Cyberattaque : le sous-traitant au centre de la crise

Aujourd’hui, les entreprises sont continuellement visées par des attaques ciblées sur leurs systèmes d’information.

Justement, un pirate s’interesse à un sous-traitant qui propose à ses clients une solution en nuage (*cloud*). Avec habilité, il use d’ingénierie sociale et réussi à tromper un employé peu vigilant. Il gagne ainsi l’accès à leur système d’information, et copie un maximum de données de l’entreprise, mais également de sociétés clientes, sans se faire détecter.

Alice, responsable de la sécurité des systèmes d'information (RSSI) et Charles, délégué à la protection des données (DPO) travaillent chez ce sous-traitant.

Des activités suspectes sont remontées par les outils de supervision. Après analyse, Alice confirme la fuite et 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* ».

La violation concerne l’entreprise de Charles (en tant que responsable de ses propres données), mais également les entreprises clientes.

Concernant son entreprise, Charles récupère des éléments auprès des équipes techniques :

- **quelles données ont fuité ?**
- **quel est le niveau de risque pour les personnes concernées, dont les employés de l’entreprise ?**

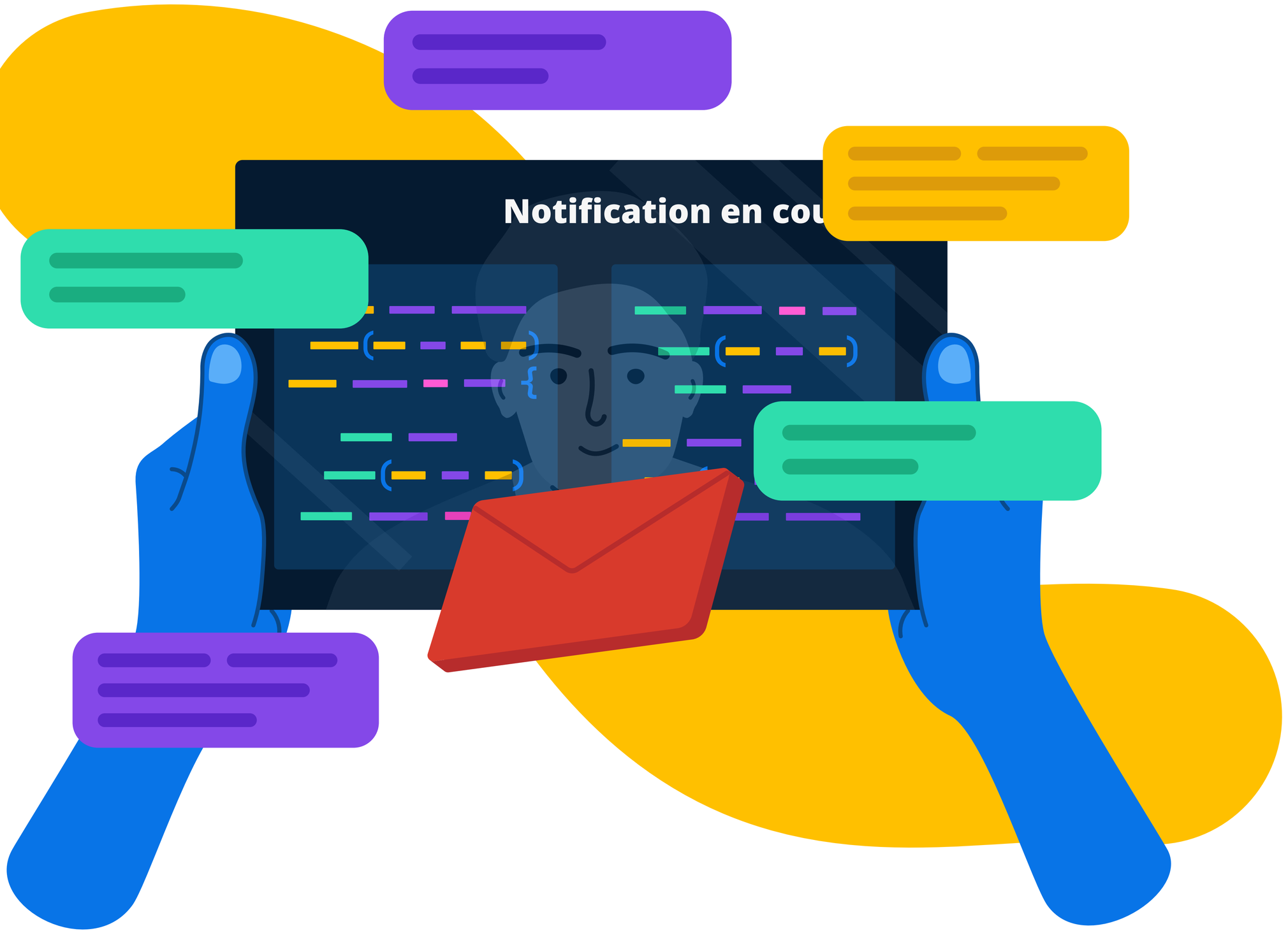
Cela lui permet d’identifier les actions à mener.

Il notifie la violation à la CNIL sous 72 h.

Charles doit également informer le plus vite possible les entreprises clientes pour qu'elles puissent remplir leurs propres obligations.

Charles envoie à chaque client un message d'information accompagné d'un guide d'aide à la déclaration et ouvre une ligne téléphonique dédiée pour répondre aux questions.

Bien que ce soit facultatif, Charles leur propose d'effectuer la notification à leur place, avec leur accord formel.



Le vol de données présente un risque élevé pour les droits et libertés des individus : chaque entreprise cliente concernée devra les informer de la violation le plus clairement possible. Charles leur propose un modèle de message d'information :

- **Que s'est-il passé ?**
- **Comment avons-nous réagi ?**
- **Quelles données sont concernées ?**
- **Quelles sont les conséquences possibles ?**