COMMENT PILOTER SA CYBERSÉCURITÉ
(dirigeants)

« Méthodologie synthétique de gestion de la cybersécurité à destination des dirigeants d'entreprises, d'associations, de collectivités et d'administrations »

1. RÉALISEZ UN ÉTAT DES LIEUX

Commencez par établir un inventaire aussi complet que possible de tous vos actifs numériques : réseaux internes, sites web, messageries, réseaux sociaux, applications ou services externalisés. Identifiez également les personnes ou services responsables de chacun d'eux (support informatique interne ou prestataire externe).

2. PRENEZ CONSCIENCE DU RISQUE

Pour chacun des systèmes identifiés, analysez le niveau de risque qu'impliquerait un piratage, une destruction ou le vol des données qu'il contient. Évaluez ainsi son importance pour le bon fonctionnement de votre organisation.

3. ÉVALUEZ VOTRE NIVEAU DE PROTECTION

Demandez à votre support informatique, qu'il soit interne ou externe, d'analyser la pertinence des mesures de sécurité en place techniques, organisationnelles et contractuelles au regard de vos enjeux. Cela inclut notamment les politiques de mots de passe, les procédures de sauvegarde, les mises à jour et le filtrage des accès externes.

4. DÉFINISSEZ UN PLAN D'ACTION

Sachant que 80 % des cyberattaques pourraient être évitées grâce à des mesures simples et peu coûteuses comme une gestion rigoureuse des mots de passe, des sauvegardes régulières, l'application des mises à jour de sécurité ou un contrôle précis des droits d'accès, établissez une liste d'actions à mener. Priorisez-les en fonction du rapport criticité / coût / efficacité.

5. FAITES-VOUS ACCOMPAGNER

Si aucune personne n'est actuellement dédiée à ce rôle, désignez un collaborateur chargé de piloter votre plan de cybersécurité. Pour évaluer techniquement le niveau de protection de vos systèmes critiques, faites appel à un prestataire spécialisé en cybersécurité, que vous pouvez identifier via la plateforme Cybermalveillance.gouv.fr.

6. SENSIBILISEZ VOS COLLABORATEURS

Vos équipes constituent un maillon central de votre cybersécurité. Qu'il s'agisse d'adopter de bonnes pratiques, de détecter une tentative d'attaque ou d'y réagir efficacement, leur rôle est crucial. De nombreuses ressources gratuites de sensibilisation sont disponibles sur Cybermalveillance.gouv.fr.

7. PRÉPAREZ-VOUS AU PIRE

Aucune cybersécurité n'est infaillible : une attaque réussie reste toujours possible. Il est donc indispensable de prévoir des dispositifs de secours pour gérer une situation de crise : annuaire de crise, plan de fonctionnement dégradé, communication interne et externe. N'hésitez pas à organiser des exercices réguliers pour tester et améliorer ces dispositifs.

8. IMPLIQUEZ-VOUS

En tant que dirigeant, votre implication est essentielle pour garantir la bonne mise en œuvre du plan cybersécurité. Pilotez-le au travers de points d'avancement réguliers, montrez l'exemple et exigez que l'ensemble des cadres et collaborateurs respecte strictement les mesures de sécurité en place.

9. CONTRÔLEZ

Assurez-vous que les décisions prises sont réellement appliquées. Pour vos systèmes les plus critiques, un audit technique et organisationnel peut être nécessaire. Vous pouvez solliciter un prestataire spécialisé en cybersécurité, répertorié sur Cybermalveillance.gouv.fr.

10. ITÉREZ

Les services numériques évoluent constamment, tout comme les techniques d'attaque. Il est donc recommandé d'appliquer à nouveau cette démarche lors du déploiement de tout nouveau service numérique, et de manière globale tous les deux à trois ans.

Retrouvez plus d'informations sur : www.cybermalveillance.gouv.fr