RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMMENT PILOTER SA CYBERSÉCURITÉ ? (DIRIGEANTS)

Pour vous informer sur les bonnes pratiques
et les principales menaces en matière de cybersécurité
rendez-vous sur :
www.cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMMENT PILOTER SA CYBERSÉCURITÉ ? (DIRIGEANTS)

Méthodologie synthétique de gestion de la cybersécurité pour les dirigeants des entreprises, associations, collectivités, administrations.

1 FAITES UN ÉTAT DES LIEUX

Dans un premier temps, il convient de dresser un inventaire le plus exhaustif possible de l'ensemble de vos actifs numériques (réseaux internes, sites Internet, messageries, réseaux sociaux, applications et services externalisés…), et de leurs responsables (support informatique interne ou externe).

2 PRENEZ CONSCIENCE DU RISQUE

Pour chaque système recensé, évaluez sa criticité pour le fonctionnement de votre organisation s'il venait à être piraté ou détruit ou si les données qu'il contient étaient dérobées par des cybercriminels.

3 ÉVALUEZ VOTRE NIVEAU DE PROTECTION

Interrogez votre support informatique interne et/ou externe sur la pertinence des mesures de sécurité techniques, organisationnelles et contractuelles appliquées au regard des enjeux, telles les politiques de mots de passe, de sauvegardes, de mises à jour ou encore de filtrage des accès externes.

4 DÉFINISSEZ UN PLAN D'ACTION

80 % des cyberattaques pourraient être évitées par l'application de mesures simples et à faible coût telles qu'une bonne gestion des mots de passe, des sauvegardes, des mises à jour de sécurité ou des droits d'accès. Priorisez les actions à entreprendre en fonction du rapport criticité/coût/efficacité.

5 FAITES-VOUS ACCOMPAGNER

Si aucun collaborateur n'est assigné à ce rôle, désignez une personne en charge de vous assister dans le pilotage du plan de cybersécurité de votre organisation. Pour l'évaluation technique du niveau de protection sur vos systèmes critiques, faites appel à un prestataire spécialisé en cybersécurité que vous pourrez trouver sur Cybermalveillance.gouv.fr.

6 SENSIBILISEZ VOS COLLABORATEURS

Vos collaborateurs sont un maillon essentiel de votre cybersécurité, qu'il s'agisse d'appliquer de bonnes pratiques de cybersécurité, de détecter ou de réagir à une tentative de cyberattaque. De nombreuses ressources gratuites de sensibilisation sont disponibles sur Cybermalveillance.gouv.fr.

7 PRÉPAREZ-VOUS AU PIRE

Il n'y a pas de cybersécurité absolue : le risque d'une cyberattaque réussie est malheureusement toujours possible. Il convient donc de préparer des plans de secours pour affronter une crise : annuaire de crise, fonctionnement dégradé, communication… Et de réaliser des exercices pour évaluer leur efficacité.

8 IMPLIQUEZ-VOUS

Pour vous assurer que le plan d'action cybersécurité est bien conduit, vous devez en tant que dirigeant vous impliquer, en le pilotant par des points de situation et d'avancement réguliers à votre niveau. Vous devez également montrer l'exemple et exiger de vos cadres et collaborateurs qu'ils ne dérogent ou ne contournent pas les mesures de sécurité décidées pour protéger leur organisation.

9 CONTRÔLEZ

Il est en effet important de vérifier que les décisions prises ont bien été mises en place. Pour les systèmes les plus critiques, un audit technique et organisationnel peut s'avérer nécessaire : il est recommandé de faire appel à un prestataire spécialisé en cybersécurité que vous pourrez trouver sur Cybermalveillance.gouv.fr.

10 ITÉREZ

Les services numériques des organisations évoluent en permanence, tout comme les moyens permettant de les attaquer. Pour en tenir compte, il est recommandé de « réappliquer » cette méthode pour tout nouveau service numérique, avant sa mise en œuvre, et de manière globale tous les deux à trois ans.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

V230419