



COMMUNIQUE DE PRESSE

Rennes, le 29 Juillet 2023



Une trentaine de professionnels du CHU a reçu ce jour un mail suspect, non encore authentifié, menaçant le CHU d'une diffusion, sur le darkweb, de tout ou partie des données ayant fait l'objet d'une exfiltration illégitime lors de la cyberattaque intervenue le 21 juin dernier.

Les professionnels du CHU ont été alertés dès ce matin et invités à ne surtout pas donner suite aux instructions mentionnées, en informant immédiatement les équipes de sécurité informatique.

En parallèle, le CHU en a immédiatement informé les autorités compétentes qui procèdent actuellement aux investigations nécessaires.

Pour mémoire, il n'est pas possible à ce jour d'identifier avec précision la nature exacte et le contenu des données qui ont fait l'objet de cet accès illégitime mais le CHU a constaté un potentiel accès à des fichiers informatiques contenant des données de santé, associées ou non à une identité, sur un périmètre restreint des systèmes informatiques du CHU de Rennes. Les données concernant les patients auxquelles l'attaquant a potentiellement eu accès relèvent du Centre de Soins Dentaires (CSD), des salles techniques de cardiologie et des laboratoires du CHU. Il ressort par ailleurs des investigations menées, que des données à caractère personnel des professionnels du CHU sont également concernées par la fuite des données (numéro de sécurité sociale, bulletin de salaires).

Une plainte a été déposée par le CHU de Rennes dès le 22 juin 2023. Une enquête est en cours, sous l'égide du Parquet de Paris, spécialisé dans le traitement judiciaire des cyberattaques.

Une notification a également été effectuée auprès de la commission nationale de l'informatique et des libertés (CNIL) dès le 21 juin 2023 comme prévu par l'article 33 du règlement européen sur la protection des données (RGPD).

Parallèlement, les professionnels du CHU ont été informés et accompagnés dans l'application des recommandations nationales disponibles en matière de protection des données personnelles.

Une information générale concernant la fuite de données personnelles et les recommandations liées est également organisée pour les patients par voie de presse, par affichage dans les salles d'attente ainsi que par un courrier en ligne sur le site internet de l'ARS Bretagne.

Conformément aux recommandations nationales émises par la CNIL, le CHU invite les patients et les professionnels à la plus grande vigilance face aux risques d'escroquerie ou d'hameçonnage qui pourraient survenir dans les prochaines semaines. En cas de constatation d'une utilisation frauduleuse de leurs données personnelles, il est recommandé aux patients de porter plainte rapidement. Ils sont également invités à en informer le CHU via l'adresse mail cyberattaque@chu-rennes.fr. Un dispositif similaire est développé pour les professionnels.

Les équipes du CHU restent pleinement mobilisées pour traiter cette cyberattaque et ses conséquences sur les personnels et patients.

Contacts presse :

CHU de Rennes / Direction de la communication – 02 99 28 42 40 – direction.communication@chu-rennes.fr

