Fraude informatique : Comment réagir en cas de failles de sécurité ?

0

15 Oct 2015 cyber attaques, cybercriminalité, données, fraudes informatiques, sécurité

by Aurelie Magniez

Qu'elles proviennent d'une erreur, d'une négligence ou de procédés illicites, les failles de sécurité représentent aujourd'hui l'une des préoccupations majeures des entreprises.
Les enjeux sont importants : piratage des systèmes de traitement automatisé de données, perte d'informations confidentielles et stratégiques, vol de données personnelles, et lourds de conséquences sur le plan financier. A cet égard, l'entreprise victime devra vérifier sa police d'assurance pour vérifier si elle est couverte pour les risques informatiques.
Aussi, dès la découverte d'une faille de sécurité, et préalablement à toute action contentieuse, plusieurs actions doivent rapidement être mises en œuvre.

Identification et correction de la faille

En interne d'abord, il est recommandé au RSSI, au DSI, ou, le cas échéant, à la société d'expertise informatique, d'identifier la faille, de la corriger avant de mettre en place un audit de sécurité et de procéder aux mises à jour des procédures internes.

Constitution d'un dossier de preuve technique

Parallèlement, il est vivement conseillé au RSSI, au DSI ou à la société d'expertise informatique de réaliser un dossier de preuve technique, comprenant a minima un rapport d'incident et les logs de connexion aux serveurs.

Qualification juridique des faits

A l'appui des éléments rassemblés dans le dossier technique, il sera ensuite possible de qualifier juridiquement les faits et de les rattacher notamment à l'une ou plusieurs des infractions d'atteinte à un système de traitement automatisé de données (STAD).

Accès et maintien frauduleux dans un STAD

Les délits d'accès et de maintien frauduleux dans un STAD sont prévus et réprimés par l'article 323-1 du Code pénal aux termes duquel : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende ».

La protection du système par un dispositif de sécurité n'est pas une condition de l'incrimination : il suffit que le maître du système ait manifesté son intention d'en restreindre l'accès aux seules personnes autorisées.

La jurisprudence retient cumulativement les qualifications d'accès et de maintien frauduleux, lorsque le maintien fait suite à un accès frauduleux.

Extraction frauduleuse de données

Nouvellement modifié par la loi n°2014-1353 du 13 novembre 2014, renforçant les dispositions relatives à la lutte contre le terrorisme, l'article 323-3 du Code pénal incrimine désormais « le fait d'introduire frauduleusement des données dans un système de traitement automatisé » et « d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient ». Cette infraction est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Se rend ainsi coupable de l'infraction toute personne qui réalise de manière volontaire, afin de s'approprier une copie de l'usage des données, l'une ou plusieurs des actions suivantes :

- extraction (par tous moyens, de données du système de traitement automatisé de données) ;
- détention ;
- reproduction ;
- transmission.

L'article 323-3 nouveau du Code pénal permet de réprimer le « vol » de données, sans toutefois recourir à la qualification de vol.

A cet égard, dans son arrêt « Bluetouff » du 20 mai 2015, la Chambre criminelle de la Cour de cassation a reconnu l'incrimination de vol de fichiers informatiques sur le fondement de l'article 311-1 du Code pénal qui incrimine le vol, et ce même en l'absence de dépossession du propriétaire des fichiers.

Détention de programmes informatiques conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions

L'article 323-3-1 du Code pénal incrimine « le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 ».

Cette infraction est punie des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Association de malfaiteurs informatiques

Le délit d'association de malfaiteurs informatiques est prévu et réprimé à l'article 323-4 du Code pénal selon lequel : « la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

Pour être constituée, l'infraction nécessite l'existence d'un groupe organisé en vue de commettre les infractions prévues aux articles 323-1 à 323-3-1 du Code pénal.

Il faut que la participation au groupement ou à l'entente soit volontaire, c'est-à-dire que l'auteur ait eu connaissance de l'activité du groupement ou de l'entente et y ait adhéré en ayant conscience d'une activité illicite, mais il n'est pas nécessaire qu'il soit au courant de l'ensemble des activités des autres membres.

Dépôt de plainte

Une plainte devra être déposée auprès du procureur de la République territorialement compétent, qui diligentera une enquête préliminaire confiée aux services de police ou de gendarmerie spécialisés que sont :

- la brigade d'enquêtes sur les fraudes aux technologies de l'information (Befti), service de la Police Judiciaire dévolu aux infractions informatiques sur la région parisienne ;
- la sous-direction de lutte contre la cybercriminalité relève de la Direction centrale de la police judiciaire (SDLC), compétente pour les attaques à l'encontre d'un système d'information situé à l'extérieur du périmètre d'intervention de la Befti ;
- l'Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), compétente sur tout le territoire français.

Le procureur de la République a trois mois à compter du dépôt de la plainte pour apprécier l'opportunité de donner une suite judiciaire à l'affaire. Si dans ce délai, il informe la victime d'un classement sans suite ou s'il ne répond pas, la victime est alors recevable à se constituer partie civile devant le juge d'instruction, en application de l'article 85, alinéa 2, du Code de procédure pénale.

Notification à la Cnil

Si l'atteinte porte sur des traitements de données à caractère personnel mis en œuvre par une entreprise fournissant un service de communications électroniques (opérateurs de télécommunications, fournisseurs d'accès à internet), le responsable de traitement devra la notifier à la Commission nationale de l'informatique et des libertés (Cnil) en application de l'article 34 bis de la loi du 6 janvier 1978 Informatique et libertés, et ce sans délai à compter de la constatation de la violation. A la suite de cette notification, la Cnil pourra décider de procéder à une mission de contrôle, à l'issue de laquelle des recommandations (modification des durées de conservation, des mesures de sécurité, etc.) ou des sanctions pourront être prononcées (avertissement, sanction pécuniaire, etc.).

Pour les autres organismes, privés ou publics, la notification de la violation des données personnelles n'est pas, à l'heure actuelle, obligatoire.

Plan média

L'entreprise confrontée à une atteinte à son système informatique ayant conduit à une violation des données personnelles devra communiquer sur cet incident en interne et auprès de toutes personnes susceptibles de la solliciter (journalistes ou clients) et réagir très rapidement pour éviter toute diffusion d'information erronée ou inexacte, toute atteinte à sa réputation, ou encore mauvaise appréciation de l'impact de l'évènement sur son activité économique.

Si la répression des atteintes au système d'information a été largement renforcée par la loi n°2014-1353 du 13 novembre 2014 introduisant le délit d'extraction de données dans un STAD et par l'arrêt « Bluetouff » de la Cour de cassation du 20 mai 2015 qui consacre le vol de fichiers informatiques, la sécurisation du système d'information reste encore le meilleur moyen de lutter contre les failles de sécurité.

Virginie Bensoussan-Brulé
Directeur du département Pénal numérique