notre agilité d'esprit,
clef de votre réussite

witkey

Conseil et accompagnement en cybersécurité

Liée à l'évolution du numérique, la cybersécurité au sein de l'entreprise n'est plus que technique : elle est stratégique, c'est désormais un sujet de haut management.

À partir du moment où une entreprise utilise un système d'information, elle est **soumise à la menace des cyberattaques** et ce peu importe sa taille ou son secteur d'activité. À l'instar d'une explosion ou d'un tremblement de terre, elle doit alors affronter les conséquences à court et moyen termes d'une cyberattaque.

À court terme

- Pertes d'exploitation, de données, des clients....
- Coûts liés à la gestion de le crise informatique, de la communication, juridiques....

À moyen et long termes

- Coût de reconstruction et de correction (peuvent monter jusqu'à 15 % du budget de la DSI)
- Activité en mode dégradé : dysfonctionnent interne, conduite de changement plus complexe, audits complémentaires...
- Impact sur l'image dans le temps à suivre : révélation dans les médias, impacts dûs aux changements organisationnels internes, perte de confiance des clients...
- Coûts liés aux conseils, suite des affaires judiciaires / juridiques, éventuelles amendes...

> *Être protégé est indispensable, mais il est tout aussi important d'être prêt à affronter une attaque. La préparation de vos équipes face à la menace fait partie intégrante de votre stratégie de protection."*
>
> **Christian Martin**
> Dirigeant wITkey

> ***Security is always seen as too much until the day it's not enough."***
>
> **William H. Webster**
> Ex-directeur du FBI
>
> *« La sécurité est toujours considérée comme excessive, jusqu'au jour où elle ne suffit pas. »*

Notre approche stratégique et opérationnelle

- Accompagnement de la Direction Générale à la formalisation de la stratégie cybersécurité
- Réalisation de l'état des lieux face au risque cyber
- Prise en compte du risque cyber dans la gestion de crise, les PCA et PRA
- Analyse de risque cyber
- Accompagnement du RSSI dans ses missions
- Rédaction des documents de politique et de procédure

Notre accompagnement ponctuel

- Sensibilisation aux risques cyber
- Exercice de gestion de crise cyber
- Exercice technique de montée en compétence de l'équipe sécurité
- Exercice d'entraînement de SOC

NOTRE PHILOSOPHIE

Vous rendre *autonomes* grâce à une *approche structurée* par étapes.

Découverte → *État des lieux* → *Restitution* → *Plan d'actions* → *Mise en œuvre* → *Bilan* → *Serious Game*

Quelques chiffres clefs*

58 %
DES ATTAQUES SONT OPPORTUNISTES ET NE VISENT PAS UNE ENTREPRISE EN PARTICULIER

27 %
SOIT MOINS D'UN EMPLOYÉ SUR 3 A DÉJÀ REÇU DES INSTRUCTIONS DE SON EMPLOYEUR (TPE/PME) SUR LES MESURES DE SÉCURITÉ À PRENDRE POUR TRAVAILLER DEPUIS DES APPAREILS PERSONNELS

6
MOIS, C'EST LE TEMPS QU'IL FAUT EN MOYENNE À UNE ENTREPRISE POUR DÉTECTER UNE VIOLATION DE SES DONNÉES

43 %
DES CYBERATTAQUES VISENT LES PETITES ENTREPRISES

41 %
DES ENTREPRISES N'ONT PAS DE PLAN D'URGENCE À ACTIVER EN CAS DE CYBER ATTAQUES

6
ENTREPRISES SUR 10 N'ONT PAS ALLOUÉ OU TRANSFÉRÉ DE BUDGET SPÉCIFIQUE POUR LUTTER CONTRE LA FRAUDE ET LA MENACE CYBER

* *Extrait de l'essentiel de la sécurité numérique pour les dirigeants et dirigeantes- Édition n°2— Avril 2021*

witkey
8 rue des Frères Caudron, 78140 Vélizy-Villacoublay
01 34 63 01 37 - contact@witkey.fr