Info-Flash Social

Vendredi 23 octobre 2026
Numéro 2026 – SOC 42

⇒ Cyberattaque : quel impact sur les salariés ?

Une entreprise victime d'une cyberattaque peut voir son activité gravement perturbée. Elle peut avoir des conséquences directes sur l'organisation du travail, la protection des données des salariés et les obligations de l'employeur. Quels réflexes adopter ?

- **Informer rapidement les salariés**

Les salariés doivent être informés de l'existence de l'incident, des éventuelles perturbations d'activité, des consignes de sécurité à appliquer, des interlocuteurs à contacter en cas d'anomalie.
L'employeur doit diffuser des consignes simples afin de limiter l'aggravation de l'attaque notamment ne pas ouvrir les courriels suspects, signaler toute activité inhabituelle, respecter les consignes du service informatique, etc.

- **Protéger les données personnelles des salariés**

Lorsque des données RH sont exposées (coordonnées, RIB, bulletins de paie, données de santé, etc.), l'entreprise doit évaluer le risque pour les personnes concernées et les en informer.

- **Réorganiser l'activité**

➢ L'employeur peut **renvoyer les salariés chez eux** sans mettre en place un dispositif juridique spécifique (activité partielle, télétravail, etc.). Dans ce cas, la situation est en principe imputable à l'entreprise. Le contrat de travail n'est pas suspendu de plein droit et la **rémunération reste due** tant que le salarié se tient à la disposition de l'employeur et que l'empêchement ne lui est pas imputable.

Dans ce cas, l'employeur peut recourir à la récupération des heures perdues si l'interruption de travail est collective (totalité de l'entreprise ou un service, un atelier, etc… lorsque les salariés concernés forment une collectivité de travail à part entière). *Voir notre Juri-Métal sur le sujet.*

➢ L'employeur peut mettre en place le **dispositif d'activité partielle**. Une cyberattaque paralysant totalement ou partiellement l'outil de travail peut être qualifiée de « circonstance de caractère exceptionnel » au sens des textes sur l'activité partielle, au même titre qu'un sinistre ou certaines crises (comme cela a été admis pour la crise sanitaire).
Sur la procédure de mise en place de l'activité partielle, voir notre Juri-Métal sur le sujet.

➢ L'employeur peut mettre en place le **télétravail** unilatéralement, sans l'accord préalable du salarié. Une cyberattaque majeure peut constituer des circonstances exceptionnelles, ou un cas de force majeure, rendant nécessaire un aménagement du poste de travail pour permettre la continuité de l'activité et garantir la protection des salariés.

➢ L'employeur peut organiser temporairement une **réaffectation** des salariés à d'autres tâches ne nécessitant pas l'usage du système d'information attaqué (activités manuelles, formation, mise à jour documentaire, procédures papier, etc.), sous conditions.

➢ En complément ou en alternative, l'employeur peut, sous réserve des règles applicables, proposer la prise de jours de RTT ou de repos compensateurs, de congés payés (en principe avec l'accord du salarié).

- **Associer les représentants du personnel**

Lorsque la cyberattaque, ses conséquences ou les mesures décidées par l'entreprise affectent durablement l'organisation du travail ou les outils numériques utilisés par les salariés, le CSE doit être informé, voire consulté.

Plateforme Juridique Inter CST UIMM
Espace WAGNER - Bât A2 - 2ème étage - 10 Rue du Lieutenant Parayre - 13290 Aix-en-Provence
Contactez-nous : 04.42.27.32.75 - labro@uimmpjsud.fr
https://www.plateformejuridiqueuimm.fr/