Auto-Évaluation Cybersécurité

CyberScore : 

Date de génération du rapport : **08/11/2026 20:16**

> Ce rapport est une simple auto-évaluation de votre niveau de sécurité informatique, basée exclusivement sur vos réponses au questionnaire conçu par les experts d'Oxydian. Il ne constitue en aucun cas un audit technique approfondi. Bien qu'il vous offre un premier aperçu de vos forces et vulnérabilités en matière de cybersécurité, il ne remplace pas une analyse rigoureuse de vos infrastructures et systèmes. Pour aller plus loin et bénéficier d'un audit technique complet, n'hésitez pas à nous contacter :
>
> contact@oxydian.fr

Synthèse :

Votre niveau de sécurité présente des faiblesses significatives qui méritent une attention immédiate. Le risque d'exploitation de certaines vulnérabilités est élevé, ce qui pourrait compromettre la sécurité globale de votre organisation. Nous recommandons fortement la mise en place de mesures correctives et envisageons un accompagnement spécialisé pour réaliser un audit approfondi.

Détail des scores par catégorie (40.0%)

Mots de Passe

Sécurité des données



Surveillance et Détection



Sécurité interne



Sécurité externe



Gestion de la sécurité



Identification des risques



Sécurité Physique



Plan d'action personnalisé :

Ce plan d'action est basé sur les résultats de votre évaluation. Nous vous recommandons de suivre ces conseils pour améliorer votre sécurité informatique.

Sécurisation du stockage des mots de passe
Assurez-vous que tous les mots de passe sont stockés dans un gestionnaire de mots de passe sécurisé plutôt que sur des supports non sécurisés.

Utiliser un antivirus
Assurez-vous que tous vos serveurs et machines sont équipés d'un antivirus à jour pour détecter et bloquer les menaces.

Remplacement des machines obsolètes
Remplacez ou migrer les machines obsolètes (Windows XP, Vista, 7, 8 ou Windows Server 2003 / 2008 / 2012) pour réduire les risques de vulnérabilités non corrigées.

Séparer les droits utilisateur et administrateur
Cette pratique consiste à attribuer des comptes distincts pour les tâches quotidiennes et les tâches administratives. Cela réduit considérablement les risques de compromission de sécurité, en limitant l'accès aux privilèges élevés uniquement aux opérations spécifiques nécessitant une gestion administrative

Mise en place d'une politique de mots de passe
Mettez en place une politique de mots de passe rigoureuse pour assurer que les mots de passe sont sécurisés, complexes et régulièrement renouvelés.

Protection de la messagerie par la 2FA
Activez l'authentification à deux facteurs (2FA) sur l'ensemble des comptes de messagerie de l'entreprise (Microsoft 365, Google Workspace..). La compromission de messagerie est le vecteur d'attaque le plus fréquent visant les PME et la 2FA bloque la grande majorité de ces attaques.

Analyse régulière des mots de passe
Effectuez régulièrement des analyses de vos mots de passe par un professionnel ou votre DSI pour détecter les mots de passe faible, les réutilisations et renforcer la sécurité.

Mise en place du chiffrement de disque
Il est fortement recommandé d'activer le chiffrement de disque sur tous les PC et les serveurs, en utilisant des solutions comme BitLocker pour Windows ou LUKS pour Linux, afin de protéger vos données sensibles contre les accès non autorisés.

Tests de restauration des sauvegardes
Planifiez des tests de restauration réguliers (au moins une fois par trimestre) pour vérifier que vos sauvegardes sont réellement exploitables et mesurer le temps nécessaire à la reprise de votre activité.

Établissement d'une cartographie des actifs externes
Mettez à jour et complétez régulièrement la cartographie de vos actifs exposés sur internet pour améliorer la gestion de la sécurité.

Mise en place de la 2FA pour le VPN
Activez l'authentification à deux facteurs (2FA) pour tous les accès VPN afin de renforcer la sécurité des connexions distantes.

Procédure de réponse à incident
Formalisez une procédure de réponse à incident : premières actions à mener, liste des contacts d'urgence (prestataire spécialisé, assureur, CNIL en cas de fuite de données) et rôles internes. Testez-la au moins une fois par an via un exercice sur table.

Mise en place de l'authentification à deux facteurs
Activez l'authentification à deux facteurs (2FA) sur tous vos comptes et services critiques pour ajouter une couche supplémentaire de sécurité.

Redondance des sauvegardes
Il est fortement recommandé de stocker vos sauvegardes dans plusieurs emplacements distincts pour réduire les risques de perte de données en cas de sinistre.

Évolution vers un EDR
Remplacez ou complétez votre antivirus classique par une solution EDR (Endpoint Detection and Response), capable de détecter les comportements malveillants et d'isoler les machines compromises face aux attaques modernes comme les ransomwares.

Centralisation des journaux
Centralisez les journaux de vos serveurs et équipements critiques sur un espace de stockage dédié et conservez-les plusieurs mois (6 à 12 mois recommandés). Cela permet de détecter les incidents et de les analyser même si l'attaquant efface les traces locales.

Établissement d'une cartographie des actifs internes
Mettez à jour et complétez régulièrement la cartographie de vos actifs internes pour améliorer la gestion de la sécurité.

Segmentation du réseau Wi-Fi
Implémentez plusieurs réseaux Wi-Fi pour séparer les accès publics et internes afin de renforcer la sécurité out en proposant un Wi-Fi public pour l'accès internet uniquement.

Mise en place d'une politique de mise à jour Externe
Adoptez une politique stricte de mise à jour pour tous vos actifs externes afin de minimiser les risques liés aux vulnérabilités.

Mise en place d'une charte informatique
Assurez-vous que tous les employés signent une charte informatique qui définit les règles et bonnes pratiques en matière de sécurité, en insistant sur la protection des données personnelles pour respecter les exigences du RGPD.

Exercices de phishing réguliers
Organisez des campagnes de faux phishing au moins une fois par an pour mesurer les réflexes de vos collaborateurs en conditions réelles et cibler la sensibilisation sur les points faibles identifiés.

Encadrement des accès prestataires
Encadrez les accès de vos prestataires : comptes nominatifs dédiés, droits limités au strict besoin, désactivation systématique en fin d'intervention ou de contrat, et traçabilité des connexions.

Contrôle d'accès à la salle des serveurs
Implémentez un contrôle strict de l'accès à la salle des serveurs pour éviter les manipulations non autorisées.

Mise en place d'un protocole d'arrivée/départ
Assurez-vous de définir un protocole clair pour l'arrivée et le départ des collaborateurs, incluant la suppression des comptes et des accès pour protéger l'entreprise contre les risques de sécurité.

Légende :

INFORMATION

Risque global nul, il s’agit simplement de remarques remontées lors de l’audit.

MINEUR

Risque global faible qui n’impose pas d’actions importantes.

MODÉRÉ

Risque global modéré qui impose des actions à moyen terme.

MAJEUR

Risque global majeur qui impose des actions à court terme.

CRITIQUE

Risque global critique qui impose des actions immédiates.