RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CERT-FR

Date : 18 septembre 2024
Version : 1.0
Nombre de pages : 10

EXFILTRATION DE DONNÉES DU SECTEUR SOCIAL : RETOUR D'EXPÉRIENCE DU CERT-FR

CONTEXTE OPÉRATIONNEL

L'année 2023 et le début de l'année 2024 ont été marqués par de nombreux incidents ciblant des entités du secteur social[1] **gérant des données à caractère personnel**[2].

Compte tenu des impacts qu'ont eu ces exfiltrations de données, le CERT-FR propose un **retour d'expérience** sur la gestion de ces incidents et des recommandations associées. Ce document n'a pas pour objectif d'être un guide sur la protection des données personnelles[3] mais bien de rassembler les enseignements et constats que les équipes du CERT-FR ont pu faire lors du traitement d'incidents. Ces derniers ont en effet été l'occasion d'**exfiltrations illégitimes** de quantités massives de données personnelles de millions de Français. Leur analyse met en évidence des **insuffisances** de **protection** dans la façon dont ces données sont traitées et les moyens par lesquels on y accède, et ce, dès la conception des projets qui en traitent.

LE SECTEUR SOCIAL : UNE CIBLE DE CHOIX

Sur l'année 2023 et le début de l'année 2024, le CERT-FR a traité, avec un degré d'engagement plus ou moins fort, **183 incidents** – **tout secteur confondu** – ayant résulté en

[1] La protection des données personnelles dans le secteur social | CNIL
[2] Le responsable d'un traitement de données à caractère personnel est en principe la personne, l'autorité publique, la société ou l'organisme qui **détermine les finalités et les moyens** de ce fichier, qui décide de sa création – Question | CNIL
[3] Une donnée personnelle est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement – Question | CNIL

une exfiltration de données – dont 60 sont la conséquence d'une compromission et d'un chiffrement par rançongiciel.

Dans ce retour d'expérience, le CERT-FR se concentre **uniquement sur les incidents** – hors rançongiciel – ciblant des **entités du secteur social**. Sur la période étudiée, le CERT-FR a appuyé **9 entités** de ce type dans le traitement d'un incident de sécurité ayant mené à une exfiltration de données.

En effet, du fait de leurs activités, ces dernières sont en possession d'un grand volume de données, en particulier des données personnelles (bancaires, de santé, etc). Ce retour d'expérience n'a donc **pas vocation à traiter de façon exhaustive** tous les scénarios de menace pouvant affecter le secteur social mais vise à **donner des clés** pour la **préparation** et la **prévention** de telles attaques, du fait des larges impacts potentiels pour les citoyens.

En effet, de **telles données**, si elles sont récupérées par une personne mal intentionnée, peuvent faire l'objet d'une **commercialisation** sur les marchés cybercriminels voire d'une **réutilisation** dans le cadre de fraudes, ou encore être **mises à disposition gratuitement** dans le cadre d'opérations de déstabilisation. Le CERT-FR constate que ces fuites de données peuvent être **revendiquées** – de façon avérée ou non – voire être **republiées**, parfois **plusieurs mois après l'incident** et par plusieurs acteurs cybercriminels ou hacktivistes.

L'accompagnement du CERT-FR sur cette typologie d'incidents de sécurité permet aujourd'hui de dégager, de **manière non-exhaustive**, un ensemble de **constats** et de **recommandations** associées.

IMPACTS ET RISQUES OBSERVÉS

Dans la logique métier, **la donnée personnelle n'est souvent pas perçue comme intrinsèquement plus sensible** que les données techniques. De ce fait, peu de mesures de sécurité sont appliquées lors de sa manipulation ou dans le contrôle des accès effectués. Les **risques identifiés** viennent aussi bien **des usagers des applications**, légitimes ou non, que **d'opérateurs techniques** ou de sous-traitants.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL)

« Les **responsables** d'un fichier et les **sous-traitants** doivent prendre toutes les mesures nécessaires pour **assurer la sécurité** et la **confidentialité des données personnelles** qu'ils traitent :

- Des mesures de **sécurité physique** : sécurité des accès aux locaux ;
- Des mesures de **sécurité informatique** : antivirus, sécurisation des mots de passe, etc.

Ils doivent également veiller à ce que seuls les destinataires autorisés puissent accéder aux données. »[4]

RISQUES ASSOCIÉS AUX USAGERS APPLICATIFS[5]

Les grands applicatifs traitant des données personnelles ont souvent un **large panel d'usagers** : ceux-ci peuvent être internes à l'organisation qui opère le système, mais aussi appartenir à diverses administrations et acteurs privés. Ces **usagers** sont **nombreux** et doivent manipuler les données de l'application avec parfois des **privilèges élevés**. **Leurs accès doivent faire l'objet de mesures d'authentification, de traçabilité et de contrôle à l'état de l'art**.

Le développement des applications peut également s'appuyer sur le principe de ***Privacy by Design and by Default***[6]. Ce principe stipule que la **protection des données** doit être prise en compte **dès la conception d'un projet** et que cette protection doit s'effectuer par défaut. Ainsi, les risques d'un éventuel non-respect du Règlement général de la protection des données (RGPD) s'en trouvent limités.

Les multiples incidents récents traités par le CERT-FR ont mis en évidence des **mauvaises pratiques** dans la gestion par les usagers privilégiés des applicatifs qui contiennent des données parfois sensibles[7].

La gestion des **authentifications d'utilisateurs**, souvent peu moderne, laisse une marge de manœuvre importante pour les attaquants. En effet, les identifiants et mots de passe sont souvent **partagés**, **réutilisés** et peuvent donc être plus facilement **récupérés** notamment par le biais d'ingénierie sociale. Le **cycle de vie** des **identifiants**, sur de larges populations concernées[8], est souvent **décalé par rapport aux besoins**. Dans le cas d'un grand nombre d'utilisateurs, la **probabilité** qu'un acteur malveillant puisse **utiliser un compte légitime** *via* une usurpation d'identité et sans être détecté est **forte**.

> *« Dans le cadre d'un incident, l'ANSSI a constaté que des **comptes** de **prestataires externes** – sans authentification forte – ont été **compromis** et **utilisés** pour exfiltrer l'intégralité d'une base de données »*

[4] Question | CNIL

[5] Un usager applicatif est une personne à qui a été confiée un accès à une application pour en faire un usage légitime. Cette personne peut être interne ou externe à l'organisation opérant l'application. Cet accès est normalement nominatif et contrôlé par des identifiants personnels, parfois multiples. Les privilèges accordés à l'usager peuvent être très variables, de la simple validation de ses propres informations à la gestion des accès d'autres usagers en passant par divers accès aux informations sensibles de tiers.

[6] Article 25 du Règlement général de la protection des données (RGPD) - CHAPITRE IV - Responsable du traitement et sous-traitant | CNIL

[7] L'expression « donnée sensible » est entendue au sens défini par la CNIL - Donnée sensible | CNIL

[8] Certaines plateformes hébergent les données de millions de français, ayant eux-mêmes des accès nominatifs.

Ainsi, dans plusieurs cas portés à la connaissance ou traités par le CERT-FR, les attaquants ont utilisé des **accès légitimes**, récupérés *via* des campagnes d'hameçonnage réussies ou sur des sites de revente d'identifiants de connexion. Au moyen de ces comptes, des **actions légitimes** de consultation des bases de données leur ont permis d'en **exfiltrer le contenu**, faute de règles ou de limites mises en place. **L'absence de supervision** et/ou le **manque de journalisation** sont également des facteurs aggravants. Les équipes techniques de ces entités ne sont alors **pas en mesure de détecter** les comportements suspects ou bien le réalisent trop tardivement.

> *« Dans le cadre d'un incident, l'ANSSI a identifié que les **limitations de consultation** mises en place pour les personnes autorisées à accéder aux bases de données ont pu être **modifiées et** facilement **contournées** par l'attaquant. Ainsi, l'attaquant s'est **connecté** à la plateforme de consultation des données, et en **simulant** des millions de recherches, il a pu, par **simple navigation**, extraire le contenu. »*

RECOMMANDATIONS

Si **l'usager** peut accéder à des données d'une tierce personne, il convient de :

- l'identifier comme un **risque pour la sécurité** de ces données. Ainsi, cet usager devient un **utilisateur à privilèges**. Il est nécessaire d'implémenter un mécanisme **d'authentification forte ou *a minima* multifacteur**[9], *a fortiori* si l'application est exposée à des réseaux non maitrisés (ex : Internet) ;
- **journaliser les actions** menées par cet utilisateur sur l'application, même pour les cas où aucune modification n'a été effectuée ;
- **assurer** une **gestion des comptes** et des **droits adaptée** à chaque besoin d'accès aux données ; les comptes inutilisés doivent être régulièrement identifiés et au moins désactivés, voire supprimés ;
- **interdire** l'usage de **comptes génériques par défaut**. L'utilisation d'un tel compte ne doit faire l'objet que d'un processus de dérogation. Cette dérogation est généralement **accompagnée de mesures de sécurité** techniques ou organisationnelles additionnelles ;
- **limiter l'exposition de l'application**, en mettant en place par exemple un système de verrouillage des accès en dehors des plages de consultations légitimes ;
- contrôler par des **règles plus restrictives** l'export massif de données, la **consultation** et la **modification** des données *via* les applications. Le cas échéant, des règles de détection simples peuvent être implémentées afin d'alerter les responsables métiers de tout comportement suspect ;

[9] Recommandations relatives à l'authentification multifacteur et aux mots de passe | ANSSI (cyber.gouv.fr)

- **protéger** en **confidentialité les données exportées** par la mise en œuvre d'un chiffrement adapté[10] ;
- **segmenter les environnements serveurs** par des règles de filtrage réseau pour contrôler les flux entrants et limiter voire interdire les flux sortants (initiés depuis le serveur).

Un non-respect de ces règles devrait faire l'objet d'une alerte auprès des équipes techniques avec également la possibilité d'une neutralisation temporaire des accès le temps d'une levée de doute.

RISQUES ASSOCIÉS AUX ACTEURS TECHNIQUES

Si les actions des usagers privilégiés doivent être considérées comme **très sensibles**, les **accès techniques** à des plateformes supportant des applications travaillant sur de grandes bases de données **sont critiques**. Ils peuvent **être détournés** de manière **consciente** – exploitation d'un compte VPN compromis – mais également de manière **involontaire**.

> *« Dans le cadre d'un incident porté à la connaissance de l'ANSSI, un **prestataire** a **volontairement utilisé ses accès administrateurs** pour exfiltrer une base de données, et ce, à plusieurs reprises. Par ailleurs, ces actions n'ont été que **tardivement détectées** par les équipes de l'entité en question malgré plusieurs facteurs aggravants qui auraient du lever une alerte : flux d'exfiltrations massifs, horaires d'activité non conformes… »*

Un **défaut d'hygiène informatique** peut mener à l'exposition non-maîtrisée de données. Ainsi, la revente et le recyclage de supports, la perte de données sur des supports non chiffrés ou bien **l'exposition sur Internet d'une base de travail** à la suite d'erreurs de manipulation sont autant de facteurs pouvant favoriser l'exfiltration de données, y compris sensibles.

Au sein de l'écosystème, les **acteurs techniques** sont nombreux : en **externe** avec des sous-traitants (pour la partie infogérance) ou en **interne** de manière temporaire (consultants intégrés à l'organisation).

Par essence, et afin de réaliser leurs missions, ces acteurs ont la **capacité d'accéder directement à la donnée brute[11], sans passer par l'application.** Ces accès peuvent être légitimes ou non mais ils **ont en commun de contourner la journalisation** applicative et les limitations en place. L'accès direct (ou non intermédié) à la

[10] Mécanismes cryptographiques | ANSSI (cyber.gouv.fr)

[11] La « donnée brute » est entendue au sens de donnée telle qu'enregistrée dans son stockage durable, sans traitement, tel que les stockages destinés à l'affichage sur une page *web* ou un écran applicatif.

base de données a permis, dans plusieurs incidents, une exfiltration de l'intégralité des données dans un laps de temps très court.

L'expérience du CERT-FR montre aussi que des informations personnelles brutes peuvent être présentes sur des **systèmes de qualification ou de préproduction**. Ces systèmes sont souvent **moins supervisés** que leurs équivalents de production et peuvent ainsi être à **l'origine de fuites** de données non détectées.

RECOMMANDATIONS

Au vu des récents incidents et de manière non-exhaustive, le CERT-FR rappelle que les **analyses de risque** menées sur ces applications **doivent se centrer** en particulier **sur de la donnée**.

- Des **mesures** de sécurité doivent nécessairement être déployées **partout** où la **donnée est manipulée**, c'est-à-dire dans les instances de l'application, les zones de transit, de stockage, de sauvegarde, etc.
- En **dehors des systèmes de production**, les **données utilisées** devraient être **simulées**. L'utilisation d'une donnée réelle est à proscrire par défaut. Si néanmoins l'utilisation de donnée purement synthétique est impossible, la **valeur** de ces données doit être **dégradée** par des mesures de bruitage de l'information[12]. L'utilisation d'une méthode de pseudonymisation[13] ou d'anonymisation doit faire l'objet d'un processus d'approbation spécifique.
- Une **intervention** d'un prestataire ou sous-traitant au sein de l'infrastructure est considérée comme un acte d'administration[14] qui ne devrait s'effectuer que depuis un **environnement dédié** avec des accès à Internet réduits et une **supervision renforcée**. En aucun cas l'accès aux infrastructures contenant les données personnelles ne doit se faire depuis un poste d'usage bureautique.
- **Le cycle de vie des accès doit suivre les évolutions RH**. En particulier, la période précédant le départ d'acteurs ayant eu des privilèges élevés représente un risque accru pour la donnée. Des restrictions des accès pourraient être mises en œuvre préalablement au départ afin de limiter les risques d'exfiltration. Ces pratiques sont à considérer avec encore plus d'attention en cas de départ conflictuel.
- Une **politique de gestion des comptes et des droits** doit être mise en place tout au long du cycle de vie de la donnée. Il est fortement recommandé **d'automatiser le processus**, par exemple en désactivant automatiquement les comptes inactifs.

[12] Il existe un grand nombre de méthodes de dé-identification conservant les propriétés générales d'un corps de données : **l'anonymisation** rend les données non rapprochables d'une identité, la **pseudonymisation** masque cette identité par un alias. L'anonymisation de données personnelles | CNIL

[13] Identifier les données personnelles | CNIL

[14] Recommandations relatives à l'administration sécurisée des SI | ANSSI (cyber.gouv.fr)

- **La chaîne de reconditionnement**[15] doit être maîtrisée pour éviter toute fuite de données.
- Les données sauvegardées doivent être protégées en **confidentialité** et **intégrité**.

EN CAS D'INCIDENT

L'ANSSI recommande idéalement de **ne pas attendre d'être la cible d'un incident de sécurité pour contractualiser** avec des prestataires de gestion de crise et de réponse à incident[16].

OBLIGATIONS RÉGLEMENTAIRES

Au moindre doute quant à une potentielle exfiltration de données personnelles, il est recommandé de faire une **notification initiale à la CNIL**[17].

Vis-à-vis du RGPD, il revient à l'entité victime de ce type d'incident d'**évaluer le risque** pour les personnes concernées et de **prendre les mesures** permettant de l'atténuer. Si ce risque est élevé, l'entité a l'obligation **d'informer les personnes**, de façon individuelle lorsque cela est possible. Par ailleurs, **d'autres déclarations ou communications obligatoires** – en-dehors du RGDP – doivent également être envisagées.

Au vu de leur sensibilité, certaines **données de santé** bénéficient d'un **cadre spécifique** pour leur hébergement, avec une obligation dans certains cas prévus par la loi[18] de recourir à des prestataires certifiés Hébergeur de Données de Santé (HDS)[19].

> **Nota** : Plusieurs groupes adeptes d'extorsion informatique ont, par erreur ou à dessein, annoncé de **fausses fuites de données** d'organisations. Les annonces venant de groupes criminels doivent être vérifiées et éventuellement confirmées. Ces vérifications pouvant prendre du temps, il est **recommandé d'effectuer les déclarations réglementaires initiales** au plus vite. Il sera ensuite possible de les clore sur un constat d'incident non avéré.

COMMUNICATION DE CRISE

En matière de communication de crise, l'exfiltration et la publication de données personnelles présentent des caractéristiques propres. Une cyberattaque avec exfiltration

---

[15] Recommandations pour le reconditionnement des ordinateurs de bureau ou portables | ANSSI (cyber.gouv.fr)
[16] Prestataires de réponse aux incidents de sécurité (PRIS) | ANSSI (cyber.gouv.fr)
[17] Notifier une violation de données personnelles | CNIL
[18] « Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet. » *L.1111-8 du code de la santé publique, modifié par la loi n° 2016-41 du 26 janvier 2016*
[19] Le référentiel de certification HDS est élaboré par la Délégation au Numérique en Santé en lien avec l'Agence du Numérique en Santé, qui publie la liste des prestataires certifiés.

et publication de données personnelles peut avoir un **impact significatif** sur l'activité mais également la **réputation** de l'entité à laquelle les données publiées appartiennent selon la nature de celles-ci, leur éventuelle portée stratégique et le niveau d'exposition. L'entité victime peut faire l'objet de pressions de la part des personnes concernées par les données divulguées. La **pression médiatique est souvent forte** : des sollicitations répétées peuvent émaner des médias régionaux, nationaux et internationaux mais également *via* un nombre important de publications ou de commentaires sur les réseaux sociaux.

La **communication** de l'organisation victime doit être **particulièrement soignée**[20] car de nombreux experts (souvent auto-proclamés) ou personnalités sont susceptibles de se saisir de l'incident et de contester les propos officiels si ceux-ci s'avèrent imprécis ou erronés.

Il est également nécessaire **d'anticiper la potentielle communication des attaquants** : publication d'une actualité et de données exfiltrées sur le *darkweb*[21], d'un communiqué de presse, de publications sur les réseaux sociaux. Une fois les données rendues publiques, l'entité concernée a peu de marge de manœuvre pour limiter leur visibilité.

Pour la partie communication, l'ANSSI recommande en amont de l'incident :

- **d'initier un dialogue** entre les communicants et l'équipe cyber ou IT hors période de crise ;
- **d'anticiper les scénarios de crise** et les réponses à apporter sur le volet communication ;
- d'anticiper des **modes de communication interne** et **externe dégradés** en amont (listes des numéros de téléphone et des emails personnels, affichage, etc.) ;
- de créer une **boîte à outils dédiée** à la gestion d'une crise cyber disponible sur clé USB et en version papier au cas où les serveurs ne seraient plus accessibles.

En complément, l'ANSSI recommande pour les communications :

- d'adopter un **ton pédagogique**, vulgarisé et rassurant ;
- d'activer une **veille médiatique** et analyse réputationnelle en continu ;
- d'expliquer simplement la nature de la cyberattaque et ses impacts sur l'entité, ses services ou ses produits ;
- d'indiquer que des **investigations** sont en cours ;
- de donner de la **visibilité sur les actions** mises en œuvre pour rétablir au plus vite les services et outils ;
- d'alerter en premier les agents/collaborateurs **en interne** car ce sont les premiers à subir de potentielles fortes perturbations de leurs activités ;
- d'informer rapidement les **parties prenantes** (clients, partenaires, prestataires…) pour leur permettre de prendre les mesures de vigilance et de protection appropriées ;

[20] Annexe « Conseils sur la communication »

[21] Définition du *Darkweb* : « Internet qui nécessite l'utilisation d'un protocole particulier (chiffrement, proxy etc) » - CyberDico de l'ANSSI

- si l'incident est **judiciarisé**, de demander **l'accord du service enquêteur** avant de dévoiler certains éléments précis de l'attaque.

L'ANSSI conseille d'éviter :

- d'adopter un ton anxiogène et d'aggraver volontairement la sophistication de la cyberattaque : la communauté cyber s'en rendra vite compte ;
- de donner trop de détails techniques sur la gestion de la cyberattaque : cela risque de brouiller le message et d'informer les attaquants sur la défense ;
- de s'engager au tout début de la crise sur une date précise de retour à la normale : la complexité des cyberattaques peut engendrer un allongement des délais ;
- d'attribuer l'attaque afin de limiter la visibilité et la publicité qui pourraient être données aux attaquants.

QUE FAIRE EN CAS DE COMPROMISSION ?

En cas de **compromission** ou de **suspicion** de compromission, le CERT-FR vous invite à prendre connaissance de cette page :

Les bons réflexes en cas d'intrusion sur un système d'information - CERT-FR (ssi.gouv.fr)

Le CERT-FR est joignable :

- **Par téléphone :**
  - Depuis la France métropolitaine au *3218* (service gratuit + prix d'un appel) ou *09 70 83 32 18*
  - Depuis certaines collectivités territoriales situées en Outre-mer ou depuis l'étranger au *+33 9 70 83 32 18*
- **Par courriel :**
  - A l'adresse *cert-fr@ssi.gouv.fr*

POUR ALLER PLUS LOIN

- CNIL : Particulier | CNIL
- CSIRT territoriaux : Les CSIRT territoriaux - CERT-FR (ssi.gouv.fr)
- Cybermalveillance : Assistance aux victimes de cybermalveillance
- Fiches réflexes de l'INTERCERT FRANCE : publications/Fiches_reflexes at main · intercert-france/publications · GitHub
- CERT Santé : fiche réflexe fuite de données Fiche_reflexes_Fuite_donnees_PR.pdf (esante.gouv.fr)
- Guide « Anticiper et gérer sa communication de crise cyber » de l'ANSSI : Anticiper et gérer sa communication de crise cyber | ANSSI

ANNEXE : CONSEILS SUR LA COMMUNICATION

Si un attaquant publie des données qu'il désigne comme étant les vôtres, il est nécessaire de préparer plusieurs communications.

- **1ère communication** : très rapidement après la publication des données exfiltrées par l'attaquant, l'ANSSI conseille **d'indiquer publiquement** que vous avez pris **connaissance** de ce **potentiel incident** touchant votre entité. Il est également important **d'indiquer** qu'une **qualification des données** est **en cours** afin de confirmer ou non qu'elles vous appartiennent réellement.
- **2e communication** : si les données exfiltrées appartiennent réellement à votre entité, nous vous recommandons de **confirmer l'exfiltration** et la **publication** de données personnelles en ajoutant également un mot d'excuse vis-à-vis du dommage occasionné pour les personnes concernées. Si c'est le cas, il est important de **préciser** les **mesures prises vis-à-vis des autorités** : l'alerte de l'incident à l'ANSSI, le dépôt de plainte auprès des services de police ou de gendarmerie spécialisés et la déclaration obligatoire auprès de la CNIL. Vous devrez également **indiquer** qu'une **qualification précise des données** est **en cours** pour déterminer leur nature et qu'un retour vers les personnes concernées par cette exfiltration sera fait.
- **3e communication** : en cas de **risque élevé sur la vie privée**, vous devez également **notifier les personnes concernées** dans les meilleurs délais.

  La communication aux personnes concernées décrit, en des **termes clairs et simples**, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures suivantes :
  - le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
  - les conséquences probables de la violation de données à caractère personnel ;
  - les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

  Nous conseillons également aux entités victimes de **communiquer publiquement sur leur site web et leurs réseaux sociaux** sur cette exfiltration et publication de données personnelles afin que les personnes concernées puissent vérifier la légitimité de l'information reçue.