Fraude via une combinaison de techniques : comment gérer ces violations de données ?

19 mars 2024

Régulièrement, la CNIL communique sur des violations de données typiques inspirées d'incidents réels qui lui sont notifiés. L'objectif est de permettre aux professionnels de comprendre et de prévenir les risques d'accès à des données par des tiers.

> Télécharger le PDF

Découvrir toute l'histoire de Manon et César

Différentes techniques pour un seul objectif : la fraude

Après un rendez-vous chez son cardiologue, Manon dépose ses justificatifs dans l'espace personnel du site de sa mutuelle afin d'obtenir un remboursement. Dans son historique, elle découvre la présence de **remboursements dont elle ne connaît pas l'origine.** Son **relevé d'identité bancaire (RIB) ainsi que d'autres données personnelles ont été modifiés** à son insu.

En réaction, elle contacte immédiatement le service client par téléphone et signale sa suspicion de fraude. Elle se souvient alors avoir reçu, quelques semaines auparavant, un courriel de sa mutuelle contenant un lien sur lequel elle avait cliqué pour répondre à une enquête, mais sans succès, la page ne s'affichant pas après qu'elle se soit authentifiée.

Aussitôt après ce signalement, **César, délégué à la protection des données (DPO) de la mutuelle**, est appelé en urgence par **le responsable du service fraude** de son entité. Ce dernier est accompagné du responsable de la sécurité des systèmes d'information (RSSI) : **une fraude** a été détectée après plusieurs signalements et analyses techniques. Un ou plusieurs tiers malveillants ont accédé à plusieurs centaines de comptes d'assurés et ont modifié leurs données personnelles, notamment les RIB. L'analyse a montré que plusieurs RIB identiques, de banques ayant manifestement procédé à des vérifications documentaires insuffisantes lors de l'ouverture d'un compte, étaient utilisés sur différents comptes n'ayant, à priori, aucun lien entre eux.

Cette fraude a été effectuée par la combinaison de différentes techniques.

- Deux sources d'attaque sont isolées :
  - Le RSSI confirme qu'un pic de tentatives de connexion sur l'espace clientèle a été détecté par les outils informatiques. Il est confirmé qu'il s'agit d'une attaque par bourrage d'identifiant (« *credential stuffing* ») , dont le principe est d'utiliser des couples identifiant et mots de passe provenant de violations passées en présumant que les personnes utilisent ces mêmes couples sur différents services. Cette situation étant malheureusement fréquente, un taux de réussite non négligeable a pu être obtenu par l'attaquant.
  - Des remontées effectuées auprès du service clients, il est apparu également que d'autres compromissions pouvaient être liées à une campagne d'hameçonnage (« *phishing* ») plus récente. Effectivement, pour certains clients, comme Manon, des courriels avec de faux liens de connexion ont été adressés par les attaquants et certaines personnes ont pu cliquer dessus. Se pensant en sécurité sur le site de leur mutuelle, elles ont fourni leur identifiant et mot de passe, directement aux pirates.

- Le responsable du service fraude indique ensuite qu'à partir de ces deux différentes sources, les attaquants auraient **analysé les conditions de remboursement** dont bénéficient les clients : remboursement dentaires et remboursements ophtalmologiques notamment, avant de sélectionner les clients les mieux couverts et d'effectuer la modification des données, notamment du RIB.
- Enfin, à partir de l'analyse précédente, des documents de demandes de remboursements auraient été téléversées afin d'obtenir des remboursements, sur le RIB frauduleux fournis. Ainsi, des feuilles de soin, ordonnances, devis signés et validés ont été envoyés à la mutuelle. Certaines demandes se sont appuyées sur des documents totalement faux, c'est-à-dire des falsifications de documents existants et retravaillés sur ordinateur par exemple ; d'autres sur des documents légitimes, vraisemblablement détournés ou volés auprès de professionnels de santé (vol d'imprimés et de feuilles de soins, vol de bloc d'ordonnances).

Comment réagir ?

La façon de procéder présentée ici ne reflète que l'organisation mise en œuvre par le responsable de traitement ayant servi d'inspiration à ce cas d'usage.

César et ses collègues font remonter l'information à leur direction. L'incident est qualifié de violation de données au sens du RGPD et il est décidé que le DPO procèderait à la notification de la violation de données auprès de la CNIL. César dispose donc de 72 heures pour réaliser cette notification auprès de l'autorité.

Heureusement, les procédures internes de gestion des incidents ont été suivies et il dispose d'assez de temps et éléments pour réaliser cette obligation. La direction juridique gérera, de son côté, le dépôt et le suivi de plainte auprès de la police.

Tout d'abord, César consolide les informations collectées avec le RSSI et **documente cet incident comme une violation de données personnelles**. Après analyse et consultation des conseils de la CNIL sur le sujet, César notifie la violation de données.

Il sait que la direction des systèmes d'information de son entreprise dispose de sauvegardes et d'une journalisation fine des actions effectuées sur les comptes. Il est ainsi possible pour la mutuelle de rétablir les données des usagers à leurs valeurs d'origine.

Des secrets appartenant aux usagers ayant été révélés et des modifications ayant été apportées sur les données bancaires des personnes concernées, le risque engendré par cette violation est considéré comme élevé. César, aidé du service communication, **rédige un message d'information à destination des personnes concernées**, 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 et les conséquences possibles pour les personnes concernées.

Il y explique que les données ont été rétablies, demande aux personnes de vérifier ces dernières et de signaler toute erreur.

Pour 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 ? ».

À la suite de l'information des personnes concernées, César réalise une **notification complémentaire** auprès de la CNIL et transmet les **nouveaux éléments**, à savoir, dans ce cas particulier, la mise à jour du nombre de personnes concernées qui a été affiné depuis, ainsi que le nombre de personnes informées et un modèle non nominatif du message adressé.

Bien entendu, le responsable de traitement **conserve des copies de toutes ces informations et transmissions en interne.**

Maintenant, il va falloir faire en sorte que la situation ne se reproduise plus !

Comment limiter ce risque ?

Pour éviter de vous retrouver dans la même situation que Manon et César, **suivez ces bonnes pratiques** :

1. En tant qu'usager d'un service en ligne

☐ Utilisez des mots de passe robustes, c'est-à-dire des mots de passe difficilement devinables par un ordinateur, en utilisant une combinaison des caractères alphabétiques en minuscule et majuscule, des chiffres et des caractères spéciaux et ayant une longueur importante.

☐ Un service, un site ou une application = un mot de passe (différent des autres).

☐ Stockez vos mots de passe au sein d'un gestionnaire de mot de passe.

☐ Dès que vous avez l'information – par le biais d'un responsable de traitement ou d'un service tiers - que l'un de vos mots de passe est compromis, ne l'utilisez plus.

☐ Ne cliquez pas sur les liens présents dans un courriel, connectez-vous à votre service par le biais de l'application ou du site web dédiés.

☐ Lorsque qu'un service vous propose une authentification multi facteur (« *MFA* »), utilisez-la !

2. En tant que responsable de traitement

☐ Sensibilisez de façon régulière vos usagers aux bonnes pratiques, informez-les que vous ne leur demanderez jamais la communication de leurs mots de passes ou autre données sensibles par le biais de courriels.

☐ Indiquez-leur de façon régulière quelles sont vos adresses courriels officielles.

☐ Mettez en place une journalisation fine des accès et actions sur vos systèmes.

☐ Analysez de façon proactive les journaux ainsi générés afin de détecter les évènements suspects pour pouvoir les traiter le plus rapidement possible.

☐ Élevez le niveau de protection autour de certaines données : en cas de modifications de RIB, adresse courriel, téléphone ou encore mot de passe, par exemple, envoyez un message automatique à l'utilisateur, voire demandez une authentification d'un niveau supérieur.

☐ Proposez une authentification multi facteur (« *MFA* »), soit pour l'ensemble du service soit lors de l'accès en visualisation ou modification de certaines données.

☐ Mettez en place une limitation de taux (« *rate limiter* ») afin de limiter la répétition de tentative de connexions malveillantes.

☐ Mettez en place des CAPTCHAS afin d'élever le niveau de protection contre les attaques automatisées.

Pour approfondir

- Les violations de données personnelles
- Tous les contenus de la CNIL sur la cybersécurité
- Phishing : détecter un message malveillant
- Que faire en cas de phishing ou hameçonnage ? - ANSSI