Auto-Évaluation Cybersécurité

CyberScore : 

Date de génération du rapport : **13/11/2024 10:28**

> 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 (40.3%)

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.

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.

Utilisation de mots de passe uniques
Adoptez une politique d'utilisation de mots de passe uniques pour chaque compte afin de limiter les risques en cas de compromission.

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.

Renforcement des sauvegardes
Il est fortement recommandé d'effectuer des sauvegardes quotidiennes de vos données pour minimiser la perte potentielle en cas d'incident.

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.

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.

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

Politique BYOD
Si vous autorisez l'utilisation d'équipements personnels, veillez à établir des politiques strictes pour sécuriser les données de l'entreprise et limiter les risques de sécurité.

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.

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.

Mettre en place un gestionnaire de mots de passe
Utilisez un gestionnaire de mots de passe pour stocker en toute sécurité et générer des mots de passe uniques et forts pour chaque compte. Il existe des solutions auto-hébergées ou en ligne. Bitwarden, une solution open source éprouvée, est disponible dans ces deux cas d'usage, offrant ainsi flexibilité et sécurité selon vos besoins.

Mise en place d'un système d'alerte
Implémentez un système d'alerte sur tous vos systèmes pour détecter rapidement les menaces potentielles.

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

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.

Élaboration et mise à jour du PRA
Élaborez un Plan de Reprise d'Activité solide et assurez-vous qu'il est régulièrement mis à jour et testé. Ce plan doit inclure des procédures claires pour restaurer les systèmes critiques et garantir la continuité des opérations en cas d'incident majeur.

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.