Assurance et Banque

Prévention Cybersécurité

Risque Cyber

Informer Alerter

Évaluer Aider

> Risque Cyber

Le risque Cyber

49 % **des entreprises ont subi une cyberattaque avec impact significatif au cours de l'année 2023[1].**

(1) source : Cesin.fr

Quelles conséquences pour votre entreprise ?

Les conséquences de cette cybercriminalité peuvent être tout aussi importantes que les conséquences de risques traditionnels, tels qu'incendie, événements naturels.

Des pertes financières

Une cyberattaque peut provoquer l'arrêt partiel de votre activité conduisant à une perte de chiffre d'affaires, voire un arrêt définitif de votre activité.

Des pertes immatérielles

Une cyberattaque peut conduire à la perte partielle ou totale de vos données/fichiers informatiques au centre de votre activité.

Des risques de mise en cause de votre responsabilité

Des réclamations de tiers au titre de votre responsabilité civile peuvent être engagées, notamment si votre entreprise détient des données sensibles ou personnelles de vos clients (données médicales, numéros de carte bancaire…).

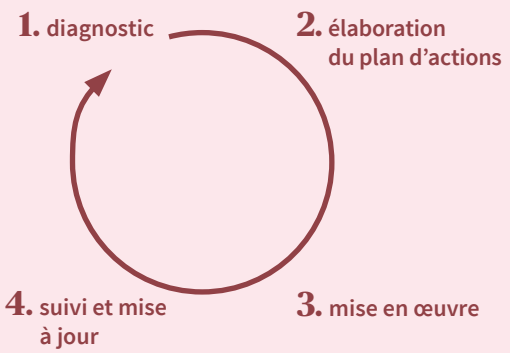
Des atteintes à votre réputation

La réputation de l'entreprise peut être dégradée, entraînant une perte de confiance de votre clientèle.

De par leur transformation digitale, les entreprises sont aujourd'hui confrontées aux risques cyber, tels que :

- la malveillance informatique : introduction de virus, accès illicite à des données personnelles ou sensibles, cryptologiciel, attaques par déni de service, intrusion numérique non autorisée en vue de détourner des données ou des fonds, hameçonnage (phishing).
- les accidents informatiques involontaires notamment dus à des erreurs humaines : divulgation involontaire de données personnelles, suppression de données / fichiers informatiques.

Une démarche par étape



> Vous informer et vous alerter

Conseils de prévention

Essentiels pour réduire l'exposition aux risques Cyber dans votre entreprise

À l'ère du « tout digital » , le taux de cybercriminalité n'a jamais été aussi élevé et les moyens mis en œuvre pour développer les actes de cyberattaques sont aujourd'hui considérables.
Si les cyber hackers innovent constamment, un certain nombre de règles élémentaires permettent de diminuer les risques !

Nos recommandations

Les incontournables

S'équiper de **pare-feu** et d'**antivirus** de qualité.

Mettre régulièrement à jour les logiciels (patchs de sécurité pour tous les systèmes d'exploitation).

Mettre en place des **sauvegardes régulières** et tester les restaurations.

Utiliser des mots de passe personnels et complexes.

Sensibiliser et former régulièrement les collaborateurs.

Ce sont des moyens élémentaires pour limiter les risques de perte des données importantes de votre entreprise.

Pour renforcer son dispositif de prévention / protection

- **Les systèmes de détection des intrusions**

Ce sont des solutions de protection qui ont pour objet, selon les cas, d'analyser en continu :

> le comportement des téléchargements ayant passé vos antivirus et à bloquer les éventuelles actions malveillantes ou suspectes,

> le trafic sur les accès réseau de votre entreprise et à bloquer les accès suspects.

Ils peuvent également permettre de sécuriser vos connexions à distance.

- **Les Plans de Reprise et de Continuité d'Activité (PRA/PCA)**

Ce sont des dispositifs de planification et de management des situations de crise ayant pour objectif d'atténuer les conséquences sur l'activité d'un risque cyber qui s'est réalisé.

C'est arrivé

- Des hackers récupèrent sur les réseaux sociaux professionnels l'identité de M. X, dirigeant d'entreprise, afin de se faire passer pour lui par mail auprès de ses collaborateurs. Le mail frauduleux, qui contient en pièce jointe, un logiciel malveillant (malware) est ouvert par un des salariés. Cette ouverture entraîne l'intrusion dans le système informatique permettant ainsi aux hackers d'accéder aux données comptables et de détourner 100 000 € en modifiant les coordonnées IBAN de RIB.

> Coût total du sinistre : **105 000 €**

Boîte à outils

- Fiche Détecter Protéger Alerter
- Fiche Réglementation GDPR
- Brochure FFA
- Vidéo PCA AXA
- Guide des bonnes pratiques de l'utilisation du SI

En savoir plus sur notre site **axa.fr**
et sur : Hack Academy
ANSSI
MOOC SecNumacadémie

> Évaluer vos risques et vous accompagner

L'aide de votre interlocuteur AXA

Vous bénéficiez de démarches de prévention adaptées à vos besoins et de l'accompagnement d'experts pour vous aider à réduire le risque cyber dans votre entreprise.

Pack de base

Inclus dans votre contrat d'assurance AXA.

Faites un point sur l'exposition au risque incendie de votre entreprise et identifiez les premiers axes de progrès.

La charte prévention

Disponible sur demande à votre interlocuteur AXA, vous bénéficiez de :

- **Conseils et outils (documents et vidéos)**
- **Bonnes pratiques**
- **Supports de sensibilisation/formation**
- **Liens Web**

Accompagnement Prévention

Nos experts prévention AXA à vos côtés

Pour optimiser votre démarche prévention, vous pouvez bénéficier d'un diagnostic préliminaire de votre exposition aux risques cyber selon votre activité.

Basé sur un questionnaire ou le cas échéant sur un bilan plus complet, ce diagnostic préliminaire permet :

- **d'identifier les risques,**
- **d'évaluer les forces et faiblesses de votre organisation,**
- **de vous proposer des actions d'amélioration par le biais de conseils.**

Option Expert Prévention

Compléter l'accompagnement avec l'option Expert Prévention

Nos experts vous accompagnent par une démarche coopérative et pédagogique d'analyse, de qualification, et d'amélioration de vos risques cyber, adaptée à l'activité opérationnelle de votre entreprise :

- **évaluation, analyse de risques et suivi de plans d'action,**
- **état de situation ISO 27002,**
- **action de sensibilisation/formation,**
- **conseil en architecture informatique,**
- **réalisation de tests d'intrusion infrastructure ou web,**
- **pour certaines configurations, réalisation d'un contrôle de présence de menaces avancées persistantes (APT ou « Advanced Persistant Threat »).**

Les + AXA

Assistance en ligne

Un numéro de téléphone dédié Cyber Secure et disponible 24h/24 7j/7.

Pour déclarer vos sinistres et bénéficier de notre réseau d'experts.

Crise majeure

Une équipe de spécialistes, présente aux côtés de vos clients dans un moment crucial pour un service adapté et disponible 24h/24, 7j/7.

En savoir +

PCA

Un accompagnement pour limiter les conséquences d'un sinistre majeur sur l'activité de l'entreprise.

En savoir +

E-réputation

Des sociétés partenaires qui peuvent s'occuper du nettoyage / noyage de propos diffamatoires sur le Web.

En savoir plus sur notre site **axa.fr** et sur :

Hack Academy
ANSSI

MOOC SecNumacadémie
Nous vous recommandons les modules :

2 • « Un monde à hauts risques » sur les différents types d'attaques
4 • « Protéger le cyber espace » sur les règles pour limiter les attaques
5 • « Les règles d'or de la sécurité » relatives aux données et responsabilités.

AXA vous répond sur :

OFFRE CITOYENNE

CONFIANCE, PRÉVENTION, ENVIRONNEMENT, SOLIDARITÉ :
avec AXA, faites le choix d'une entreprise engagée. Nos offres citoyennes contribuent au respect de la planète, de tous et de chacun. Toutes nos actions concrètes sont à découvrir sur **axa.fr**

Réf : 2004884 02 2024 - Illustrations : AdobeStock