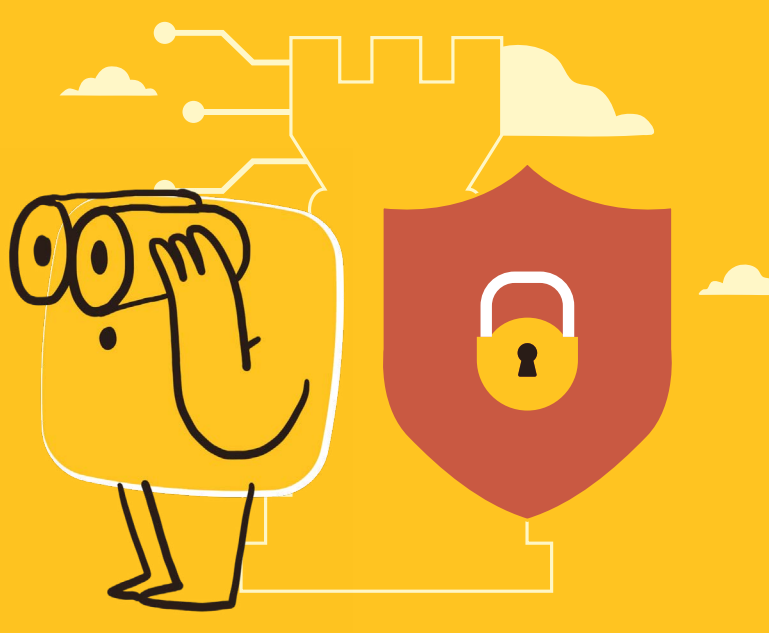
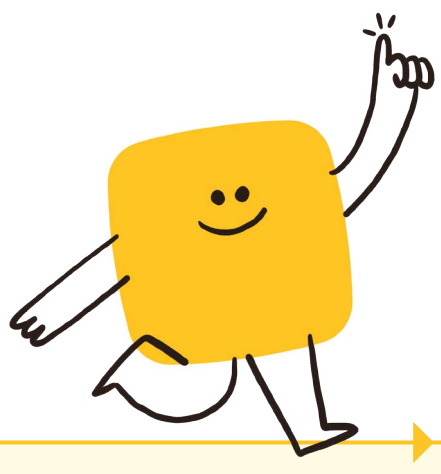
Quel est le niveau de cybersécurité de votre entreprise ?



Garantissez la continuité de votre activité en suivant les 5 étapes de ce plan



ÉTAPE 01

Identification des menaces

En cybersécurité aussi, mesurer les risques, c'est mieux reconnaître les danger. Afin de rendre votre entreprise vraiment sûre, il est important de commencer par une préparation minutieuse. Savez-vous où se cache le danger, sur quels appareils vos collaborateurs travaillent , si ces appareils sont sécurisés et quelles données de l'entreprise sont les mieux protégées ? Vous hésitez ? Préparez un plan d'action et obtenez une meilleure vision de votre infrastructure informatique et de vos données critiques en mettant en place :

- → **une analyse approfondie des risques à tous les niveaux de votre système IT;**
- → **une analyse des vulnérabilités : recherchez le talon d'Achille de votre système IT;**
- → **un plan stratégique de gestion des risques : quelles solutions et stratégies mettre en place pour éviter une menace potentielle ?**

ÉTAPE 02

Protection des actifs de l'entreprise

Vous avez passé au crible l'ensemble de votre infrastructure informatique, vous connaissez les faiblesses et vous savez où elles se trouvent. Il est temps de vous protéger efficacement :

SÉCURISER L'ACCÈS AU RÉSEAU ET AU SYSTÈME

Limitez l'accès aux processus et réseaux critiques de l'entreprise et n'autorisez que les utilisateurs autorisés. Vous évitez ainsi que des personnes non autorisées accèdent aux données sensibles de l'entreprise ou aux systèmes, ce qui rend l'accès à votre infrastructure informatique plus difficile pour les pirates informatiques. Quelques exemples connus sont les pare-feu, les VPN, la confiance zéro et l'authentification multifactorielle.

CRYPTER LES DONNÉES ET STRATÉGIES DE SAUVEGARDE

Vous avez tout de même été piraté ? Avec une politique de cybersécurité solide, ce n'est pas forcément la fin du monde. Le cryptage des données rend vos données professionnelles sensibles illisibles pour les personnes non autorisées, même si les données sont interceptées. Avec des sauvegardes automatisées, vous restaurez vos données immédiatement au point où elles se trouvaient avant le crash ou l'attaque.

SENSIBILISER ET FORMER VOS COLLABORATEURS

Vos collaborateurs sont-ils formés à la détection et à la prévention des cyberdangers potentiels ? Organisez des coachings afin que votre équipe reste au courant des derniers développements, des applications et des solutions en matière de cybersécurité. Dans ce blog, vous découvrirez l'importance du travail d'équipe au sein d'une entreprise très avancée en termes de cybersécurité.

ÉTAPE 03

Détection des infractions

Des solutions informatiques intégrées, comme l'apprentissage automatique et l'IA, analysent les nombreuses notifications de sécurité et veillent à ce que seules les notifications pertinentes soient visibles. Les dangers potentiels sont donc détectés plus rapidement et plus efficacement. Optez pour des outils qui surveillent votre infrastructure informatique 24h/24, signalent les actions suspectes et y mettent fin rapidement :

- → **mise en place d'outils de surveillance et de détection qui surveillent votre infrastructure informatique 24h/24 et détectent immédiatement les actions suspectes ;**
- → **mise en place d'un Centre des Opérations de Sécurité (SOC) ;**
- → **utilisation de services MDR (Managed Detection and Response).**

ÉTAPE 04

Réagir aux incidents

Vous avez été piraté, que faire ? Il est important de réagir rapidement afin que tous les membres de votre organisation sachent ce qu'il faut faire ou ne pas faire :

- → **Créez un plan d'intervention en cas d'incident afin que votre personnel puisse immédiatement passer à l'action.**
- → **Communiquez de manière transparente avec vos collaborateurs et les parties prenantes.**
- → **Rédigez un rapport détaillé de l'incident, les conséquences et les mesures mises en place. Cela permet de mieux comprendre la situation, d'identifier les points sensibles et d'éviter les attaques à l'avenir.**

ÉTAPE 05

Rétablissement après une cyberattaque

Reprendre vos activités immédiatement après une cyberattaque ? Implémentez un plan stratégique de reprise après sinistre afin de lancer immédiatement les systèmes de sauvegarde et les procédures de reprise. Ce faisant, n'oubliez pas de fixer des objectifs de récupération :

- → **Quel est votre Recovery Time Objective (RTO) soit la durée maximale pendant laquelle un processus d'entreprise peut être hors ligne ?**
- → **Quel est votre Recovery Point Objective (RPO) soit la quantité maximale de données susceptibles d'être perdues, mesurée en temps ?**

Élevez le niveau de cybersécurité de votre entreprise avec Telenet Business

Vous cherchez un partenaire pour élaborer votre plan de cybersécurité ?
Prenez contact avec l'un de nos experts.

Contactez nous

Business