Pour nous contacter :
Equipe IP/IT & Data Protection
ebarbry@racine.eu | (+33) 6.13.28.91.28

Cyberattaques : plainte pénale obligatoire à compter du 25 avril 2023

La cyber-attaque dont est victime la ville de Lille est un nouvel exemple du tsunami auquel font face les entreprises comme les acteurs publics.

Face à ce fléau, il est important que tout le monde ait en tête l'impact de l'article 5 de la loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur qui crée l'article L 12-10-1 du code des assurances.

Cet article précise que « Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime. »

L'article lui-même prévoit qu'il sera applicable 3 mois après la promulgation de la loi.

Ainsi, à compter 25 avril 2023 aucun assuré ne sera indemnisé des préjudices et pertes causés par une attaque informatique s'il n'a pas déposé plainte dans les 72h.

Cet article mérite quelques explications.

Tout d'abord il faut se féliciter qu'ait été écartée l'idée initiale qui consistait à interdire purement et simple à l'assureur de payer une rançon. Le pragmatisme est de rigueur. Si évidemment il faut tout faire pour ne pas payer de rançon et donner du grain à moudre aux pirates, dans certains cas la victime n'a pas le choix : payer ou mourir…

72h apparaît comme un délai très court mais il est calé sur le délai de notification à la Cnil et comporte le même point de départ « après la connaissance » par la victime. Ceci étant dit, la réalité est sensiblement différente car dans le cadre de la notification à la Cnil, le RGPD (article 33) précise que si la notification n'a pas été réalisée dans un délai de 72h elle est « accompagnée des motifs du retard ». Ainsi, les 72h pour les plaintes sont des délais impératifs, là où il y a un peu plus de souplesse côté données personnelles.

Le texte ne vise pas spécifiquement les rançonwares. La version première de la loi limitait effectivement l'obligation de déposer plainte pour les demandes de « paiement de rançon » Le texte final vise toutes les infractions informatiques des articles 323.1 à 323.3.1 du code pénal. Donc tout acte d'intrusion, de maintien frauduleux, d'altération du bon fonctionnement du SI, etc … doit faire l'objet d'une plainte en bonne et due forme pour que les dommages soient pris en charge par l'assureur.

Il est curieux que l'article L-12.10.1 ne vise que les infractions dites informatiques et ne porte pas sur les infractions du code pénal en matière de données personnelles qui est souvent l'un des fondements d'une plainte en cas de cyber attaque.

Dura lex sed lex, il ne serait pas nécessaire pour les assureurs de revoir leurs contrats pour tenir compte de cette évolution règlementaire donc inutile de se réjouir si une telle obligation ne figure pas noir sur blanc dans votre contrat d'assurance. Il y a tout lieu de penser que ce texte ne s'appliquera que pour les sinistres à compter du 25 avril et qu'il ne sera pas nécessaire de déposer plainte pour les sinistres en cours pour lesquels une plainte n'aurait pas été déposée.

Cette obligation s'impose aux personnes morales et aux personnes physiques « dans le cadre de leur activité professionnelle ». Exit les attaques sur des personnes physiques dans leur sphère privée. Ceci étant dit peu de personnes physiques sont assurées à titre personnel pour ce type de risque ce qui est assez désolant.

En résumé,

1. Le risque Cyber est, et reste assurable et nous ne pouvons que vous conseiller vivement de vérifier que vous être couverts pour ce type d'attaque sachant que les assurances classiques excluent ce type de risque. Il faut donc nécessairement se tourner vers une assurance cyber dédiée. Il faut noter que les conditions d'accès à ces assurances se durcissent fortement ;

2. Modifier la méthodologie interne de gestion des cas de cyber attaques pour être certain qu'elle contient bien un item sur la nécessité de déposer plainte dans le délai de 72h ;

3. Pour le dépôt de plainte Il est d'usage, notamment en cas d'urgence, de déposer une plainte directement entre les mains du Procureur ce qui est plus chronophage qu'un dépôt de plainte simple dans un commissariat ou une gendarmerie mais plus efficace. Si l'entreprise souhaite maintenir cette pratique, il lui faudra disposer d'un modèle de plainte pré-rédigé dans laquelle elle n'aura plus qu'à expliciter les faits et choisir les infractions appropriées.

Quoi qu'il en soit, la démarche en cas de cyber attaque sera la suivante à compter du 25 avril 2023 :

Etape 1 – Déclarer le sinistre à votre assureur notamment dans les cas où il est prévu une intervention urgente de prestataires spécialisés

Etape 2 – Recueillir le maximum d'informations pour procéder d'une part à la notification à la Cnil et d'autre part au dépôt de plainte dans le délai imparti de 72h. Bien entendu la plainte comme la notification Cnil pourront être complétées après le délai de 72h

Etape 3 – Analyser la situation pour voir s'il est nécessaire ou non de prévenir les « personnes concernées » dont les données auraient été compromises ou détruites.

Etape 4 – Analyser la situation sous un angle contractuel pour voir si la responsabilité d'un tiers (prestataire notamment) peut être mise en cause

Etape 5 – Documenter avec la plus grande précision possible les opérations réalisées (forensic et remédiation) pour les mettre à la disposition de la Cnil en cas de contrôle suite à la notification.

Etape 6 – Mettre à jour le registre des violations.

Et évidemment s'assurer avant toute chose de votre conformité au RGPD car vous pourriez en cas d'attaque glisser du statut de victime à celui de coupable aux yeux de la Cnil pour ne pas avoir respecté les dispositions en termes de données personnelles.

Auteurs

Eric Barbry
Avocat associé
ebarbry@racine.eu

Olivier Quelin
Juriste
oquelin@racine.eu