VOUS AUSSI PRENNEZ LE RISQUE DE RÉUSSIR !

RISK@ CYBER

www.riskattitude.net

A PROPOS DE **RISKATTITUDE**

Riskattitude a été créé en 2010 par son fondateur David Museur, après 5 ans de réflexions et d'études approfondies sur la faisabilité et la durabilité de cette entreprise dans le temps. En l'espace de Quinze années dédiées à l'analyse et à la maîtrise des Risques Opérationnels et Aléatoires, son gérant et fondateur David Museur a acquis de nombreux diplômes qui lui ont permis d'obtenir de solides connaissances des risques d'entreprise, technologiques et environnementaux.

81 %

des entreprises françaises ont été visées par une cyberattaque en 2015

NOS VALEURS

Nos trois valeurs servent à orienter nos actions et notre comportement qui caractérisent en propre l'identité de Riskattitude.
Elles sont le fruit d'un ambitieux projet réfléchi depuis 5 ans et sont régulièrement réactualisées.
Elles permettent, entre autres, de rendre Riskattitude unique dans son mode de fonctionnement.

NOS INNOVATIONS

RiskAttitude cultive un état d'esprit orienté vers la recherche, l'amélioration continue et les processus d'innovation globale pour ses parties prenantes et ses clients. Nos valeurs d'innovations, de réactivité et de loyauté servent à orienter nos actions et notre comportement. Cet état d'esprit caractérise en propre et rend unique l'identité de RiskAttitude. Nous formalisons mensuellement nos rencontres et développement par notre site internet et grâce à une newsletter mensuelle.

60 %

des victimes ne maintiennent pas leurs activités après une cyber attaque

48 %

des incidents de cybersécurité ont été générés – malgré eux – par des collaborateurs

AVANT LE **SINISTRE**

TEST **HACKING**

TEST BLANC

Dans le « Test blanc », l'attaquant ne connaît rien de la structure de l'entreprise. Il va devoir utiliser des méthodes d'identification des portes d'entrées de votre système.

Exemple : Phishing, NMap, Envoi de mail, etc

TEST GRIS

Dans le « Test gris », l'attaquant possède certaines informations qui lui permet d'entrer dans le système de votre entreprise. Il connaît donc une partie de l'architecture à cause d'une fuite de données, d'un acteur interne ou externe à votre entreprise, etc..

Exemple: un ancien employé, agent de maintenance, etc..

TEST NOIR

Le « Test noir » est la pire attaque cyber qui pourrait arriver. En effet, dans ce cas, l'attaquant connaît toute l'architecture de l'entreprise ou il est directement sur place et relié à votre système.

Exemple : un employé, un prospect, un client, un agent de maintenance etc..

AVANT LE
SINISTRE

CYBER AUDIT

Un audit cyber est une phase d'immersion totale dans l'entreprise pendant quelques jours, avec la réalisation d'interviews des acteurs internes et une inspection de l'établissement, des éléments informatiques et du réseau. Celui-ci permet d'identifier les principales menaces pour l'entreprise.

Nous détectons et proposons des recommandations pour réduire au maximum les risques cyber et fraude dans votre entreprise. Nous réalisons ensuite des tests hacking sur une durée de 6 mois aléatoirement pour s'assurer que les menaces et les risques sont limités.

Les grandes étapes :

- Pré-diagnostic des risques grâce à un « Test blanc »,
- Identification des vulnérabilités grâce la visite sur site,
- Réalisation d'un audit avec proposition de recommandations,
- « Test gris » et « Test noir » sur 6 mois après l'audit.

AVANT LE **SINISTRE**

CYBER **ASSURANCE**

Une cyber assurance est devenue aujourd'hui l'une des seules solutions pour faire face aux conséquences causées par une cyber attaque.

60% des entreprises ferment leurs portes après avoir subi une cyber attaque. Avec la mise en place d'une cyber assurance, le risque de l'arrêt définitif de vos activités est considérablement réduit, votre entreprise est protégée en cas d'attaque.

Avantages

Grâce à une cyber-assurance vous serez certain d'être protégé face à un risque fréquent et souvent très grave.

Coût

Plus le risque cyber est bien géré mois le coût sera élevé.

Nous pouvons vous aider à souscrire l'assurance qui correspond au mieux à vos besoins.

Comment ?

En supprimant ou en limitant tout d'abord les risques les plus importants pour remplir les conditions d'éligibilité à la souscription d'une cyber assurance.

En démontrant ensuite que votre entreprise maîtrise le risque de cyber attaque sur le long terme.

AVANT LE **SINISTRE**

NOS **FORMATIONS**

Cyber réflexe

Cyber fraude

Cyber initiation

APRÈS
LE SINISTRE

Les conséquences d'une cyber attaque sont souvent désastreuses. Que ce soit d'ordre financier, commercial ou psychologique, une cyber attaque vous laisse sans défense.
Ne restez pas tout seul ! Demandez de l'aide est la meilleure solution pour vous en sortir.

CONTRÔLE DES DÉGATS

La première étape consiste à contrôler les dégâts subis et d'établir le plus rapidement un plan de défense pour arrêter les dommages. Cette démarche peut être réalisée par téléphone, dans les minutes suivant l'attaque.

La deuxième étape consiste à venir sur place et à établir une plan de reprise d'activité pour revenir le plus vite possible à la normal. L'origine de l'attaque sera identifiée et traitée.

773 000 €

Une étude auprès de 1000 dirigeants révèle qu'une cyberattaque coûte en moyenne 773 000 euros à une entreprise.

NOS ETAPES

CONTRÔLE
DES DÉGATS

ETABLISSEMENT
PLAN DE CRISE

AUDIT
D'AMÉLIORATION

ÉTABLISSEMENT D'UN **PLAN DE GESTION DE CRISE**

Etablir un plan de gestion de crise est primordial lorsque l'entreprise est connue médiatiquement ou qu'elle possède des données sensibles. En effet, vous pouvez perdre l'ensemble de vos clients à la suite d'une attaque si vous n'avez pas préparé votre communication en amont.

AUDIT D'AMÉLIORATION

Lorsque l'entreprise est stabilisée, un audit cyber est nécessaire pour garantir le maintien de cette stabilité et éviter de nouvelles attaques. Une entreprise attaquée a 75% de chances de se faire attaquer à nouveau.

Une phase d'immersion est nécessaire pour identifier tout les risques. Nous proposerons à la fin de cette phase d'immersion un plan d'amélioration avec des recommandations à mettre en place.

400 avenue roumanille
06906 Sophia Antipolis

(+33) 4 93 00 87 44
(+33) 6 08 64 65 42

commercial@riskattitude.net
www.riskattitude.net