Cyberattaque : le sous-traitant au centre de la crise

27.5.2026 - | Commission Nationale de l'Informatique et des Libertés

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'incidents réels notifiés à la CNIL.

L'histoire d'Alice la RSSI et Charles le délégué à la protection des données

En 2026, plus que jamais, les systèmes d'information des entreprises sont continuellement visés par des attaques tant opportunistes que ciblées. Il est primordial pour tout responsable de traitement de prendre, en amont, les mesures nécessaires afin de contrer les acteurs de la menace et défendre son patrimoine informationnel et les données personnelles.

Les responsables de la sécurité des systèmes d'information (RSSI) et délégués à la protection des données (DPO) sont mobilisés afin d'assurer la conformité des traitements des données et la mise en œuvre de mesures de sécurité adéquates.

Une violation chez un sous-traitant, des impacts multiples

Alice (RSSI) et Charles (délégué à la protection des données) travaillent pour un sous-traitant qui propose à ses clients une solution en nuage (*cloud*) leur permettant la gestion de leur clientèle et de développer leur activité.

Malgré les mesures de sécurité mises en œuvre, des pirates informatique tentent continuellement d'attaquer les systèmes d'information, en profitant de la nuit, des week-ends et des périodes de congés.

Les attaquants n'ont besoin que d'un seul succès là où Alice et Charles ont pour tâche de surveiller tous les accès, vérifier chaque activité, corriger chaque erreur logicielle. L'entreprise peut s'appuyer sur des prestataires ou des solutions techniques et organisationnelles, mais ils ne sont pas à l'abri de failles, d'erreurs, ou de mauvaises décisions.

Un pirate a réussi à trouver un point de contact en interne. Avec habileté, il use d'ingénierie sociale et **réussit à faire exécuter un code à un employé négligent et mal préparé**. À partir de là, il gagne ainsi l'accès au système d'information du sous-traitant. **Il dispose à présent de la possibilité de parcourir le réseau interne**. Il accède aux données non structurées accessibles sur les espaces de partage interne ainsi qu'aux hyperviseurs sur lesquels les machines virtuelles des clients sont exécutées. **Le pirate copie ainsi un maximum de données de l'entreprise, mais également des sociétés clientes, sans se faire détecter**.

Alice est sollicitée au cours de sa pause estivale par ses équipes. **Des activités suspectes sont remontées par les** outils de supervision . Elle analyse rapidement les premières remontées, parvient à déterminer qu'une activité anormale est bien en cours, qu'une fuite est avérée. Elle enclenche la procédure prévue : remontée de l'alerte aux personnes désignées et mise en protection du système, ce qui plonge l'entité et ses clients dans le « *blackout* ».

Comment réagir ?

Le principe :

- le sous-traitant doit aider ses clients concernés par la violation à effectuer leur notification – il doit également faire une notification pour lui-même car, dans le cas présent, des données qu'il traite pour son propre compte ont été exposées ;
- les personnes doivent être correctement informées en cas de risque élevé.

- ## Définir qui doit faire quoi

La cellule de crise se réunit afin d'analyser la situation.

Dans un premier temps, Alice et Charles doivent faire un état des lieux afin de confirmer la méthodologie de l'attaque et d'en connaître son ampleur et ses impacts directs. Les équipes techniques commencent, des prestataires dédiés sont prévenus et renforcent les investigations.

Ils doivent gérer la situation auprès des équipes en interne, mais également auprès des clients et du monde extérieur, notamment de la presse qui s'intéresse de plus en plus aux violations de données.

La gestion de tels incidents est complexe et multiforme, **il est important que chacun sache quoi faire et que la communication entre les décisionnaires soit claire et limpide**.

Sur l'aspect RGPD, il est décidé que Charles serait la tête de pont. Il y a deux points principaux à gérer de son côté :

- La **violation subie** par son entité, **en tant que responsable de traitement** ;
- La **violation subie par ses clients**, responsables de leurs propres données et ayant choisi l'entreprise de Charles comme sous-traitant.

- ## En tant que responsable de traitement : notifier la violation à la CNIL sous 72 heures

S'agissant de la violation subie en tant que responsable de traitement, Charles va devoir récupérer les éléments auprès des équipes techniques, déterminer quelles sont les données concernées, estimer un niveau de risque pour les droits et libertés des personnes concernées (majoritairement les employés dans son cas) et effectuer les actions nécessaires.

Charles va donc 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.

Il connaît les prochaines étapes :

1. **Documenter et notifier à la CNIL**. Il consolide les informations collectées 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 par le biais du téléservice dédié.
2. Bien que cela ne soit **pas requis par le RGPD**, il est décidé que la notification effectuée auprès de la CNIL englobera deux parties : la première, classiquement, comportera **les éléments concernant la violation** touchant directement l'entreprise, **en tant que responsable de traitement**. Il sera également ajouté une **seconde partie concernant les clients**. L'objectif est double : aider les clients dans leur démarche et fournir les informations d'une façon centralisée et la plus pertinente possible.
3. **Informer les personnes** en fonction du risque. En effet, le RGPD prévoit que les personnes concernées doivent être informée **si le risque est considéré comme élevé**.

Il y a deux populations à gérer pour Charles :

- « ses » employés, c'est-à-dire ceux pour lesquels sa société est responsable de traitement ; et
- « ses » clients, pour lesquels il agit en tant que sous-traitant, mais qu'il va **aider et conseiller**, étant le mieux placé pour réaliser l'analyse de risque.

Il peut parfois être nécessaire de réaliser des investigations afin de savoir quelles données sont réellement concernées, d'effectuer une analyse détaillée des éléments concernées. Analyser des données non structurées aux seins de répertoires sur des dossiers de partage peut prendre du temps.

À court terme, en lien avec l'équipe de gestion de crise, Charles décide de diffuser **une information globale en interne sur l'incident, ainsi qu'à l'ensemble des clients**. Une information détaillée et dédiée sera réalisée ensuite pour les individus victimes si la violation engendre un risque élevé pour leurs droits et libertés.

- ## En tant que sous-traitant : accompagner les clients à effectuer leur notification

S'agissant de **la violation subie en tant que sous-traitant**, l'entreprise de Charles **doit informer le plus rapidement possible les responsables de traitement concernés** afin que ces derniers puissent remplir leurs différentes obligations, notamment vis-à-vis du RGPD. Ces derniers n'étant pas nécessairement des experts sur le sujet, l'entreprise de Charles va les aider et accompagner dans cette démarche.

Il y a, à ce stade, la nécessité de **gérer la violation en deux étapes**.

1. Dans un **premier temps** court, chaque client a subi une violation par la perte de **disponibilité** causée par la coupure du service par Charles. Cette coupure, non prévue, pouvant perdurer, génère un risque et entraîne l'obligation pour chaque responsable de traitement de notifier la violation.
2. Dans un **second temps**, il faudra déterminer ceux pour lesquels une atteinte à la **confidentialité** est avérée et de mener les actions adéquates.

Charles avait déjà prévu la situation. Il dispose des ressources permettant d'affronter la situation :

- **Un guide rédigé en interne (une bonne pratique)** permettant aux clients de réaliser leur

notification pas à pas et correctement. Dans ce guide, il est prévu que l'entreprise cliente fasse figurer, dans sa propre notification, le numéro de la notification déposée par l'entreprise de Charles : cela permet à la CNIL de mieux comprendre l'ampleur de la violation. Il a également **adapté** le guide pour les clients étrangers, en indiquant les coordonnées de l'autorité de protection des données à contacter.

- En lien avec le service communication et la cellule de crise, l'entreprise envoie **un message à destination des entreprises clientes**. De même, une ligne téléphonique dédiée est ouverte et les salariés répondant sur cette ligne sont formés sur le sujet afin de pouvoir répondre ou aiguiller correctement les interlocuteurs.
- L'entreprise de Charles propose également de **réaliser les actions** de notification **pour le compte des clients**, **en leur nom et après leur accord formel uniquement**. Cette option est tout à fait envisageable si le sous-traitant dispose de toutes les informations permettant aux responsables de traitement impactés de satisfaire leurs obligations auprès de la CNIL.

Par ailleurs, **des mises à jour** de la situation sont faites de façon **régulière** auprès des clients afin de les tenir informés de la situation et de l'évolution de cette dernière.

Au fur et à mesure que la situation s'éclaircit et que le périmètre touché se précise, Charles va être en mesure d'alerter les clients pour lesquels une atteinte à la **confidentialité** est établie et pour lesquels il sera nécessaire de **compléter la notification initiale effectuée**.

Au regard des données dérobées, le risque pour les droits et libertés des individus est considéré comme élevé : il sera donc nécessaire d'informer les personnes concernées.

Les collègues de Charles conçoivent une **trame de message d'information à destination des individus concernés**, qu'il propose à ses clients afin de les aider dans cet exercice. Il est obligatoire dans ce cas de fournir certains éléments : 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 (arnaques, usurpation d'identité, réutilisation de données bancaires, etc.).

Après avoir contacté la cellule violation de la CNIL () 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 ? ».

Avec l'appui de sa structure, d'Alice et de la cellule de crise, Charles est en mesure de gérer la notification de violation de sa société, mais également d'aider les clients à gérer leur propre notification.

https://www.cnil.fr/fr/cyberattaque-le-sous-traitant-au-centre-de-la-crise