Vol de matériels et détournement de services dans le cadre scolaire : comment gérer les violations de données ?

15 avril 2024

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 par des tiers en présentant un exemple de réaction appropriée.

> Consulter au format PDF

Découvrir toute l'histoire d'Hubert et son équipe

Le contexte

Hubert, directeur du groupe scolaire René Coty, met en œuvre depuis plusieurs années la numérisation de son établissement. Dans ce cadre, des équipements tant matériels que logiciels ont été déployés.

Ces outils sont partagés entre les différentes activités scolaires et périscolaires proposées par l'établissement. Des tableaux numériques, ordinateurs portables et tablettes ont été mis à disposition des personnels et des élèves, ainsi que des espaces numériques de travail (ENT). En particulier, les tablettes numériques sont partagées entre professeurs des écoles.

Un incident peut en cacher un autre

En fermant l'école le vendredi soir précédant les vacances de Noël, **Hubert ne retrouve plus la tablette** malgré de minutieuses recherches. En tant que responsable, il applique alors la procédure habituelle et consigne la perte du matériel.

Pendant les vacances scolaires, Hubert est alerté par les représentants des parents d'élèves : **des messages étranges ont été envoyés** par le biais de l'ENT, **des cahiers de textes numériques ont été supprimés** et **des notes d'élèves ont été effacées ou modifiées.**

Hubert contacte son prestataire pour l'ENT et lui explique la situation. Le prestataire lui indique lancer une investigation immédiate. L'équipe sécurité de l'ENT, après une journée et demi d'enquête approfondie, ne trouve aucune trace de compromission extérieure. En revanche, l'analyse des journaux indique que **ces envois, suppressions et modifications ont été réalisées par un compte connu**, celui de **Dolorès, professeure des écoles en CM1**, qui se serait connectée tard dans la nuit du dimanche au lundi.

Devant cette situation incongrue, Hubert contacte Dolorès qui lui indique ne pas être à l'origine de cette connexion, ni même de ces envois ou modifications. Dolorès précise par ailleurs ne plus être ne possession de son équipement informatique.

Hubert fait alors **le lien entre la disparition de la tablette et cette activité non désirée sur l'ENT**. Dolorès lui confirme laisser ses sessions ouvertes sur le navigateur et avoir, par ailleurs, enregistré dans le navigateur de la tablette son identifiant et mot de passe, en méconnaissance des risques

Comment réagir ?

La façon de procéder présentée dans ce document ne reflète que l'organisation mise en œuvre par le directeur d'établissement ayant servi d'inspiration à ce cas d'usage.

Hubert a entrepris les actions suivantes pour respecter ses obligations et limiter les risques :

- **Signalement** : Hubert fait remonter l'information au délégué à la protection des données (DPO) de son académie. Il a été décidé que, sur ce cas, il gérerait lui-même la **violation de données que constitue, au sens du RGPD, l'incident**. Il dispose donc de 72 heures depuis sa découverte pour réaliser cette notification auprès de la CNIL. Grâce aux procédures internes de gestion des incidents, il dispose d'assez de temps et d'un certain nombre d'éléments pour réaliser une notification initiale. Par ailleurs il devra, comme il lui a été demandé par le rectorat, effectuer un dépôt de plainte auprès de la gendarmerie.

- **Documentation** : Hubert consolide les informations collectées auprès de Dolorès et 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, Hubert notifie à celle-ci la violation de données.

- **Rétablissement des données** : il sait, par le biais de son prestataire, qu'il dispose de sauvegardes et d'une journalisation fine des actions effectuées sur l'ENT. Il est ainsi possible pour lui de rétablir les notations des élèves et les cahiers de textes numériques à leurs valeurs d'origine, ainsi que de supprimer les messages envoyés.

- **Information les personnes concernées** : des données relatives à des mineurs ayant été compromises, le risque engendré par cette violation est considéré par Hubert comme élevé. Hubert souhaite également communiquer auprès des différentes parties prenantes. Il **rédige un message d'information à destination des parents**, 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 les vérifier et de signaler toute erreur. Il invite également les parents à être vigilants et à lui signaler directement tout évènement pouvant être lié à cette violation, notamment en cas de tentative d'hameçonnage.
  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 ? ».

- **Sensibilisation des équipes** : Hubert réunit également ses équipes afin de leur faire part de la situation et en profite pour les sensibiliser à la protection des données, notamment celles relatives aux enfants.

- **Finalisation de la notification à la CNIL** : à la suite de l'information des personnes concernées, Hubert réalise une **notification complémentaire** auprès de la CNIL et transmet les **nouveaux éléments** : la mise à jour du nombre de personnes concernées qui a été affiné depuis, le nombre de personnes informées et un modèle **non nominatif** du message adressé à ces dernières.
  Bien entendu, l'établissement scolaire **conserve 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 que votre journée soit comme celle d'Hubert et de Dolorès, **suivez ces bonnes pratiques** :

1 En tant qu'utilisateur

☐ 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 sécurisé, accessible uniquement après l'utilisation d'une clé maitresse ;

☐ 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, sur aucun système ;

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

☐ En cas d'utilisation d'un appareil partagé, utilisez des sessions personnelles différentes et sécurisées par un mot de passe robuste ;

☐ Évitez de rester connecté à vos sessions applicatives, notamment lorsqu'un appareil est partagé. En fin d'utilisation, déconnectez-vous.

2 Du côté du responsable de traitement (l'établissement)

☐ 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 ;

☐ Définissez, testez et améliorez vos procédures de gestion des incidents ;

☐ Assurez-vous qu'une journalisation fine des accès et actions est mise en place sur vos applications ;

☐ En tant que sous-traitant proposant un outil hébergé, 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 ;

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

☐ N'autorisez l'utilisation que d'équipements et supports mobiles chiffrés par défaut, évitez de les laisser sans surveillance, non attachés et avec des sessions non verrouillées ;

☐ Imposez, à vos utilisateurs et personnels, l'utilisation de sessions personnelles, associées à un compte nominatif individuel protégé par un mot de passe robuste ;

☐ Demandez à disposer de sauvegardes régulières de vos applications et que des tests de rétablissements soient effectués.

Pour approfondir

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