeur	Un onduleur non piloté ne protège pas contre l'arrêt brutal lors d'une coupure longue. L'arrêt non propre des serveurs corrompt les bases de données et les systèmes de fichiers, nécessitant des interventions lourdes de réparation.	Corruption de données	Connecter USB/Réseau onduleur
Majeur	L'accès physique libre aux serveurs permet le vol de disques, le branchement de périphériques malveillants ou l'extinction accidentelle. La sécurité physique est la première couche de la sécurité informatique.	Intégrité physique	Verrouiller l'accès
Modéré	Sans outils de supervision, la DSI navigue à l'aveugle. Les pannes (disque plein, service arrêté) ne sont découvertes que lorsque les utilisateurs sont bloqués, entraînant une réactivité médiocre et des arrêts de service évitables.	Exploitation réactive	Installer sonde monitoring
Faible	Négliger les mises à jour firmware expose le matériel à des bugs de stabilité connus et à des failles de sécurité bas	Stabilité et Sécurité	Mise à jour annuelle

Niveau	Risque Identifié	Impact Métier	Action Recommandée
	niveau. Cela réduit la fiabilité globale de l'infrastructure serveur.		
Faible	L'absence de documentation technique crée une dépendance critique envers les personnes. En cas de départ du référent technique, la reprise en main de l'infrastructure devient complexe et risquée.	Maintenabilité réduite	Rédiger dossier architecture

Besoin d'un audit approfondi sur site ?

Nos ingénieurs certifiés interviennent partout au Maroc.

Contact : +212 5 22 52 32 32 | contact@x-zone.ma

Ce document est un rapport préliminaire automatisé. Il ne remplace pas un audit physique complet.