
cyberglobal

Les chiffres

60 % des TPE et PME qui font l'objet d'une cyber-attaque majeure déposent le bilan dans les 6 mois.

La sécurité du système informatique des petites et moyennes entreprises **ne fait pas partie des priorités des chefs d'entreprises.**

Le **pourcentage des attaques** vers les entreprises de moins de 250 salariés progressent. Il passe de **18% à 31% en 4 ans**.

COVID 19, Télétravail.
La plateforme publique cybermalveillance.gouv.fr, qui aide entreprises et particuliers à se défendre face aux attaques informatiques, a vu sa fréquentation **augmenter de plus de 300 %** depuis le confinement.

S'introduire dans un réseau d'entreprise peut prendre entre 30 mn et 10 jours (4 jours en moyenne).
Avec un taux de « réussite » de 93%.

En 2019, 47% des entreprises de moins de 50 collaborateurs ont été touchées par un cyber-incident.

En France, le **coût moyen** des cyberattaques des TPE s'élève à 50 000 € contre 10 000 € en 2019, soit une augmentation de 400% !

Idées reçues

- ✓ La mise en place d'un anti-virus et les sauvegardes régulières des données sont suffisantes pour se protéger.
- ✓ Les cybercriminels ne s'attaquent qu'aux grandes entreprises.
- ✓ En cas de défaillance de mon système informatique, mon prestataire informatique rétablira rapidement la situation.
- ✓ On ne peut pas imposer à tous les collaborateurs des règles de sécurité strictes.

L'impact d'une panne informatique sur mon business est maîtrisé.
Un arrêt de quelques jours de mon informatique ce n'est pas un drame.
On n'a jamais été piraté alors pourquoi aujourd'hui ?

Il n'est plus question de se demander **"Si"** votre entreprise va subir une cyber-attaque mais bien **" Quand"** celle-ci va se produire et si vous avez **anticipé ce risque**.

Françoise - Cheffe d'entreprise

« Comme tout le monde j'entends parler dans les médias de sociétés qui ont été piratées. Pour moi c'était un sujet abstrait, loin de mes préoccupations.

Un ami chef d'entreprise m'a confié avoir été victime d'une cyberattaque. Le logiciel de facturation bloqué, avec à la clef une demande de rançon.

On se connait depuis longtemps c'est un type solide un « vrai patron », mais là il était désemparé, il ne savait pas comment gérer la situation, vers qui se tourner. »

Vincent – DAF

« Le budget informatique augmente tous les ans. Matériel à remplacer, renouvellement des abonnements Internet et de téléphonie, les licences, sans parler des contrats de services avec les prestataires informatiques et Télécom à renégocier.

Je budgétise tous les postes de dépenses, mais en cas de cyber attaque, qu'est-ce que l'on a prévu ? qui va protéger l'entreprise ? »

Sylvie – DRH

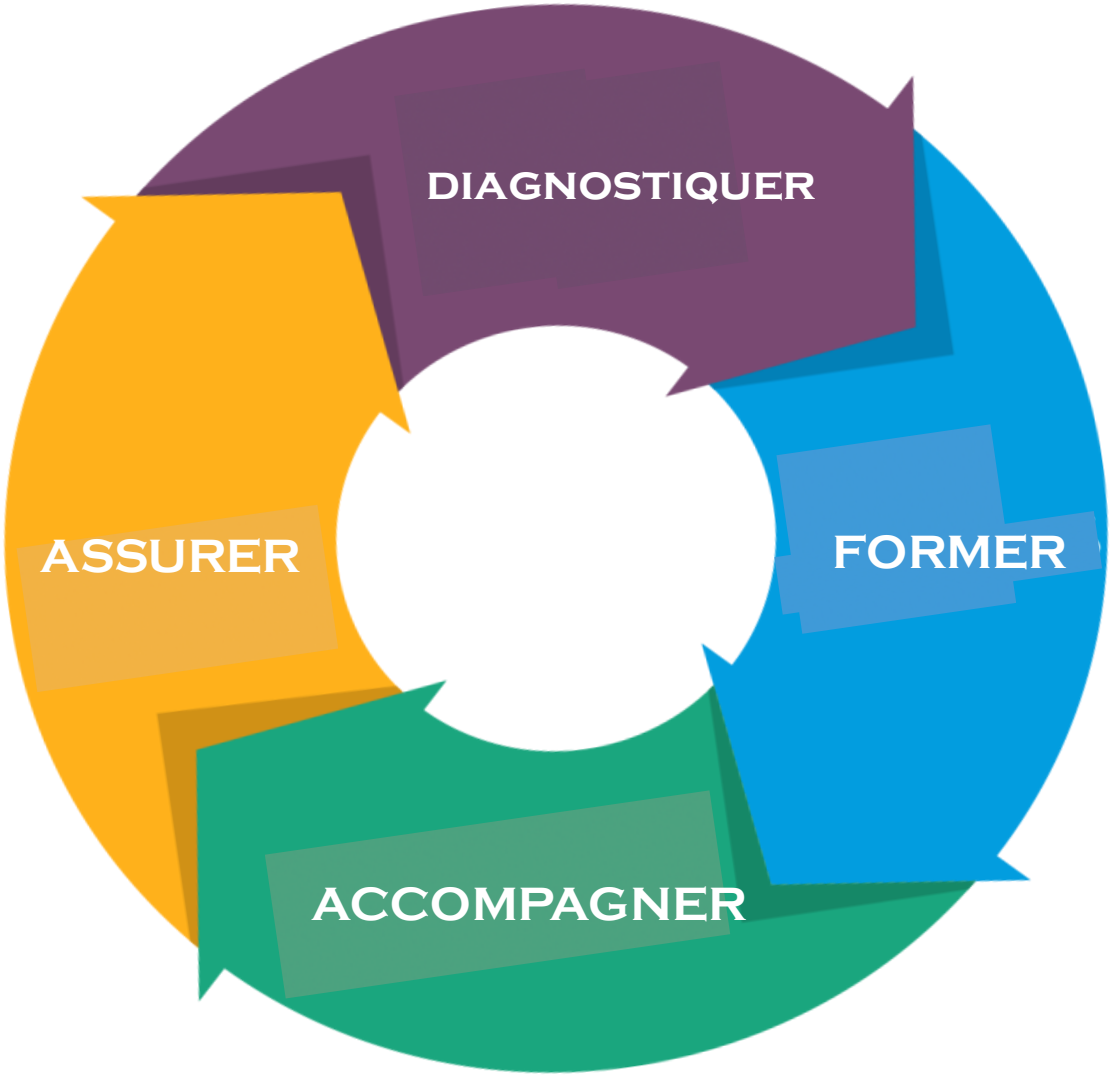
« Le confinement nous a imposé de réorganiser le travail, et comme beaucoup d'entreprises nous n'étions pas prêts. Il a fallu dans l'urgence renvoyer des salariés chez eux sans même savoir s'ils avaient une connexion Internet correcte.

On pensait que cela allait durer quelques jours, avec le recul je me rends compte que l'on a très mal géré par manque d'anticipation. »

cyberglobal

NOTRE engagement = VOTRE Cyber-résilience

Identifier les défaillances technologiques, humaines et process afin de limiter les risques pour votre entreprise, vos clients, en matière de réputation, perte de productivité, perte financière



COMPRENDRE, POUR ANTICIPER

En dressant une cartographie complète de votre système d'information, et de l'environnement dans lequel vous évoluez.

Au-delà des performances de votre SI, nous identifions vos usages, vos enjeux métiers, vos points de crispations, et vos attentes en terme de pilotage.

Les conclusions de notre diagnostic sont sans concession. Elles vont en toute objectivité mettre en avant les points de conformité et aussi de non-respect des règles essentielles de sécurisation et d'intégrité de votre «patrimoine numérique».

ACCOMPAGNER, POUR METTRE EN OEUVRE

Nous allons mettre en pratique les recommandations qui font suite aux conclusions du diagnostic.

Ensemble nous traitons au sein de votre entreprise, des sujets aussi nombreux que variés, comme la sécurisation physique des sites, la sécurisation des équipements informatiques, le maintien opérationnel des services numériques, les process IT, et les moyens de contrôle et de pilotage.

FORMER, POUR FEDERER

Adhérer au changement demande à chaque collaborateur un effort d'adaptation, d'intérêt, d'envie de mieux faire.

La maîtrise des outils assure à vos collaborateurs la capacité d'appliquer les bonnes pratiques dans toutes les situations, au bureau, en nomadisme, en télétravail,…

Chacun doit s'accaparer les outils, les procédures, afin de garantir un haut niveau de sécurisation de votre SI.

CONTRÔLER, POUR PILOTER

La sécurité est une démarche de remise en question permanente, un cercle vertueux d'excellence.

C'est à cette seule condition que l'on peut tenir l'engagement d'avoir tout mis en œuvre pour assurer l'intégrité et la pérennité des outils numériques.

ASSURER L'IMPREVU

Parce que malgré toutes les bonnes volontés mobilisées et tous les moyens mis en œuvre, le 100% sécurité ne peut jamais être garanti. Il faut se préparer à ce que vos services soient interrompus ou que votre outil de production soit stoppé.

Terrible situation où vous aurez besoin d'un **appui financier** pour remettre l'entreprise en ordre de marche.

Au final, vous bénéficiez de toutes les garanties de continuité de vos activités et vous restez concentré sur votre cœur de métier.

CYBER Protégés – CYBER Accompagnés – CYBER Assurés.

« Et vous le resterez. »

Un diagnostic à 360° de votre société, afin d'évaluer votre exposition aux cyber risques.

Un plan d'action concret avec des mesures correctives immédiates pour protéger votre entreprise.

Un accompagnement avec la mise en œuvre d'un plan de Sécurisation de votre Système d'Information à 2, 4 et 8 mois et un parcours de formation de vos collaborateurs.

Des outils financiers pour protéger la potentielle perte de productivité de votre entreprise.

MERCI POUR VOTRE ATTENTION

CYBERGLOBAL
826, Grande rue
01700 Miribel
@ contact@cyberglobal.fr
w cyberglobal.fr