Alerte presse

Cyber-assurance : tout savoir sur la nouvelle obligation de dépôt de plainte sous 72h

Paris, le 21 avril 2023 **– Prévue dans la loi LOPMI, promulguée en janvier, l'obligation légale pour les victimes de cyberattaques de déposer plainte dans un délai de 72h si elles veulent être indemnisées par leur assurance entre en vigueur lundi 24 avril.**

A cette occasion, Hiscox, assureur spécialiste du risque cyber, fait le point sur les conséquences de cette nouvelle disposition et les réflexes à adopter en cas de sinistre.

« En donnant aux autorités françaises davantage de visibilité sur les cyberattaques subies par les professionnels et les entreprises, la loi LOPMI apporte des avancées significatives dans la lutte contre la cybercriminalité en France. En précisant les conditions de prise en charge des risques de cyber, elle clarifie également le cadre législatif pour les assureurs. Mais elle s'accompagne également, avec l'obligation du dépôt de plainte, de nouvelles contraintes qu'il est important de bien connaître pour agir sereinement et efficacement en cas de cyberattaque », commente Nicolas Kaddeche, Directeur technique d'Hiscox France.

Ce qui change avec la loi LOPMI

A compter du 24 avril, tout professionnel ou entreprise qui subit une attaque doit déposer plainte dans un délai de 72h maximum, à compter du moment où il a eu connaissance de l'incident.

Cette étape est obligatoire pour permettre une éventuelle indemnisation au titre d'un contrat d'assurance Cyber en vigueur. Si la plainte n'est pas déposée dans ce délai, le professionnel ou l'entreprise ne pourra pas être indemnisé par son assureur.

Cette disposition d'ordre publique s'applique à tous les contrats d'assurance en cours, quand bien même cette obligation ne figure pas dans les contrats.

les garanties d'assistance peuvent être mobilisées sans attendre de déposer la plainte pour aider à identifier la faille de sécurité et les données personnelles ou les données confidentielles compromises, préconiser les 1ères solutions pour limiter les conséquences de l'attaque et constituer un dossier de recours. Le dépôt de plainte reste obligatoire sous 72h quoi qu'il en soit.

Qui est concerné ?

Sont concernées, toutes **personnes morales** – entreprises, associations, administrations publiques – et **toutes personnes physiques** – professions libérales, travailleurs indépendants, etc. – qui subissent une cyberattaque dans le cadre de leurs activités professionnelles.

Le professionnel ou l'entreprise doit être immatriculé en France et être assuré par un contrat d'assurance français.

Les particuliers subissant une attaque à titre personnelle ne sont donc pas concernés par l'obligation. Mais le dépôt de plainte demeure recommandé pour permettre l'identification de suspects et favoriser la reconnaissance du préjudice subi par la victime.

Quels sont les types d'attaques visés par la loi ?

Toutes les cyber-attaques sont concernées :

- Attaques par logiciels malveillants dont les ransomwares
- Vols de données
- Attaques par déni de service
- Hameçonnages (phishing)
- Modification non-sollicitée d'un site Internet
- Interceptions de communication (ex. un réseau wifi public)
- Exploitation de vulnérabilité jusqu'alors non-corrigée présente dans un logiciel
- Etc.

Comment réagir en cas de cyber-attaque ?

En cas de cyberattaque, il est essentiel de connaître les consignes à suivre afin de réagir efficacement et de protéger au mieux son entreprise. Il faut donc :

- **Éteindre** les unités et les accès réseaux et **déconnecter** les sauvegardes
- **Communiquer** les consignes aux **collaborateurs**
- **Contacter immédiatement son assureur** pour limiter au plus vite les conséquences de l'incident
- **Alerter les forces de l'ordre** sans attendre, en appelant le 17 ou via l'application gouvernementale MaSécurité. Attention, cette alerte ne dispense pas du dépôt de plainte qui reste obligatoire
- **Porter plainte** dans un délai de 72h maximum à compter de la prise de connaissance de l'incident
- **Notifier à la CNIL en cas de violation de données à caractère personnel** (article 33 du RGPD), dans un délai maximal de 72h également, via le site dédié de la CNIL
- **Lancer le plan de gestion de crise**, notamment les process de continuité de l'activité prévus dans le Plan de continuité d'activité (PCA)
- **Déclarer son sinistre** par courrier à son assureur

Comment déposer plainte ?

Il est nécessaire dans un premier temps de **préparer sa plainte** pour documenter tout élément utile à l'enquête :

- Préserver toutes les traces visibles de l'attaque (photos, captures d'écran, etc.)
- Lister par ordre chronologique toutes les actions entreprises à la suite de l'attaque
- Apporter ou tenir à disposition un maximum de preuves (fichiers, photos, images, vidéos, clés USB, CD/DVD, disque dur, etc.)

La victime doit ensuite **porter plainte dans une brigade de gendarmerie ou un commissariat** dans un délai de 72h maximum à compter de la prise de connaissance de l'incident**.**

Si l'entreprise, immatriculée en France et assurée par contrat d'assurance français, est victime d'une cyber-attaque à l'étranger, deux options s'ouvrent à elle :

1. Déposer plainte en France sous 72h maximum
2. Déposer plainte dans le pays d'implantation sous 72h maximum. L'obligation de dépôt de plainte sera respectée – à condition que la cyberattaque concernée constitue également une infraction dans ce pays.

L’assureur : un soutien essentiel dès les premiers instants

Il est très important de garder en tête que les garanties d’assistance peuvent être mobilisées sans attendre le dépôt de plainte pour aider à identifier la faille de sécurité et les données personnelles ou les données confidentielles compromises, préconiser les premières solutions pour limiter les conséquences de l’attaque et constituer un dossier de recours.

« *En tant qu’assureur spécialiste, engagé aux côtés de nos clients, nous offrons un soutien précieux dans la gestion de crise. Outre l’accompagnement que nous apportons lors de la souscription du contrat d’assurance, en termes de prévention et de mise en place d’une cybersécurité robuste, nous apportons un service d’assistance disponible 24h sur 24, 7 jours sur 7, afin d’accompagner au plus près les entreprises et professionnels dans leurs démarches lorsqu’ils sont touchés par des cyberattaques pour limiter dans un premier temps les pertes et dommages, avant de préparer la phase d’indemnisation* », explique Nicolas Kaddeche.

A propos d'Hiscox en France

Hiscox, assureur spécialiste depuis 1901, est établi en France depuis 25 ans où il assure près de 100 000 particuliers et professionnels. Assureur historique de l’Art et des biens d'exception pour la clientèle privée, Hiscox a su ensuite développer son expertise dans le domaine des assurances professionnelles avec une gamme spécialisée couvrant aujourd’hui près de 500 métiers de services. Distribué via des courtiers spécialisés, des partenaires banquiers ou assureurs, Hiscox a été pionnier de l’assurance en ligne et via conseillers pour les entrepreneurs et indépendants. L’entreprise est aujourd’hui leader de l’assurance des métiers de l’informatique et du digital et a développé une offre cyber parmi les plus complètes du marché. C’est la connaissance et la compréhension des métiers de ses clients et de leurs risques, la mobilisation des meilleurs experts avant pendant et après les sinistres qui permettent à Hiscox de construire des couvertures adaptées à leurs besoins. Hiscox a l’ambition de changer l’expérience de l’assurance pour ses clients et l’objectif de protéger au mieux ce qui compte pour eux.

https://www.hiscox.fr

Contact presse:

Weber Shandwick Paris
Hiscox@webershandwick.com

Romain MERLE - 06 60 35 18 43