

La menace interne : négligence, départ fâché, malveillance

Toutes les menaces ne viennent pas d'Internet. Prévenir les risques venus de l'intérieur — sans transformer l'entreprise en zone de suspicion.

8 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/menace-interne

Le fichier clients parti avec le commercial démissionnaire, la base effacée par un prestataire mécontent, le stagiaire qui branche n'importe quoi, l'administrateur qui était le seul à connaître les mots de passe : une part significative des incidents vient de l'intérieur. Le sujet est délicat — il touche à la confiance — mais il se traite sainement : par des garde-fous structurels qui protègent tout le monde, pas par la surveillance généralisée.

1. Trois profils très différents

- Le négligent (l'écrasante majorité) : clic malheureux, fichier envoyé au mauvais destinataire, mot de passe faible — il ne veut aucun mal ; la réponse est la formation et des outils qui pardonnent (voir notre guide sensibilisation)
- L'opportuniste du départ : celui qui « emporte » le fichier clients ou ses dossiers en partant — souvent sans même percevoir l'illégalité ; la réponse est le cadre clair + la maîtrise des accès
- Le malveillant (rare mais coûteux) : sabotage, vol organisé, vengeance — souvent lié à un conflit ; la réponse est la limitation des pouvoirs de chacun et la traçabilité

2. Les garde-fous structurels (qui ne visent personne)

- Le moindre privilège : chacun accède à ce dont il a besoin — le commercial n'exporte pas TOUTE la base, le comptable ne touche pas aux serveurs (voir notre guide accès)
- Jamais d'homme-clé unique : les mots de passe d'administration documentés dans le coffre d'entreprise, les compétences critiques partagées — protège autant du départ fâché que de l'accident de la vie
- La traçabilité par défaut : comptes nominatifs et journaux d'accès sur les systèmes sensibles — dissuasif et probant, sans surveiller quiconque en particulier
- Les sauvegardes hors de portée : y compris des administrateurs eux-mêmes (copies immuables) — le sabotage ne doit pas pouvoir tout emporter
- La séparation des pouvoirs sur les actions critiques : double validation des virements, suppression de données en binôme

3. Les moments à risque

- Le départ annoncé ou conflictuel : revue des accès dès l'annonce, vigilance sur les exports massifs et transferts vers des adresses personnelles dans la période précédente
- Le conflit ouvert (litige prud'homal, sanction) : coordination RH + IT sur les accès, dans le respect du droit du travail

- Les prestataires en fin de mission : leurs accès suivent les mêmes règles que ceux des salariés — et s'éteignent à la fin du contrat
- La croissance rapide : les droits s'accumulent, personne ne fait le ménage — la revue annuelle des accès est le correctif

ATTENTION

Le cadre légal protège aussi les salariés : la surveillance doit être proportionnée, déclarée et transparente (charte, information du CSE). Lire les messages personnels, installer des mouchards ou surveiller en secret expose l'employeur à des sanctions CNIL et à l'irrecevabilité totale des preuves. La bonne traçabilité est systématique et annoncée — jamais clandestine.

4. Si l'incident survient

- Préserver les preuves avant tout : journaux, emails, exports — avec méthode (un constat d'huissier pour les cas lourds)
- Couper les accès concernés sans délai, en coordination RH/direction/juridique
- Qualifier juridiquement avant d'agir : vol de données, abus de confiance, violation du secret des affaires — les fondements existent et les tribunaux condamnent régulièrement
- Le fichier clients parti chez un concurrent : mise en demeure rapide (au partant ET au nouvel employeur), action en concurrence déloyale — la réactivité pèse lourd
- Notifier la CNIL si des données personnelles sont concernées : la violation interne est une violation comme une autre

L'essentiel à retenir

- 01 Appliquer le moindre privilège et les comptes nominatifs partout
- 02 Éliminer les hommes-clés : documentation et coffre d'entreprise
- 03 Protéger des copies de sauvegarde même des administrateurs
- 04 Standardiser la procédure de départ, renforcée en cas de conflit
- 05 Encadrer la traçabilité dans la charte, en toute transparence
- 06 Préparer la réponse juridique (preuves, mise en demeure) avant d'en avoir besoin

Questions fréquentes

Un salarié peut-il emporter « son » fichier clients en partant ?

Non — le fichier clients appartient à l'entreprise, et son appropriation est sanctionnée (abus de confiance, concurrence déloyale, violation du RGPD s'il est réutilisé). Beaucoup de partants l'ignorent sincèrement : le rappel écrit dans la charte et à l'entretien de départ prévient l'essentiel des cas, la voie judiciaire traite le reste.

Comment protéger l'entreprise de son propre administrateur informatique ?

Pas par la défiance — par la structure : comptes d'administration nominatifs et journalisés, mots de passe critiques dans un coffre accessible à la direction, sauvegardes immuables qu'aucun compte ne peut purger, et documentation exigée du système. Un administrateur sérieux adhère volontiers : ces garde-fous le protègent aussi (soupçons, accident, surcharge).

Peut-on consulter l'ordinateur d'un salarié absent ou parti ?

Les fichiers et emails professionnels, oui — c'est l'outil de travail de l'entreprise. Limites strictes : ce qui est marqué « personnel » reste protégé par le secret des correspondances, et la consultation doit répondre à un besoin légitime, pas à la curiosité. En contexte contentieux, faites-vous accompagner : la forme conditionne la validité des preuves.

Pour aller plus loin

CNIL — surveillance des salariés : les règles — www.cnil.fr/fr/travail-vie-privee

ANSSI — Guide d'hygiène informatique — cyber.gouv.fr/publications/guide-dhygiene-informatique

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaula pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr