cybercriminalité, aspects juridiques

Bien qu'il existe différents moyens pour les cybercriminels de s'approprier de manière illégale les données personnelles d'un individu, les attaques par ransomware ou rançongiciel sont un vrai sujet d'actualité, avec une augmentation sans précédent sur les dernières années. Voici comment se protéger juridiquement.

L'Agence nationale de la sécurité des systèmes informatiques (Anssi) a traité 104 cas d'attaques par rançongiciel entre janvier et août 2020. Le FBI ainsi que Interpol soulignent l'importance d'adopter des systèmes informatiques sécurisés afin de limiter le risque d'attaques par rançongiciel. Un type d'attaque dont l'Agence européenne de la sécurité des réseaux et de l'informatique a décrété comme étant à la hausse et faisant actuellement partie des 15 menaces cyber les plus importantes.

Compte tenu de l'imposante hausse à la fois de la fréquence, mais aussi de l'ampleur des attaques cyber depuis 2018, les gouvernements n'ont plus l'option de simplement ignorer ce sujet. En effet, la protection de données personnelles ainsi que la prévention des failles de sécurité sont devenues une priorité incontournable pour tout type d'organisations à travers le monde. Dans le cadre de la crise sanitaire du Covid -19, nous avons pu observer une transition plus que significative vers le digital et ceci a eu comme résultat de largement faciliter l'accès aux données personnelles de n'importe qui par des cybercriminels. La massification du recours aux systèmes informatiques n'a fait qu'augmenter le nombre d'attaques ainsi que leur gravité ; les attaquants saisissent cette opportunité qui est, pour eux, une opportunité en or, pour lancer des attaques ciblées sur des systèmes fragilisés.

mode opératoire du rançongiciel

Tout d'abord, notons l'importance de définir ce qu'est une attaque par rançongiciel, la définition officielle donnée par l'Anssi est la suivante *« un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon »*. Lors d'une attaque par rançongiciel, le système informatique de la victime est mis hors d'état de fonctionner. Une fois que l'attaquant a procédé à mettre le système informatique hors de fonction, il va ensuite envoyer un message non chiffré à la victime en lui proposant de récupérer l'accès à ces données contre le paiement de la rançon. L'intrusion sur le système peut se faire sous plusieurs formes, par exemple à la suite de l'ouverture d'une pièce jointe ou encore simplement l'utilisation d'un site web déjà compromis. Le but recherché dans ce type d'attaque cyber est la plupart du temps d'extorquer une somme d'argent à la victime, cependant il y aussi des cas où le seul but est l'endommagement du système ciblé ou d'atteindre à la réputation de la victime.

un niveau beaucoup plus développé

Un facteur notamment plus qu'inquiétant est que les groupes de cybercriminels sont à un niveau beaucoup plus développé qu'auparavant. Alors, quand dans le passé les cibles principales étaient des particuliers, le niveau de sophistication des ces réseaux de malfaiteurs leur donne le pouvoir de s'attaquer à des cibles aux moyens financiers nettement plus importants. De grands groupes français ont subi des attaques, des collectivités locales ainsi que des établissements de santé ont aussi été victimes. Le niveau de ressources techniques ainsi que les moyens financiers de ces organisations criminelles sont en augmentation constante, et frôle le même niveau que les opérations d'espionnage gouvernementales. Ceci leur donne la capacité de s'en prendre à des cibles financièrement importantes, permettant ainsi la demande de rançons considérables, ces sommes atteignant plusieurs millions d'euros.

impact

Ces attaques peuvent avoir un impact plus que significatif sur leurs victimes, elles entraînent généralement une dégradation d'activité, voire un arrêt complet, et, dans le cadre d'une entreprise, il peut même en aller de sa survie. Dans l'éventualité où la rançon est effectivement payée, les attaques offrent un modèle économique très rentable aux cybercriminels. C'est exactement pour cette raison que payer la rançon n'est jamais la solution conseillée, le paiement ne fait rien d'autre qu'entretenir

cette activité criminelle et ne garantit en aucun cas la bonne récupération des données personnelles.

les bons réflexes

Comment réagir en cas d'attaques par rançongiciel ? Tout d'abord, adopter les bons réflexes pour tenter de réduire les dégâts. La première chose à faire est de déconnecter l'ensemble des ordinateurs de la connexion internet et du réseau informatique, bien évidemment les ordinateurs qui ont déjà été infectés, mais aussi le reste des machines qui pourraient potentiellement être touchées. Afin d'éviter la propagation aux appareils encore indemnes, il est crucial de déconnecter les supports de sauvegarde après avoir obtenu la certitude que ces derniers ne sont pas infectés. Après l'exécution de ces premières étapes, il est conseillé d'éteindre la totalité des systèmes informatiques utilisés et de contacter une société spécialisée en cybersécurité.

dépôt de plainte

La conservation de preuves est aussi un élément important à prendre en compte, ceci sera utile lors du dépôt de plainte aux autorités. La constitution du dossier des preuves techniques est généralement entreprise par la DSI de l'organisme victime et les experts en cybersécurité.

Des copies physiques des serveurs touchés, des fichiers chiffrés ou, encore mieux, le message piégé serviront comme preuves de l'attaque. Le dépôt de plainte au commissariat de police ou alors au procureur de la République se fait lorsque toutes les preuves utilisables ont été réunies. Une fois la plainte déposée, une enquête préliminaire est confiée aux services de la Brigade de lutte contre la cybercriminalité (BL2C) ou à l'Office central de la lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)
Le dépôt de plainte permet une qualification juridique des faits, c'est-à-dire de rattacher les faits de l'attaque à une ou plusieurs infractions listées dans le Code pénal, par exemple accès frauduleux à un système de traitement automatisé de données (STAD), extraction, détention, reproduction ou transmission de données issues d'un STAD ou encore extorsion de fonds ou tentative de ce délit, si la rançon n'est pas payée.

notifier la Cnil

Faut-il informer la Commission nationale de l'informatique et des libertés (Cnil) de la violation de données ? L'obligation légale est de notifier la Cnil de tous cas de violation de données personnelles dans un délai maximal de 72 heures, sauf à justifier du motif du retard. Les informations généralement exigées sont les suivantes : la nature de la violation (perte de confidentialité, intégrité ou disponibilité), les conséquences possibles de la violation pour les personnes concernées, les coordonnées de la personne à contacter (le délégué à la protection des données de l'organisme, s'il en existe un) et les mesures prises pour remédier à la situation et en limiter les conséquences.

plan média

En outre, la mise en place d'un plan média adapté est essentiel afin d'éviter toute diffusion d'informations erronées ou inexactes qui pourrait porter préjudice à la réputation de l'organisme. Il s'agit donc, tout d'abord de communiquer en interne a toutes personnes affectées, mais aussi à toutes autres personnes susceptibles de la solliciter (autorités de tutelle, clients, fournisseurs, presse). ■

Thaut Images/AdobeStock

Raphaël Liotier
[avocat au Barreau de Paris, responsable d'activité du département droit pénal de l'informatique et du numérique]

Edouard Turchi
[étudiant en droit, stagiaire au sein du département droit pénal de l'informatique et du numérique
Lexing Alain Bensoussan - Avocats]
→ www.alain-bensoussan.com