Compromission de données chez un sous-traitant : quels sont les risques des accès non sécurisés ?

23 avril 2025

Régulièrement, la CNIL communique sur des violations de données typiques inspirées d'incidents réels qui lui sont notifiés. Cette publication a pour objectif de permettre à tous les professionnels de comprendre et de prévenir les risques d'accès à des données détenues par les sous-traitants.

Le cas présenté dans cette fiche est fictif même si inspiré d'un cas réel.

L'histoire de Bu3ba et Dan

Le déroulement de l'attaque

1. Quelques semaines avant l'attaque, Bu3ba, un pirate informatique, a récupéré une multitude d'adresses e-mails professionnels sur le *dark web*.

2. Il lance ensuite une campagne **d'hameçonnage**, une opération peu coûteuse et efficace. Avec l'une des adresses récoltées, Bu3ba envoie un message à une plateforme logistique en se faisant passer pour un client connu de la société (il a repéré le logo de celle-ci sur la page « Nos clients » du site web de la plateforme).

Le faux message, qui semble légitime, demande une action urgente et fournit un lien vers un écran d'authentification aux couleurs de l'entreprise cliente. **L'employé de la plateforme s'authentifie machinalement avec l'identifiant et le mot de passe partagé au sein de l'équipe.** Un message indiquant que le système est indisponible apparaît.

3. Bu3ba a réussi son attaque et commence sa récolte : il remarque **un accès direct, sans aucune protection**, à un service qui semble contenir un volume important de données. Il se consacre alors entièrement à ce dernier.

4. En se connectant avec le compte usurpé de l'employé, Bu3ba découvre qu'il n'a accès qu'aux données relatives à deux entreprises clientes. L'accès est cependant total et, **l'outil le proposant**, il lance un téléchargement des données pour chacune de ces bases de données.

5. À partir de ce même compte, **il accède aux autres bases clientes en modifiant les requêtes envoyées à la base de données**. Les données d'un troisième grand compte client s'affichent : il les télécharge. Patiemment et méticuleusement, il récupère un volume important de données de chaque client, qu'il commence alors à analyser.

Vu le service proposé (logistique), les données sont principalement des données personnelles : état civil, coordonnées postales, adresses e-mails, téléphones, mais également des références de commandes et des demandes spécifiques, en très grandes quantités. **Plusieurs millions de lignes sont présentes dans ces différentes bases.**

6. Pour masquer un minimum ses traces, Bu3ba a utilisé différents VPN passant par plusieurs pays, pas forcements coopératifs entre eux. Le niveau global de sécurité était (très) faible : il n'y avait pas besoin d'appartenir à une certaine plage d'adresse IP ou d'utiliser un VPN pour se connecter depuis Internet. Il n'y a pas eu de coupure lorsqu'il a lancé les différents téléchargements : il suspecte l'absence de DLP (*Data Loss Prevention* ou prévention des pertes de données), un dispositif qui permet normalement de contrer ce type de téléchargement massif. Ne sachant pas s'il existe une journalisation minimale, il patiente quelques mois avant de publier ses trouvailles.

7. Bu3ba publie le fichier sur un forum du *dark web* et y ajoute une capture d'écran de quelques centaines de lignes de la base de données. Dans peu de temps, l'information va se répandre : comme souvent, c'est à ce moment-là que la victime va découvrir le piratage, vraisemblablement par une

publication l'apostrophant sur un réseau social. Dans le meilleur des cas, ce sera un service de recherche sur Internet de fuites d'informations (RIFI) de l'un des clients qui l'alertera.

Comment réagir ?

L'enquête interne

Quelques heures après la publication de Bu3ba, Dan, délégué à la protection des données d'un client de la plateforme logistique, reçoit un appel de la police lui indiquant que des données appartenant à son organisme seraient en ligne sur le *dark web*. Un internaute a détecté un **fichier** contenant de nombreuses données dont certaines seraient rattachées à l'employeur de Dan et a lancé l'alerte.

Les équipes de Dan analysent l'échantillon mis en ligne et arrivent à la conclusion que ces données semblent leur appartenir. Cependant, le Centre des Opérations de Sécurité (« SOC » ou « *Security Operations Center* ») de l'entreprise de Dan n'a pas détecté d'attaques massives sur leur système d'information qui auraient pu donner lieu à une compromission générale.

En revanche, après des investigations plus poussées, il apparaît que ces données correspondent à ce qui est transmis à un **sous-traitant** à des fins de livraisons. Rapidement, Dan contacte son sous-traitant, qui vient d'être alerté également par un autre de ses clients. Le point d'entrée est ainsi découvert.

La notification de la violation à la CNIL et l'information aux personnes

Aidé par son sous-traitant, Dan va devoir gérer la **violation de données personnelles que constitue l'incident au sens du RGPD**. Il dispose donc de **72 heures** depuis la découverte de l'incident afin de réaliser cette notification auprès de la CNIL.

Le sous-traitant dispose de procédures internes de gestion des incidents et collecte un certain nombre d'éléments afin d'aider les responsables de traitement à réaliser leurs notifications de violation de données.

1. **Documenter et notifier à la CNIL**. Tout d'abord, Dan consolide les informations collectées auprès de son prestataire et **documente cet incident comme une violation de données personnelles.** Après analyse et consultation des conseils de la CNIL sur le sujet, il lui notifie la violation de données.

2. **Informer les personnes.** Les données impactées ne sont pas sensibles au sens de la loi. Cependant, plus d'un million d'adresses, d'e-mail et de numéros de téléphone ont fuité à la suite de cette violation : le risque est à considérer comme élevé. Il **rédige un message d'information à destination des clients touché**s, en donnant les informations obligatoires : les circonstances de l'incident, la nature des données concernées, le point de contact pour avoir des informations supplémentaires, les mesures déjà prises et envisagées ainsi que les conséquences possibles pour les personnes concernées, dans ce cas précis, le vol de données bancaires.

Après avoir contacté la cellule violation de la CNIL (violations@cnil.fr) pour s'assurer que l'information soit la plus claire possible pour les destinataires, il est décidé de l'écrire sous la forme de réponses aux questions suivantes :

- « Que s'est-il passé ? »
- « Comment avons-nous réagi ? »
- « Quelles données sont concernées ?»

- « Quelles sont les conséquences possibles ? »
- « Quelles sont nos recommandations ? »
- et « Qui contacter si vous avez des questions ? ».

3. **Compléter la notification.** À la suite de l'information des personnes concernées, Dan réalise une **notification complémentaire** auprès de la CNIL et transmet les **nouveaux éléments** : un chiffre affiné du nombre de personnes concernées, le descriptif du cheminement pris par l'attaquant, les mesures mises en œuvre afin que cela ne se reproduise plus, le nombre de personnes informées et un modèle non nominatif du message adressé à ces dernières.

4. **Éviter de nouvelles attaques**. Une fois la crise gérée, Dan, dont la hiérarchie a déjà diligenté un audit interne, reviendra vers le sous-traitant sur l'insuffisance de ses mesures de sécurité et demandera le renforcement de celles-ci compte tenu des risques.

Comment limiter ce risque ?

☐ En tant que responsable de traitement, imposez des mesures de sécurité et des audits réguliers à vos sous-traitants dans vos contrats.

☐ Ne permettez pas le partage de comptes ou de mots de passe au sein d'une équipe : chaque utilisateur doit avoir un compte personnel, cela est nécessaire en cas d'attaque afin de retracer le déroulé et savoir d'où la compromission est partie ; par ailleurs, la vente de comptes de la part d'employés est une réalité, un compte personnel limite ce risque.

☐ Assurez-vous qu'une journalisation fine des accès et actions est mise en place sur toutes les applications.

☐ Analysez de façon proactive les journaux ainsi générés afin de détecter les évènements suspects pour pouvoir les traiter le plus rapidement possible. Informez vos clients de mesures de sécurité mises en place.

☐ Evitez la possibilité d'un accès malveillant aux outils depuis Internet. Imposez l'utilisation d'un VPN et d'une authentification multi facteur pour les accès distants.

☐ Ne permettez pas aux utilisateurs, sauf pour des rôles bien définis pour lesquels il s'agit d'une absolue nécessité, la possibilité de télécharger l'ensemble des données : limitez cette possibilité à la fois en termes d'étendue des droits d'accès et de fréquence et de taille des requêtes.

☐ Mettez en place une ségrégation forte entre les différentes bases de données, clientes ou autre, et réalisez des audits sur ce point.

Pour approfondir

- Les violations de données personnelles
- Tous les contenus sur la cybersécurité