DROIT PÉNAL DES AFFAIRES

Cybercriminalité et vie des affaires : quels sont les risques et comment s'en prémunir ?

Au mois de septembre, le Premier ministre a annoncé qu'un budget conséquent serait alloué à la police et à la gendarmerie afin de lutter efficacement contre les nouvelles formes de délinquance et notamment la cybercriminalité. Les cyberattaques à l'égard des entreprises se multiplient, dans un contexte international tendu, et deviennent de plus en plus sophistiquées et donc imprévisibles. On ne soulignera donc jamais trop la nécessité de se protéger efficacement contre ce type d'attaques en assurant la sécurité de ses outils informatiques et la formation de ses employés aux bons réflexes.

Par Camille Potier, associée,

Le terme général de cybercriminalité désigne à la fois les délits qui sont « numériques » par nature, comme l'atteinte à un système de traitement automatique de données (STAD), et les infractions ordinaires commises à l'aide d'un réseau électronique (ex. : une escroquerie en ligne, une usurpation d'identité numérique, etc.). Les STAD sont à la base du fonctionnement de tous les acteurs de la société moderne : c'est le système informatique d'une entreprise commerciale, celui de paiement par carte bancaire, celui de réservation des compagnies aériennes, etc.

En parallèle de cette infraction cyber par essence, coexistent les délits ordinaires commis au moyen de réseaux électroniques. Ces derniers sont protéiformes et s'illustrent par les techniques de phishing/hameçonnage, défacement, fraude au président, phreaking, etc. La plus connue de ces attaques est le ransomware ou rançongiciels. Il s'agit d'un programme malveillant qui chiffre les données de la cible afin de bloquer son système, et propose le paiement d'une rançon sous menace de ne jamais communiquer de clef de restauration du service et/ou de rendre publiques les données piratées. L'attaque subie par le centre hospitalier de Corbeil-Essonnes et revendiquée par le groupe russophone Lockbit 3.0 en est une récente illustration. 43 % des notifications reçues par la Commission nationale de l'informatique et des libertés (Cnil) au cours de l'année 2021 concernent des attaques par un rançongiciel.

Quelle que soit la forme de la cyberattaque, les risques qui pèsent sur les entreprises victimes (ou les administrations) sont majeurs. Les données piratées peuvent être utilisées de façon frauduleuse créant une faille dans le système de traitement des données.

Les risques d'une cyberattaque

Quelle que soit la forme de la cyberattaque, les risques qui pèsent sur les entreprises victimes (ou les administrations) sont majeurs. Les données piratées peuvent être utilisées de façon frauduleuse créant une faille dans le système de traitement des données. Par exemple, le hacker peut publier certaines informations sensibles ou favoriser l'exfiltration des documents obtenus, « données qui seront ensuite négociées sur le marché de l'information ou des provinces plus sombres de l'Internet »[1]. Dans cette typologie d'attaques, le chantage et le sabotage sont donc deux risques majeurs à prendre en compte.

Une cyberattaque peut non seulement figer l'activité d'une entreprise, mais elle peut également en empêcher la reprise : perte de données, modification des process post-introduction dans le STAD, blocage des systèmes de paiements, etc. L'ampleur du phénomène et sa durée sont donc susceptibles de provoquer une perte de chiffre d'affaires très importante et à terme de mettre en jeu la survie de l'entreprise. C'est peut-être ce qu'a pu éprouver le groupe Camaïeu victime en juin 2021 d'une cyberattaque majeure ayant perturbé la gestion des stocks des magasins et rendu inaccessible le site de vente en ligne.

Enfin, une telle attaque cyber peut avoir un impact sur l'image et la renommée de l'entreprise, en raison de la vulnérabilité qu'elle semble incarner à l'égard des données de ses clients et partenaires. En effet, en cas de « fuite » de données – intentionnelle de la part

des pirates – ce sont alors des secrets d'affaires ou des informations sensibles qui sont dévoilés au grand public et parfois monnayées à des tiers.

Il faut également toujours s'interroger sur l'origine d'une cyberattaque qui peut avoir pour objectif un but idéologique ou politique[2]. Ainsi, on peut redouter des attaques au moment des votes en assemblée générale qui s'opèrent souvent à distance via un accès sur un site internet ou par boîtier électronique.

Se prémunir contre une cyberattaque

En amont d'une potentielle attaque, toute entreprise devrait effectuer une cartographie des risques cyber auxquels elle est exposée par l'utilisation d'outils électroniques (de la simple tablette au serveur interne). Cela permettra de définir qui a accès à quelle information, comment et qui peut modifier ces données.

Il faudra également recenser toutes les données personnelles (ex. : informations sur un client) et sensibles (ex. : comptabilité), pour assurer leur bon traitement. Les risques d'intrusion, qui sont de nature purement technologique et seront identifiés par les équipes IT de l'entreprise, devront être mis en rapport avec leurs conséquences sur tous les aspects de la vie de la société. Ensuite, il faudra effectuer des sauvegardes et mises à jour régulières des programmes de sécurité (antivirus, filtre spam, etc.).

Des moyens efficaces de se prémunir contre une cyberattaque, et pourtant évidents, sont : le renforcement du mot de passe et la conservation de son caractère secret, l'interdiction d'utilisation des outils ou plateformes professionnelles à des fins personnelles, et la nécessité de vérifier l'expéditeur d'un courriel ou l'initiateur d'une action électronique afin d'éviter, par exemple, l'hameçonnage ou la prise de contrôle par introduction frauduleuse au sein du STAD.

Enfin, il est essentiel de se rapprocher de son assureur pour identifier correctement la nature des risques cyber pris en charge par la police. En effet, l'évolution technologique des attaques étant parfois difficile à prévoir, il est préférable d'être précisément informé sur l'interprétation des clauses d'assurance du risque cyber.

En aval, c'est-à-dire au moment de l'attaque cyber, il est indispensable d'activer le plan de continuité ou de reprise d'activité préalablement défini. Ce plan s'accompagne souvent d'une identification de la brèche dans le système et du déclenchement de l'isolation de la partie attaquée afin d'éviter que le hacker n'ait accès à toutes les données.

L'entreprise devra également notifier l'incident à la Cnil dans les 72 heures si des données personnelles ont ou risquent d'avoir été consultées, modifiées ou détruites. Il en va de même si la sécurité ou le fonctionnement du système de traitement de ces données personnelles est affecté. Il est par ailleurs nécessaire d'alerter sa banque pour mettre fin à toute opération suspecte ou frauduleusement commandée.

Il est essentiel de se rapprocher de son assureur pour identifier correctement la nature des risques cyber pris en charge par la police. En effet, l'évolution technologique des attaques étant parfois difficile à prévoir, il est préférable d'être précisément informé sur l'interprétation des clauses d'assurance du risque cyber.

De plus, une excellente communication en interne au sein de l'entreprise, et en externe auprès des clients, des partenaires commerciaux et du grand public permet d'informer de la bonne gestion de la crise et de la sécurisation des canaux d'utilisation des plateformes de la société. Enfin, il faut déposer une plainte visant l'ouverture d'une enquête et l'identification des auteurs de l'attaque. Ces plaintes permettent également aux services spécialisés de faire progresser leurs enquêtes par le recoupement des modes opératoires constatés.

Pour conclure, il peut être opportun pour une entreprise de recourir à une solution de cyber sécurité certifiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). De tels dispositifs assurent une protection efficace et robuste contre les cyberattaques, ce qui peut être un bon moyen de protection lorsque l'on sait que les intrusions avérées dans les systèmes d'informations ont augmenté de 37 % en un an en 2021. ■

Anae Fouquet-Chevalier, avocate, Chatain & Associés

1. Catherine Chambon, commissaire générale, IGPN, lors de la conférence « Les rencontres de la cybersécurité » du 20 et 23 juin 2022, Librairie Dalloz.

2. Pierre-Yves Caniotti, chef de la division stratégie, prospective et partenariats, commandement de la gendarmerie dans le cyberespace, lors de la conférence « Les rencontres de la cybersécurité » du 20 et 23 juin 2022, Librairie Dalloz.