Guide Cybersécurité

La responsabilité du Dirirgeant

Quietic Expert Cyber

Sommaire

Dirigeant, c’est vous le responsable !

Cyberattaque, quelles consequences ?
En voici quelques unes :

- Perte financière, arrêt de production
- Atteinte à l’image
- Responsabilite juridique !

En cas de fuite de données, la responsabilité personnelle du dirigeant peut être engagée

01

Fuite de données

Les conséquences inattendues

Fuite de données, les sanctions

ENTREPRISE

La CNIL sanctionne lourdement les personnes morales

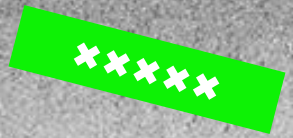
le montant des sanctions peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial.

DIRIGEANT

C'est votre responsabilité pénale qui peut être mise en cause

5 ans d'emprisonnement et 300 000 euros d'amende

Vous êtes responsable, dans quels cas ?



- Défaut de mise en place de mesures de sécurité proportionnées au risque
- Traitement non autorisé des données sensibles
- Transfert de données non prévues par la loi hors Union Européenne
- Conservation de données au-delà de la durée autorisée, etc

source : #RGPD : quelle(s) responsabilité(s) du dirigeant ? - HAAS Avocats (haas-avocats.com)

Responsable par Négligence ?

La notion de « négligence » n’implique pas seulement la responsabilité propre du dirigeant mais le rend également responsable du comportement d’un salarié étourdi ou non formé sur le sujet !

02 Qui peut porter plainte contre vous ?

Les actionnaires	Les associés	Les Autorités	Les victimes
• Pour le préjudice subi par l'entreprise • Pour leur préjudice personnel	• Ou autres dirigeants	• Les autorités de contrôle • Le Ministère Public	• Les victimes de fuite de données • Cela peut être vos propres salariés
Plainte pénale			

Source : tipstrickscyberscuritepisode4-responsabilite-du-dirigeant.pdf (bakermckenzie.com)

Ce que l’on peut vous reprocher

Négligence

Négligence et insuffisance de préparation de l’entreprise

Manquement

Manquement à l’obligation de s’assurer de la sécurité des données

Défaut

Défaut de notification de la violation de données aux autorités de contrôle et aux personnes concernées

Il importe donc de bien se protéger, non seulement pour être en conformité avec la loi

mais également pour protéger son business

03 Limiter les dégâts

Former

Tous les collaborateurs

Mesures de protection

L’essentiel à avoir

Faire appel à un expert

Externaliser la gestion informatique

La cyberassurance

MFA et EDR peuvent réduire la prime

Former les employés

78%

des employés

sont au courant des risques de liens malveillants dans les emails mais cliquent quand même dessus

52%

des entreprises

ne savent pas quoi faire en cas d'incident cyber

70%

de réduction

des risques liés à la cybersécurité quand les entreprises investissent dans une formation pour leurs employés

Source : notre partenaire usecure

Mesures de sécurité essentielles

- Sécuriser les postes de travail (antivirus, EDR…)
- Sécuriser les éléments réseau (pare-feu…)
- Mettre à jour les systèmes et logiciels
- Sauvegarder régulièrement, et tester la restauration
- Opter pour la double authentification (MFA)
- …

Consultez la fiche réalisée par Cybermalveillance

Les 10 mesures essentielles pour assurer votre cybersécurité - Assistance aux victimes de cybermalveillance

Externaliser

Pourquoi travailler avec un prestataire externe ?
Le spécialiste est confronté à toutes sortes de situations. Pour bien le choisir, privilégiez la proximité, et le conseil. C’est mieux s’il comprend votre réalité.

Cyberassurance

Parmi les outils de prévention, deux sont des conditions souvent sine qua non des contrats d'assurance car elles permettent **de réduire jusqu'à 80% les risques cyber :**

MFA

La double authentification est la méthode privilégiée pour lutter contre le phishing ou les usurpations d'identité.

EDR

permet de détecter les menaces sur les postes clients et d'automatiser une réponse, avec l'envoi d'alertes ou l'impossibilité d'exécuter un programme

Le fait d'effectuer régulièrement des **simulations de phishing** est en passe de devenir obligatoire pour souscrire une cyberassurance.

En résumé

Dirigeant, votre responsabilité personnelle peut être engagée.

Le manque de sécurité informatique peut vous être directement reproché, et risque de nuire gravement à votre entreprise, vis-à-vis de vos clients et partenaires.
Les sanctions peuvent être très lourdes, mais il est possible d'agir en amont.

Quietic est un MSP (Manged Service Provider) - labellisé Expert Cyber

Vous souhaitez en savoir plus sur nos services ?

Contactez-nous : contact@quietic.fr