NOTE D'ALERTE

N° 7973/1828/2019 GEND/PJGN/SCRCGN du 19 février 2019

SERVICE CENTRAL RENSEIGNEMENT CRIMINEL

PLANIFICATION COLLECTE TRAITEMENT DIFFUSION ANALYSE

LES ESCROQUERIES AU RGPD (Règlement général sur la protection des données) : une nouvelle niche pour les escrocs.

Avec l'adoption du Règlement Général sur la Protection des Données (RGPD), de nombreux escrocs ont vu dans cette norme européenne une nouvelle niche pour extorquer de l'argent à des entreprises et collectivités encore trop peu au fait des démarches qu'elle impose. Leur faisant craindre des sanctions pécuniaires en cas de non-mise en conformité, les individus parviennent à se faire remettre quelques centaines d'euros en échange d'une mise aux normes factice, par téléphone ou par une technique de hacking.

Le Règlement Général sur la Protection des Données est un règlement de l'Union Européenne qui constitue **le texte de référence** en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Europe.

Ce règlement, adopté par le Parlement Européen en avril 2016, est applicable depuis le 25 mai 2018 et revêt un caractère obligatoire dans les **entreprises et associations** des 28 Etats membres ainsi que celles issues des pays hors UE mais collectant et traitant des données de résidents européens (comme Google ou Amazon par exemple). La date butoir de la mise en conformité a été fixée au 25 mai 2018.

Il est à noter qu'en cas de non-respect du RGPD, plusieurs sanctions peuvent être appliquées par la CNIL (article 58 du RGPD), de manière graduelle en fonction de la gravité des actions constatées contraires au RGPD.

Dès la mise en application de ce règlement, les escrocs se sont emparés de l'actualité pour frauder et mettre en place des escroqueries, jouant sur la crainte engendrée par les lourdes sanctions prévues en cas de non-respect de la législation.

Des manières d'opérer plus ou moins perfectionnées

De manière générale, les victimes sont contactées par les escrocs par différents moyens : courrier, téléphone, ou fax. Leur interlocuteur leur indique qu'ils ne sont pas en conformité avec le règlement et que de fait, ils risquent des **sanctions** (amendes, poursuites pénales et financières, voire contrôle de l'URSAFF ou redressement de 4% du chiffre d'affaires). Il leur est alors demandé soit de contacter par téléphone une plateforme téléphonique soit de se connecter sur un site web afin d'effectuer un paiement pour procéder à un diagnostic des données, ou pour payer un pseudo-service de mise en conformité.

Les victimes s'exécutent et communiquent leurs coordonnées bancaires. Le prélèvement est effectué immédiatement.

Les hackers ont également profité de cette opportunité. On constate l'apparition d'une nouvelle génération de Ransomware

(logiciel informatique malveillant qui prend en otage des données et demande une rançon pour les débloquer): le **Ransomhack**. À la différence du Ransomware, **les données de la victime ne sont pas cryptées; l'auteur menace de les diffuser** sur le web ou de rendre public la fuite des données, ce qui induirait des sanctions pour l'entreprise indélicate. En effet, l'article 33 du RGPD prévoit des sanctions pouvant atteindre 4% du chiffre d'affaires si les données sont insuffisamment protégées..

Certaines victimes s'aperçoivent de l'escroquerie lorsqu'elles ne parviennent plus à joindre leurs interlocuteurs ou après avoir pris des renseignements auprès de la CNIL qui les informent que la mise en conformité est gratuite. Quelques-unes réussissent à faire opposition au prélèvement et ne sont victimes que d'une tentative. En revanche certaines entreprises ou sociétés subissent un préjudice pouvant atteindre 3 000 euros. Sur 90% des affaires renseignées dans TAJ, le **préjudice total s'élève à 57 000 euros**.

Orientations opérationnelles

#arnaquesRGPD

VIGILANCE

-Sensibilisation des entreprises, commerçants et professions libérales via les référents sûreté et dans le cadre de la PSQ (Police de Sécurité du Quotidien)

-Prise de contact avec les associations et les mairies de la circonscription par les unités de terrain aux fins d'information et de mise en garde.

En cas de doute ...

Ne répondez pas, n'envoyez pas d'argent — **Alertez votre réseau** — **Consultez le communiqué CNIL / DGCCRF ***

- Faire remonter au SCRC les éléments recueillis quant aux méthodes employées et aux auteurs identifiés.

dr.scrcgn@gendarmerie.interieur.gouv.fr

Gendarmerie nationale