Violations massives de données en 2024 : quels sont les principaux enseignements et mesures à prendre ?

28 janvier 2025

En 2024, plusieurs violations de données d'une ampleur exceptionnelle ont touché de grandes bases de données et entraîné l'exfiltration des données de millions de Français. Pour prévenir ces violations, la CNIL propose des mesures adaptées et contrôle leur mise en œuvre.

Les violations touchant les grandes bases de données se sont multipliées en 2024

En 2024, la CNIL a été notifiée de 5 629 violations de données personnelles, soit 20 % de plus qu'en 2024. Au-delà de cet accroissement notable, la tendance la plus préoccupante est celle d'une recrudescence de violations de très grande ampleur. En plus des violations sans précédent qui ont concernées les opérateurs du tiers payant, France Travail ou encore la société Free, la CNIL constate que le nombre de violations touchant plus d'un million de personnes a doublé en un an.

5 629 violations de données

ont été notifiées à la CNIL en 2024

+20 % par rapport à l'année précédente

En réaction, la CNIL a fait de la cybersécurité un des 4 axes de son plan stratégique 2025-2028.

En pratique son action se traduit par :

- l'accompagnement des organismes, en produisant des recommandations permettant de protéger les données personnelles au regard de l'évolution de la menace et de l'état de l'art ;
- des contrôles sur la mise en œuvre des mesures de sécurité par les organismes ;
- l'information et la sensibilisation des particuliers à la cybersécurité pour les rendre acteurs de la protection de leurs données.

Parallèlement, la CNIL intensifie la coordination avec les acteurs de la cybersécurité, en particulier l'ANSSI et cybermalveillance.gouv.fr.

Un besoin de renforcer les mesures de sécurité au regard des risques

Pour tout traitement de données personnelles, le RGPD impose à l'organisme responsable de mettre en place les mesures de sécurité adéquates par rapport aux risques. À cet égard, le guide de la sécurité des données personnelles publié par la CNIL rappelle les précautions qui devraient être mises en œuvre.

Pour les traitements de grandes bases de données, les incidents intervenus en 2024 démontrent que des mesures de sécurité renforcées sont requises au regard des risques. En particulier, les mesures de sécurité dites « périmétriques », qui visent à protéger un système d'information (SI) de menaces qui lui sont extérieures. Ces mesures peuvent utilement être complétées par des mesures de « défense en profondeur » destinées à protéger de menaces ayant déjà atteint le SI lui-même.

Les violations de données massives sont souvent dues à des défauts de sécurité récurrents

Les informations fournies par les organismes dans les notifications ou obtenues à l'occasion des contrôles diligentés par la CNIL, montrent que les modes opératoires des attaquants sont souvent similaires et exploitent régulièrement les mêmes failles. Ces informations amènent notamment les constats suivants :

- les informations de connexion utilisées pour l'attaque avaient été compromis ;
- les intrusions et exfiltrations n'ont pas été détectées par l'organisme avant la mise en vente des jeux de données ;
- une part significative des incidents impliquait un sous-traitant ;

Pour montrer comment des mesures de sécurité peuvent aider à détecter et stopper les accès potentiellement suspects, avant l'exfiltration des données, la CNIL présente le mode opératoire le plus souvent constaté dans les récentes attaques.

À cet égard, l'analyse des différentes phases des violations révèle qu'**une succession de défauts de sécurité courants** ont permis à l'attaquant de passer d'une étape à la suivante.

Dans ce contexte, le déploiement de mesures de sécurité couvrant l'ensemble des niveaux doit être un objectif de mise en œuvre d'une « défense en profondeur » permettant de réduire à la fois la vraisemblance mais aussi la gravité des violations. Celles-ci concernent les responsables de traitement comme les sous-traitants.

Accès à des données de connexion

Accès au système d'information

Analyse du système et accès aux données

Extraction massive des données

Proposition des données à la vente

1 L'attaquant obtient des données de connexion (identifiant + mot de passe) légitimes d'un collaborateur ou partenaire

Principaux événements constatés

Le moyen permettant d'obtenir les données de connexion n'est pas forcément connu, au moment de la notification. Toutefois, les causes les plus fréquemment constatées dans les incidents notifiés à la CNIL sont les suivantes.

- Des comptes de connexion sont génériques ou partagés.
- Un utilisateur a reçu un message (hameçonnage) l'invitant à saisir son identifiant et son mot de passe sur un faux site.
- Un logiciel malveillant a été installé sur le poste d'un utilisateur et a permis de dérober les données de connexion (*malware*, *infostealer*).
- Un utilisateur a accepté de vendre ses données de connexion.
- Des données de connexion, issues d'une précédente fuite, sont proposées sur le marché noir.

Exemples de mesures pouvant prévenir ces risques

- Mettre en place une authentification multifacteur, en particulier pour les accès à distance, et systématiser les comptes nominatifs individuels.
- Sensibiliser / former les collaborateurs aux enjeux en matière de sécurité.

2 L'attaquant obtient un accès au système d'information

Principaux événements constatés

- Un SI est accessible librement depuis Internet.
- Une ou plusieurs failles de sécurité dans des pare-feux, passerelles VPN ou passerelles de filtrage ont pu être exploitées.

Exemples de mesures pouvant prévenir ces risques

- Limiter l'accès au réseau (y compris via VPN) aux seuls équipements authentifiés.
- Mettre en œuvre une veille pour être en capacité d'appliquer les mises à jour dès que possible.

3 L'attaquant analyse le système d'information et accède aux données de façon massive

Principaux événements constatés

- De nombreux utilisateurs peuvent accéder à d'importants volumes de données, du fait d'habilitations trop larges.
- La récupération de toutes les entrées dans une application est possible par du script.
- Il n'existe pas de limitations quant aux requêtes ou à la fonctionnalité applicative d'export susceptibles d'être effectués par un utilisateur.
- Les données sont collectées ou partagées avec un sous-traitant de façon excessive au regard de la finalité du traitement.
- Les données en base active sont conservées pendant une durée excessive.

Exemples de mesures pouvant prévenir ces risques

- Mettre en œuvre une politique d'habilitation et définir des droits d'accès restreints à ce qui est strictement nécessaire (en fonction des besoins métier, fonctionnels, des périmètres temporel, géographique, etc.).
- Appliquer des mesures assurant un cloisonnement effectif des données à chaque niveau des applications (du frontend au backend).
- Appliquer des limitations temporelles sur le nombre de requêtes pouvant être effectuées, sur les volumes de données exportables, au global ou par des utilisateurs individuels.
- Appliquer de façon stricte les principes de durée de conservation limitée des données personnelles par un mécanisme d'archivage ou de purge automatique.

4 L'attaquant extrait les données de façon massive

Principaux événements constatés

- Les indicateurs devant permettre de détecter une activité anormale, et réagir rapidement en cas d'alerte, sont inexistants, insuffisants ou pas exploités.

Exemples de mesures pouvant prévenir ces risques

- Mettre en place une analyse en temps réel des flux réseau et des journaux, ainsi qu'une capacité opérationnelle à traiter les alertes.

5 L'attaquant propose les données à la vente

Principaux événements constatés

- Le responsable du traitement ou le sous-traitant n'ont pas détecté l'exfiltration massive et/ou ne se sont pas aperçus de la mise en vente des données.

Exemples de mesures pouvant prévenir ces risques

- Mettre en place une recherche de fuite sur Internet, dans le respect du RGPD et du code pénal.

Dans tous les cas :

- Vérifier périodiquement que les garanties de sécurité offertes par les sous-traitants / prestataires sont suffisantes et prévoir la mise en place des mesures de sécurité adaptées dans les contrats.
  Fiche 14 – Gérer la sous-traitance, Guide de la sécurité des données de la CNIL

- Journaliser les accès (aux applicatifs, aux API, au système, au réseau) à monitoring à génération et traitement des alertes afin de réagir rapidement et permettre une levée de doute par un humain
  Fiche 16 – Tracer les opérations, Guide de la sécurité des données de la CNIL