Cybersécurité : 15 mises en demeure à l'encontre de sites web insuffisamment sécurisés

08 juillet 2022

Dans le cadre de la thématique prioritaire sur la cybersécurité du web français, la CNIL a contrôlé vingt-et-un organismes en 2021. Quinze ont été mis en demeure pour des défauts de chiffrement des données ou de gestion et de sécurisation de comptes d'utilisateurs.

De forts enjeux pour les organismes et les personnes concernées

Dans le cadre de l'une de ses thématiques prioritaires de 2021, « la cybersécurité du web français », la CNIL a réalisé une série de contrôles en ligne et sur pièces (c'est-à-dire sur la base de documents transmis) auprès de vingt-et-un sites web d'organismes français du secteur public (communes, centres hospitaliers universitaires, ministères…) et du secteur privé (plateformes de e-commerce, prestataires de solutions informatiques...).

Cette thématique a été privilégiée par la CNIL car **les défauts de sécurité des sites web figurent parmi les manquements les plus souvent constatés lors des contrôles**, et sont susceptibles de conduire à des violations de données personnelles.

Les violations de données personnelles en 2021

5 037 notifications reçues en 2021

+ 79 % par rapport à 2020

43 % concernent une attaque par rançongiciel

Ces contrôles ont également eu pour but de renforcer le niveau de sécurité des sites web édités par les collectivités territoriales, notamment car elles sont particulièrement susceptibles d'être victimes d'attaques informatiques telles que des rançongiciels.

L'ensemble des vérifications faites par la CNIL l'a amenée à **clore** six procédures et à **mettre en demeure** quinze organismes :

- **les clôtures,** justifiées par la faible gravité des manquements constatés, prennent la forme d'un courrier alertant les responsables de traitement sur les mesures à mettre en œuvre afin de se conformer totalement au RGPD ;
- **les mises en demeure** portent sur des pratiques non conformes à des points de sécurité importants, rendant les organismes vulnérables à des attaques informatiques.

Les principaux manquements constatés par la CNIL

Les manquements relevés par la CNIL portent sur l'obligation générale du responsable de traitement de sécuriser les données personnelles traitées (article 32 du RGPD).

La CNIL s'est référée aux recommandations délivrées par l'ANSSI en matière de sécurité, en particulier, pour le secteur public, dans le référentiel général de sécurité (RGS). Celui-ci fixe les règles que les téléservices mis en place par des administrations doivent obligatoirement respecter pour assurer la sécurité des informations échangées.

La CNIL s'est également appuyée sur sa recommandation relative aux mots de passe de 2017, actuellement en cours de mise à jour et soumis à consultation publique.

Les vérifications réalisées par la CNIL ont donc essentiellement porté sur des points techniques et organisationnels.

Des données insuffisamment chiffrées

Concernant la robustesse du chiffrement des données, la CNIL a constaté que de nombreux acteurs permettaient un accès non sécurisé (HTTP) à leur site web, mettaient en place des versions obsolètes du protocole TLS devant assurer la sécurité des données en transit, utilisaient des certificats et des suites cryptographiques non conformes pour les échanges avec les serveurs des sites contrôlés.

Des comptes utilisateurs à protéger

Concernant la gestion des comptes utilisateurs, la CNIL a principalement constaté le défaut de dispositifs permettant de tracer les connexions anormales aux serveurs.

Concernant la sécurisation de l'accès aux comptes utilisateurs, la CNIL a notamment constaté le recours à des mots de passe insuffisamment robustes et des procédures permettant de les renouveler ne sécurisant pas suffisamment leur transmission et leur conservation.

Les organismes mis en demeure disposent d'un délai de trois mois pour prendre toute mesure permettant d'assurer un niveau de sécurité adapté.

Texte reference

Les textes de référence

> Article 32 du RGPD
Texte reference

Pour approfondir

> Sécuriser les sites web
> Guide de la sécurité des données personnelles (PDF, 413 ko)
> La CNIL publie une recommandation relative aux mesures de journalisation
> Le contrôle de la CNIL
> La procédure de mise en demeure
Document reference

Cybersécurité - Le RGPD : la meilleure prévention contre les risques cyber

Cybersécurité - Chiffres 2021
[PDF-803 Ko]