CYBERCRIMINALITÉ : QUELS SONT LES RISQUES POUR VOTRE ENTREPRISE ?

INTRODUCTION

Les technologies de l'information sont des **techniques informatiques** permettant aux utilisateurs de partager, stocker ou de manipuler des informations par Internet et les réseaux sociaux. Si ces outils offrent un **meilleur accès à l'information**, ils regorgent aussi de **logiciels malveillants** et de **documents contenant un virus**.

Jerome Powell, le président de la Réserve fédérale des États-Unis, a indiqué que la **cybercriminalité** et les **cyberattaques** contre les entreprises représentent le risque actuel le plus important pour l'économie américaine.

Le président de la République français, Emmanuel Macron, a présenté le 12 novembre 2018 un **appel de Paris pour la sécurité du cyberespace**. Cet appel a été signé par 79 États, 35 organismes publics et administrations territoriales, 391 organisations et membres de la société civile, 706 entreprises et entités du secteur privé.

Le 10 juin 2021, le Sénat a publié un rapport d'information intitulé "La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?" Les sénateurs soulignent **4 raisons à la banalisation des cyberattaques et de la cyberdélinquance** : (i) la **numérisation** de l'économie, (ii) la **professionnalisation** de la cybercriminalité avec son **industrialisation** et le développement des cryptomonnaies, (iii) la **difficulté** de la prévention et de la répression et (iv) la place du cyberspace dans la **géopolitique**.

QUELQUES CHIFFRES

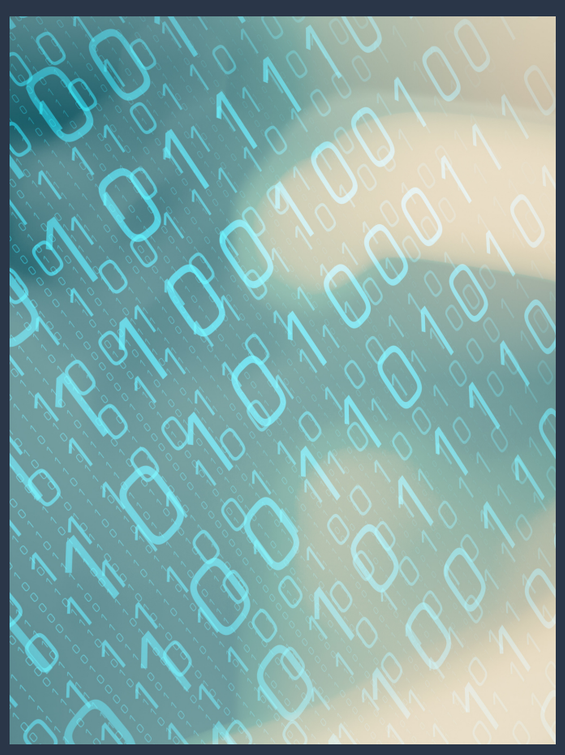
50% des entreprises déclarent avoir connu au moins 1 cyberattaque en 2020

19% des entreprises ont été victimes d'une attaque aux rançonlogiciels

1 entreprise sur 2 est inquiète sur sa capacité à gérer une cyberattaque

57% des entreprises comptent augmenter le budget lié à la cybersécurité

Source : CESIN, février 2021



Selon Kapersky, entreprise multinationale spécialisée dans la sécurité des systèmes d'information, avant 2017, "*Les victimes de rançongiciels étaient principalement des passants occasionnels. Les cybercriminels lançaient des spams partout en espérant trouver au moins un utilisateur qui aurait des fichiers importants dans son ordinateur, et qui ouvrirait la pièce jointe malveillante.*

La situation a changé en 2016. Les listes aléatoires des spammeurs ont été de plus en plus remplacées par les adresses des employés d'une entreprise qui avaient été trouvées en ligne, et spécifiquement collectées. Les coupables avaient clairement compris qu'il était beaucoup plus rentable d'attaquer les entreprises."

I. QU'EST-CE QUE LA CYBERCRIMINALITÉ ?

Depuis le premier confinement décidé en mars 2020, la cybersécurité est devenue **l'affaire de tous**, incluant les TPE, les PME et les acteurs publics.

De manière régulière, les cyberattaques font l'actualité.

A titre d'exemple, au cours de l'été 2021, les hôpitaux publics de Paris ont été victimes d'une cyberattaque de grande envergure. Les données d'environ 1,4 millions de personnes qui ont effectué un test de dépistage du Covid-19 en Ile-de-France mi-2020 ont été dérobées. Les données dérobées incluent de nombreuses données sensibles et confidentielles telles que l'identité ou encore le numéro de sécurité sociale.

Encore plus récemment, le groupe agroalimentaire AVRIL a annoncé le 5 novembre 2021 avoir fait l'objet d'une cyberattaque bloquant l'accès au serveur ainsi qu'aux mails professionnels. Plusieurs sites fonctionnaient en mode dégradé.

La cybercriminalité fait partie des **nouvelles formes de criminalité**. L'utilisation de plus en plus massive des nouvelles technologies par les entreprises engendre donc de nouveaux risques. Chaque entité peut être menacée par un cyber-délinquant, ce dernier pouvant **voler des données, modifier ou détruire** le système informatique de l'entreprise. Le vol de données est particulièrement fréquent.

Les attaques des pirates informatiques peuvent être classées en 4 catégories : **cybercriminalité**, **atteinte à l'image**, **espionnage** et **sabotage**.

Au sein de la cybercriminalité, il existe une multitude de types d'attaques comme les attaques par déni de service (DoS) et par déni de service distribué (DDoS), les malwares ou logiciels malveillants, les attaques Man-in-the-middle attack ou attaque de l'homme du milieu, les attaques par injection SQL ou encore les attaques zero-day.

On dénombre trois formes principales d'intervention des cyber-délinquants :

- les **botnets** qui sont les logiciels d'infiltration fonctionnant en réseau
- Les **rançongiciels** (ransomware) sont des logiciels malveillants qui bloquent l'accès à l'ordinateur et réclamant le paiement d'une rançon, la plupart du temps, en bitcoins
- Le **hameçonnage** (phishing) qui est une technique de fraude dans laquelle les cyberdélinquants se font passer pour un tiers (administration, police, banque…) pour obtenir des données sensibles (mots de passe, identifiants, code de carte bancaire…).

ATTAQUES LES + COURANTES

Phishing : **80%**
Exploitation d'une faille logicielle : **52%**
Arnaque au président : **42%**
Tentative de connexion : **41%**
Acquisition de noms de domaines illégitimes : **35%**
Attaque par déni de service : **33%**
Rançongiciel : **20%**

Source : CESIN, février 2021

II. LA LUTTE CONTRE LA CYBERCRIMINALITÉ EN FRANCE

En France, l'**Agence nationale de la sécurité et de défense des systèmes d'information** (Anssi) est l'autorité nationale en matière de cybersécurité. L'Anssi a pour mission d'**accompagner** les acteurs publics et privés dans le **développement de leur sécurité informatique** afin de **lutter contre la criminalité informatique** et **assurer la sécurité de l'information et des données**. Elle a également pour mission de préserver la souveraineté de l'État français et l'autonomie décisionnelle et stratégique de l'Etat au niveau national et international.

Quant aux services d'enquête, l'**Office central contre la criminalité liée aux technologies de l'information et de la communication** (OCLCTIC), dépendant de la sous-direction de la cybercriminalité, est un service d'enquête spécialisé dans les enquêtes liées à des cyberattaques. Au niveau de la gendarmerie, il s'agit du **centre d'action contre les criminalités numériques** (C3N) **du Service central du renseignement criminel** (SCRC). Le 25 février 2021, il a également été créé le **commandement de la gendarmerie dans le cyberspace** en charge de coordonner et fédérer les actions des services spécialisés.

Face à l'ampleur des attaques informatiques et de la cybercriminalité, l'État a annoncé la mise en place d'un plan d'1 milliard d'euros d'ici 2025 pour renforcer la sécurité des entreprises et des administrations publiques et former des experts en cyberdéfense.

"La tendance à la hausse des attaques par rançongiciels à l'encontre d'organisations publiques et privées identifiées depuis 2018, s'est à nouveau confirmée en 2020, tant à l'échelle internationale que nationale. En 2020, l'Anssi note une augmentation de 255% des siganlements d'attaque par rançongiciels par rapport à 2019".

Rapport de l'Anssi, Etat de la menace rançongiciel à l'encontre des entreprises et des institutions, sept. 2021

III. LES RISQUES GENERES PAR UNE ATTAQUE INFORMATIQUE

La sécurité informatique de l'entreprise est indispensable face aux menaces de cybercriminels, hackers, pirates informatiques qui profitent et exploitent des failles de sécurité des systèmes informatiques et des réseaux informatiques. L'entreprise ne doit pas être vulnérable à des attaques informatiques, qu'elles soient massives ou à des tentatives d'actes de piratages.

Une attaque informatique ou une cyberattaque génère 4 risques :

- Un **risque technique** sur le réseau informatique et la perte et fuite de données personnelles et sensibles.

- Un **risque réputationnel** vis-à-vis des clients qui risquent de perdre confiance en l'entreprise, les fuites de données étant particulièrement sensibles pour les clients.

- Un **risque économique** en ce qu'une cyber-attaque peut engendrer une perte d'exploitation et une perte d'investisseurs et de clients, ayant pour conséquence une perte de chiffres d'affaires. Ces pertes peuvent aboutir à la liquidation judiciaire de l'entreprise.

- Un **risque juridique** pour l'entreprise qui peut voir sa responsabilité engagée en application du règlement européen (UE) 2016/679 du 27 avril 2016 sur la protection des données personnelles (RGPD), notamment en cas de défaut d'information à la suite de la constatation d'une cyberattaque.

"Au-delà des conséquences financières, la réputation des entreprises est évidemment affectée par un sinistre Cyber. Ainsi 50% des français sont prêts à poursuivre en justice les entreprises pour négligence sur leurs données personnelles. Les nouvelles réglementations européennes (RGPD) renforçent, par ailleurs, les responsabilités des entreprises sur ce sujet."

Professeur François CAZALS, Professeur adjoint HEC Paris, Lieutenant-colonel - Revue trimestrielle de la gendarmerie national, avril 2019, n° 264

IV. QUE FAIRE EN URGENCE FACE À UNE ATTAQUE INFORMATIQUE ?

Lors de la découverte d'une cyberattaque, la première étape consiste à **alerter immédiatement** le département informatique et/ou le prestataire informatique de votre société pour obtenir l'assistance requise.

La rapidité de la prise en charge est d'une importance capitale, et pourra permettre d'atténuer les conséquences liées à la cyberattaque.

En cas de cyberattaque, il convient de réunir une **cellule de crise**.

Cette cellule permet de prévenir l'extension de la menace à l'ensemble du système et des sauvegardes de votre entreprise.

La cellule de crise doit notamment :

- **Élaborer** une stratégie de confinement d'un incident de sécurité
- **Préparer** un plan de déconnexion du réseau
- **Vérifier** l'état des données
- **Réparer** ou **reconstituer** les données
- **Annuler** toutes les autorisations d'accès
- **Désigner** un huissier de justice, chargé d'authentifier les faits
- **Émettre** un **rapport d'incident** qui permettra aux équipes d'**actualiser les process interne**, de **mettre en place une communication adéquate** et d'**assurer le suivi** des coûts et pertes générés par cet incident ainsi que de la **procédure pénale**.

.

ChapelleAvocat

GESTION D'UNE CYBERATTAQUE

Les acteurs économiques sont de plus en plus touchés par les cyberattaques. Les cyberdélinquants cherchent à collecter les données afin de solliciter une rançon et/ou de les vendre sur internet. En France, une entreprise sur deux est inquiète sur sa capacité à gérer une cyberattaque. Il est essentiel de connaître les principales étapes de la gestion d'une cyberattaque et de développer des process internes afin d'intervenir rapidement et de limiter les conséquences.

CYBERATTAQUE

RISQUE TECHNIQUE
RISQUE REPUTATIONNEL
RISQUE ECONOMIQUE
RISQUE JURIDIQUE

STEP 1. ISOLER L'INCIDENT

l'incident doit être identifié et catégorisé. Sa gravité doit être appréciée afin de déclencher la cellule de crise si nécessaire

STEP 2. PROTEGER

La cellule de crise doit être alertée. Le ou les postes critiques doivent être isolés des autres postes. Les travailleurs doivent être immédiatement alertés

STEP 3. INVESTIGUER

Le périmètre de l'attaque doit être délimité, les données touchées listées, la source, identifiée et les preuves sauvegardées

STEP 4. RÉPARER ET DECLARER

L'incident doit être réparé, les déclarations d'incident effectuées à l'assurance et à la CNIL, les clients alertés et le dépôt de plainte effectuée

STEP 5. SUIVI

L'incident terminé, il faut actualiser les process interne, communiquer auprès des clients et partenaires économiques et assurer le suivi de la procédure pénale afin d'obtenir réparation des préjudices

NOUS CONTACTER : CABINET@CHAPELLEAVOCAT.COM - 06.99.66.48.50

#LEDROITPENALEN1CLINDOEIL

V. QUELLES SONT LES REPERCUSSIONS JURIDIQUES D'UNE ATTAQUE INFORMATIQUE ?

Si vous êtes dirigeant, l'**assistance d'un avocat** vous est doublement utile : d'une part, pour vous **informer** sur vos **obligations légales** à la suite de cette attaque ; d'autre part, pour **déposer plainte** et **demander l'indemnisation de vos préjudices.**

1-LE RESPECT D'OBLIGATIONS LÉGALES D'INFORMATION POUR LE DIRIGEANT

En matière de cybercriminalité, les attaques impliquent une potentielle **violation des données personnelles** de l'entreprise et de ses clients. Il convient donc de veiller au respect des règles issues du règlement général sur la protection des données (**RGPD**).

L'assistance d'un avocat est alors particulièrement utile pour connaître les obligations qui incombent au dirigeant suite à l'attaque

L'entité victime est soumise à deux obligations :

- La **documentation de l'incident** en vue d'une qualification pénale
- La **notification de l'attaque** auprès de la Commission nationale de l'informatique et des libertés (CNIL) dans un délai de 72 heures après la connaissance de la violation.Cette notification est **obligatoire** lorsque l'incident porte atteinte aux droits et libertés des personnes physiques, clients de la société.

Conseil #1

Lors de votre dépôt de plainte, il vous faut vous munir des renseignements suivants :

- Les documents non confidentiels rassemblés en cellule de crise
- Les références des personnes contactées, et notamment de la cellule de crise intervenue suite à l'attaque
- Les références des transferts d'argent frauduleux effectués
- Le numéro complet de votre carte de crédit ayant servi au paiement contesté
- En cas de débit, le relevé de compte bancaire où apparaît le débit frauduleux.

2- LE DÉPÔT DE PLAINTE ET L'INDEMNISATION DES PRÉJUDICES

La procédure judiciaire est doublement utile en cas d'attaque : elle permettra d'**identifier l'auteur** et le **condamner**, mais aussi d'acter le statut de victime de l'entité commerciale pour obtenir réparation.

Le **dépôt de plainte**, auprès d'un service de police ou du procureur de la République, permet d'ouvrir une **enquête** menée par les services de police nationale ou de la gendarmerie nationale.

Pour construire cette plainte, la **documentation réunie en cellule de crise** sert de base à la qualification juridique des faits constatés.

Le plus souvent, il s'agit d'infractions spécifiques, dites « **atteintes de systèmes de traitement automatisé de données** » (STAD), et prévues par le Code pénal.

Le droit pénal français réprime notamment :

- L'**usurpation d'identité numérique** (article 226-4-1 du code pénal)
- Le **vol d'informations personnelles** (article 311-1 du code pénal)
- L'**escroquerie par fraude à la carte bancaire** (article 313-1 du code pénal)
- L'**accès et/ou le maintien frauduleux dans un STAD** (article 323-1 et suivants du code pénal)
- L'**introduction frauduleuse de données dans un STAD** (article 323-1 et suivants du code pénal)

VI. COMMENT PRÉVENIR UNE ATTAQUE INFORMATIQUE ?

L'anticipation d'une cyber-crise est essentielle pour se protéger efficacement. En la matière, la **proactivité** est la pièce maîtresse d'une **défense efficace**.

Aujourd'hui, il est indispensable pour une entreprise, quelque soit sa taille, et pour les administrations publiques de se doter d'un **plan de prévention et de gestion du risque de cyberattaque**, qui inclut aussi bien le réseau informatique que le site internet de l'entité, pour se protéger des attaques informatiques.

Il convient de noter que les **petites et moyennes entreprises** sont particulièrement visées par les hackers et cyberdélinquants car elles sont connues pour être vulnérables à des attaques informatiques, les cyberdélinquants utilisant les **brèches** et **failles de sécurité** de ces entités.

Différentes actions sont à engager :

- **Connaître** et **se former** aux règles élémentaires de l'hygiène informatique (l'Anssi a publié un guide d'hygiène informatique en 2017 qui rassemble 42 mesures pour protéger les informations des entreprises et entités publiques)
- **Former** et **informer les salariés de l'entreprise** aux risques induit par une cyber-attaque et aux bons gestes à avoir, notamment sur l'ouverture des mails (comment repérer un email malveillant) et l'utilisation d'internet (site internet frauduleux, hameçonnage)
- **Mettre en place** un **plan d'intervention et de sécurisation** du système en cas de cyber-attaque. La mise en place d'un **système de management de la sécurité de l'information** est fourni par la **norme ISO 27001**.
- **Créer une cellule de crise** afin de centraliser les informations et coordonner les actions
- **Prévoir un plan de communication** auprès des autorités et des clients
- **Associer** les responsables des systèmes d'information pour s'assurer de la sécurité des mesures déjà appliquées dans l'entreprise.

Conseil #2

Si votre entreprise a subi une attaque informatique, nous vous conseillons de vérifier votre police d'assurance pour vérifier si le sinistre et ses conséquences sont pris en charge (pertes de données, pertes d'exploitation, prise en charge des dépenses liées au traitement de la cyber-attaque).

Si vous n'avez pas souscrit de cyber-assurance, il est conseillé de le faire en cas de nouvelles cyberattaque.

ChapelleAvocat

Votre **situation est unique**, notre **stratégie aussi**

Cabinet d'avocats pénalistes
Défense pénale et conseil en gestion du risque pénal

2 rue de la Planche - 75007 Paris
T.: 06.99.66.48.50 | F.: 01.84.10.80.95
cabinet@chapelleavocat.com | www.chapelleavocat.com