99 ADVISORY
A clever transformation

COMMENT RÉPONDRE AUX ATTENTES RGPD DE LA CNIL FACE AUX CYBER-ATTAQUES ?

CONTEXTE GÉNÉRAL

En 2018, **80% des entreprises ont subi au moins 1 cyber-attaque** et 48% d'entre elles ont subi au moins 4 cyber-attaques.[1]

[1] Étude réalisée par OpinionWay auprès de 174 membres du CESIN.

Trop d'entreprises restent exposées au danger. En effet, près de

59% d'entre elles se déclarent **« pas prêtes »** ou **« pas du tout prêtes » à faire face** à une cyber-attaque de grande ampleur.[1]

Pendant le confinement, le recours généralisé au **télétravail offre une surface d'attaque** bien plus grande aux pirates informatiques.

Des **impacts très négatifs** sur les entreprises visées[2] :

26% Ralentissement de la production

23% Indisponibilité du site web

12% Retard sur la livraison

11% Perte de CA

9% Arrêt de la production

[2] Pourcentage d'entreprises touchées par l'impact cité.

ATTENTES ET RISQUES

En cas de cyber-attaque, l'entreprise doit se référer aux **articles 33, 34 RGPD** et **respecter les attentes de la CNIL**. Plusieurs contraintes :

- Nombreux documents à collecter
- Évaluations précises
- Délais très courts
- Peu d'informations au cas par cas

Les établissements attaqués font face à **de nombreux risques** :

Vis-à-vis des clients :
Risque de réputation
Perte de confiance
Communication de crise

Vis-à-vis des autorités :
Risque de sanctions lourdes

Entre mai 2018 et janvier 2019, les régulateurs européens ont infligé plus de **114 millions d'euros d'amendes** pour violation du RGPD dont 50 millions d'euros à l'encontre de Google.

ACCOMPAGNEMENT

Afin de répondre au mieux aux attentes RGPD de la CNIL face aux cyber-attaques, 99 Advisory accompagne ses clients en :

1. Production conforme de normes internes
2. Gestion de la relation CNIL
3. Analyse des risques
4. Production conforme de notifications
5. Création de registres de violation

Contactez-nous !