Anticipez votre audit de sécurité : le plan d'action pour un Cyberscore optimal

Maîtrise du périmètre et des accès

• Réaliser un inventaire exhaustif des actifs : lister équipements, logiciels et services cloud pour définir le périmètre réel.

• Appliquer le principe du moindre privilège : limiter les accès administrateurs et révoquer systématiquement les comptes inactifs ou anciens collaborateurs.

• Généraliser l'authentification multifacteur (MFA) sur tous les services exposés, en priorité pour les accès distants et les comptes à hauts privilèges.

Protection des données et résilience

• Sécuriser les sauvegardes via la règle du 3-2-1 : 3 copies, 2 supports différents, 1 copie hors ligne ou immuable.

• Chiffrer les données sensibles au repos sur les disques et en transit via le protocole TLS 1.2 ou supérieur.

Maintenance et surveillance proactive

• Appliquer les correctifs de sécurité critiques sous 48 heures pour tous les systèmes exposés.

• Centraliser les journaux d'événements (logs) de sécurité et configurer des alertes automatiques sur les comportements anormaux.

Culture de sécurité et capacité de réaction

• Sensibiliser régulièrement les collaborateurs aux vecteurs d'attaque comme le phishing et aux bonnes pratiques de gestion des mots de passe.

• Élaborer et tester annuellement un Plan de Continuité d'Activité (PCA) et un Plan de Reprise d'Activité (PRA).

• Valider le niveau de sécurité réel par un test d'intrusion ou un audit à blanc réalisé par un prestataire externe qualifié (type PASSI).