Labgroup | Your documents. Your data. Our business.

Quelle est la résilience de votre système IT ?

& 5 leviers pour renforcer la robustesse de votre SI

VOS RÉSULTATS

Q1 – Avez-vous mis en place un plan un plan BCP ou DR ?

- ✅ Oui, testé : Très bon réflexe, continuez.
- ⚠️ Oui, non testé : À formaliser et tester rapidement.
- ⚠️ En cours : Bonne démarche, à finaliser vite.
- ❌ Non / Je ne sais pas : Risque élevé en cas de crise.

Q2 – Comment contrôlez-vous les accès aux données sensibles ?

- ✅ IAM + MFA : Excellent niveau de sécurité.
- ⚠️ Par rôles internes : À renforcer avec MFA.
- ⚠️ Au cas par cas : Failles potentielles, à structurer.
- ❌ Pas de stratégie : Données exposées.

Q3 – Sur quoi repose votre résilience ?

- ✅ Sauvegardes : Base indispensable.
- ✅ Cloud / Redondance : Très bon point.
- ✅ Surveillance proactive : Prévention efficace.
- ✅ Formation des équipes : Clé contre les erreurs humaines.
- ❌ Aucune mesure : Risque critique.

Q4 – Quel est votre plus grand risque ?

- Ransomware : Protégez vos sauvegardes.
- Erreur humaine : Formez vos équipes.
- Fuite interne : Renforcez les accès et les audits.
- Panne matérielle : Mettez en place un PRA.
- Autre : Intégrez-le à votre stratégie globale.

Q5 – Comment évaluez-vous votre préparation à une crise IT ?

- ✅ Très préparé : Continuez à tester.
- ⚠️ Moyennement : Consolidez vos points faibles.
- ❌ Peu / Pas du tout : Réagissez vite.
- ❌ Je ne sais pas : Ce flou est un risque en soi.

Vos réponses au diagnostic montrent peut-être des besoins d'amélioration. Pour vous aider à passer à l'action, **voici les leviers essentiels à activer pour mieux protéger votre système d'information.**

Les 5 leviers pour renforcer votre résilience IT

01 Une stratégie de sauvegarde éprouvée

- Appliquer la méthode 3-2-1 : 3 copies – 2 supports différents – 1 hors site
- Tester régulièrement la restauration des données

02 Simuler un incident pour mieux réagir

- Exercices de type “table-top”
- Tests de récupération après sinistre
- Scénarios cyber & techniques

03

Protéger vos données au-delà de vos murs

- Exercices de type “table-top”
- Tests de récupération après sinistre
- Scénarios cyber & techniques

04 Former vos utilisateurs : le maillon humain

- Sessions courtes (30 min à 1h) sur : le phishing, la réaction à une attaque, les bonnes pratiques de mot de passe
- Campagnes de tests simulés

05 Simuler un incident pour mieux réagir

- Audit de sécurité tous les 12-24 mois
- Scan de vulnérabilités et tests d'intrusion
- Vérification des accès, mises à jour, et procédures de crise

Besoin d'un regard extérieur ?
Notre équipe est là pour vous accompagner à chaque étape.

Construisons ensemble une stratégie de sauvegarde adaptée à votre environnement.

Il vous suffit de remplir ce court formulaire : notre équipe vous recontactera rapidement pour un échange personnalisé.

CONTACTEZ-NOUS