RGPD AVOIR TOUJOURS LES BONS RÉFLEXES

Fiche n°8

Que faire si je constate dans les médias (presse, réseaux sociaux,...) que mon organisation a fait l'objet d'une fuite de données ?

CONTEXTE

Avec la multiplication des canaux de communication, la veille d'image globale et systématique de son organisation est plus que jamais indispensable (médias traditionnels, veille internet, surveillance des réseaux sociaux).
Cette veille contribue à l'analyse de la e-réputation d'une marque ou d'une entreprise.

La veille sert aussi à être alerté très rapidement d'une éventuelle divulgation d'informations confidentielles, volontaire ou non (atteinte à l'image, etc...) et permet à l'entreprise de réagir très rapidement pour vérifier la réalité de la violation et contrôler la communication autour de cet incident.

Dans le cas d'une communication média sur une éventuelle fuite de donnée, il faut impérativement impliquer le service communication (qui doit être partie intégrante) afin d'agir en fonction du contexte et de la stratégie de communication de l'entreprise.

L'ESSENTIEL À RETENIR

Avertir au plus vite toutes les personnes compétentes de l'entreprise (RSSI, DSI, DPD, etc...)
Vérifier la véracité de la fuite
Demander le soutien des organismes publics (CNIL, ANSSI)
Avoir déjà des organisations et procédures en place pour répondre au plus vite à ce type de problématique
Maintenir une veille d'image régulière par le service communication
Intégrer le service communication dans la cellule de crise s'il n'en n'est pas déjà membre

ACTIONS À RÉALISER

1. Vérifier si la fuite/violation de données a bien eu lieu

L'incident peut être détecté par différentes sources : utilisateurs, équipe SI, prestataires/partenaires... une procédure de signalement d'incident de sécurité et de traitement doit donc être mise en place

A. Qui contacter ?

Analyse et qualification par le RSSI (Responsable sécurité & systèmes d'information) de la criticité de l'incident
Informer la DSI pour vérifier la véracité de cette information (déclaration d'incident)
Prévenir l'interlocuteur RGPD qui est le responsable de traitement
Contacter le DPD, l'incident étant relatif à une violation de données personnelles

B. Quelles actions ?

Activation d'une cellule de crise
Déterminer l'origine et la nature de la fuite/violation : est-ce une faille informatique ou une action malveillante ?
Ex : Fuite intentionnelle, perte de données, virus, piratage...
Déterminer le taux de criticité des outils et effectuer un audit
Solliciter le soutien de l'ANSSI pour résoudre cet incident
Voir si le/les sous-traitant(s) sont touché(s) et concerné(s) : ils ont également l'obligation d'avertir le RT
DPD doit prévenir la CNIL à titre préventif et préciser que le sujet est connu et traité.

2. Contrôler & Communiquer

Il faut impliquer le service communication pour agir en fonction du contexte et de la stratégie de communication de l'entreprise.

A. Si l'information n'est pas avérée...

En fonction de la complexité et de l'impact de l'information :
Déterminer si une communication officielle est utile ou non (il peut être plus judicieux de ne pas réagir).
S'il faut communiquer : démentir l'incident et assurer/affirmer sur les moyens déployés pour protéger les données personnelles des utilisateurs.
Confirmer auprès de la CNIL du non-lieu de l'incident

B. Si l'information est avérée...

DPD a obligation d'annoncer la fuite de données à la CNIL dans un délai de 72h, au plus tard après en avoir pris connaissance : Notification (cnil.fr)
Communiquer selon les risques encourus des droits et libertés des individus aux personnes concernées par la fuite de données personnelles.
Conduire une investigation pour identifier la source de la fuite et documenter la traçabilité des violations
Sensibiliser les différents acteurs : utilisateurs, équipe SI, prestataires/partenaires...

Pour tout complément d'information : se référer à la Fiche Réflexe n°7 : Que faire si je constate une fuite de données au sein de mon organisation ?

POINTS DE VIGILANCE

Etablir une procédure de signalement d'incident de sécurité et de traitement avec tous les acteurs (principe de coresponsabilité des sous-traitants dans les contrats).
Superviser tous les flux sortants, mettre à disposition un outil de supervision pour la détection (développement interne à chaque entreprise).
Mettre en place les organisations et les instances pour répondre et réagir (ex : création d'une cellule de crise)

RISQUES

Atteinte à l'image et à la réputation de l'organisation, perte économique
Atteinte aux droits et libertés des individus, le risque ne concernant pas uniquement l'entreprise
Amende administrative en cas d'action de la CNIL ou d'une autorité administrative si l'entreprise n'a pas mis de moyen pour éviter une fuite de données

POUR ALLER PLUS LOIN

- La CNIL a déposé une fiche nommée : « Notifier une violation de données personnelles », qui se suffit à elle-même : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
- Pour se prémunir d'une fuite de données sur Internet, la CNIL a mis en place une fiche dédiée aux recherches préventives : La recherche sur Internet de fuite d'informations (RIFI)
- Se renseigner sur des exemples concrets, comme : Fuite de données de santé (21 septembre 2021)