L'ENTREPRENEUR ET LA CYBERSÉCURITÉ

Quels sont les risques et quelles mesures adopter pour les limiter ?

La digitalisation grandissante de la société, notamment accélérée par la pandémie de Covid19, a entrainé une augmentation de 50% des cyberattaques d'après le Centre belge pour la Cybersécurité (CCB). Contrairement aux idées reçues, ce genre d'intrusion n'est pas réservée qu'aux grandes entreprises, aux états ou organismes politiques.

Selon l'agence européenne pour la cybersécurité (ENISA), 68% des entreprises de taille moyenne ont été victimes d'une cyberattaque en 2020.

Même constat dans le rapport d'activité 2021 de la CNIL, où les PME et les micro-entreprises représentaient 69 % des notifications de violations de données personnelles liées au piratage informatique. 25 % correspondaient aux ETI (Entreprises de Taille Intermédiaire) et 6 % aux grandes entreprises.

D'après le CCB, 60% des attaques ont pour objectif la collecte de données et 50% des entreprises seraient vulnérables en cas d'attaque. Selon une étude française, 70% des PMEs qui subissent une cyberattaque ne s'en relèvent pas.

C'est pourquoi, il est essentiel pour tout entrepreneur de comprendre comment son entreprise pourrait devenir victime de cyberattaque, d'en connaitre les risques notamment juridiques et de savoir comment, tant que possible, s'en protéger.

Sommaire :

LawellMcMiller

I. Quelles sont les attaques les plus fréquentes ?

Les statistiques de l'ENISA démontrent que **80% des attaques se basent sur un facteur humain** (méthodes de phishing par exemple).

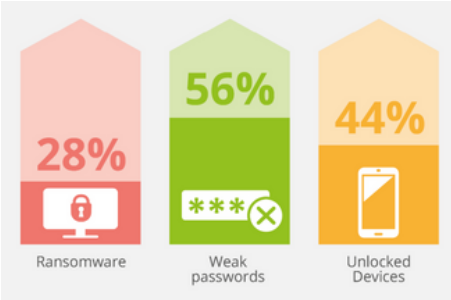
Le CCB classe **la "fraude au président"** au rang de la 3e attaque la plus fréquemment utilisée. Elle consiste en l'usurpation de l'identité d'un donneur d'ordre afin d'exiger d'un collaborateur, en urgence et de manière confidentielle, un important virement.

L'installation d'un logiciel malveillant par l'intermédiaire d'une pièce jointe sur l'appareil d'un utilisateur reste l'attaque la plus fréquente. Ce logiciel peut alors espionner ce qu'il se passe sur votre ordinateur ('spyware') ou le prendre en otage contre rançon ('ransomware', 'rançongiciel').

L'attaque DoS est également très fréquente. Il s'agit d'une attaque réseau par laquelle les hackers inondent le système de requêtes de sorte qu'il soit surchargé et cesse de fonctionner.

Le fait de **ne pas protéger ses appareils par un mot de passe, ainsi que la faiblesse et l'absence de changement régulier des mots de passe utilisés,** constituent souvent une faiblesse supplémentaire de l'entreprise.

S'ajoutent également la **faible protection des sites internet** (dont 4/10 utilisent un FTP non crypté) **et la vulnérabilité d'un nom de domaine** sur six qui rend plus facile la création de fausses adresses email.



ENISA, *Cybersecurity for SMEs,* June 2021

II. Quels sont les secteurs privés les plus à risque ?

Bien qu'aucune entreprise ne soit à l'abri d'une cyberattaque, certains secteurs sont plus à risque que d'autres compte tenu de la masse et du type de données en leur possession. Il s'agit généralement :

- des secteurs de la finance, banque, assurances;
- des secteurs liés à la santé, qui sont deux fois plus susceptibles d'être la cible de cyberattaques;
- des commerces en ligne;
- des établissements d'enseignement et/ou de recherche;
- des entreprises de service en communication.

Ainsi que nous l'avons déjà évoqué, l'objectif principal des cyberattaques est de collecter des données.

Ces données constituent un capital financier important, elles peuvent en effet être vendues au plus offrant sur le ”darkweb”, ou servir à l'usurpation d'identité classique ainsi qu'à des fraudes bancaires.

III. Quels sont les risques encourus en cas de cyberattaque ?

1. Un préjudice à la réputation de l'entreprise

Ce n'est pas un secret, les citoyens sont de plus en plus attentifs à ce qu'il advient de leurs données personnelles.

Une faille de sécurité peut causer un préjudice grave et irréparable à la réputation de l'entreprise ou de sa/ses marque(s). L'entreprise est vue comme moins performante, les clients perdent confiance et se tourneront probablement vers la concurrence.

2. Un préjudice économique important

Cette situation engendre évidemment aussi un coût économique important.

Premièrement, l'atteinte à l'image de l'entreprise impactera la comportement des clients et très probablement une perte du chiffre d'affaire en relation avec la gravité de la cyberattaque.

Une compagnie d'assurance américaine a estimé à 272 jours, la durée moyenne de rétablissement d'une entreprise après une cyberattaque.

-3-

L'entreprise Camaïeu a été victime d'une cyberattaque en 2021 ayant paralysé pendant plus d'une semaine son site en ligne, à quelques semaines des soldes.

Cette attaque a couté à l'entreprise déjà en difficulté pr!s de 40 millions d'euros, ce qui a probablement contribué à sa disparition.

Outre, l'impact sur le chiffre d'affaire, la gestion d'une cyberattaque entraine des coûts importants comprenant potentiellement :

- des frais d'avocat;
- les frais relatifs à la notification de la cyberattaque auprès des clients;
- les frais IT afférents aux mesures correctrices et préventives prises:
- les frais liés aux services de spécialistes en relations publiques,
- les frais liés à la paralysie potentielle des activités de l'entreprise pendant et après la cyberattaque;
- les frais liés aux assurances;
- les dommages liés à de potentielles divulgations de secrets d'affaire,
- etc.

Une étude menée par Deloitte suggère que les répercussions financières d'une cyberattaque, notamment en cas de vol de données personnelles, pouvaient se faire sentir jusqu'à 5 ans après l'attaque.

3. La mise en cause de la responsabilité de l'entreprise sur base du RGPD.

En qualité de responsable de traitement, vous avez l'obligation de prendre les mesures de sécurité techniques et organisationnelles appropriées afin de protéger les données personnelles que vous traitez.

En cas de violation ou de défaillance à cette obligation, **l'entreprise s'expose à une mise en cause de sa responsabilité ainsi qu'à des amendes administratives** pouvant aller jusqu'à 4% du chiffre d'affaire mondial ou 20 millions d'euros.

Vous devez également **vous assurer que vos sous-traitants prennent les mesures de sécurité adéquates**, notamment en signant un contrat de sous-traitance comportant des clauses spécifiques. Le cas échéant, l'entreprise pourrait être tenue pour responsable des actions de ses sous-traitants.

IV. Quelles mesures prendre pour limiter ces risques ?

1) Investissez dans un audit sérieux de votre infrastructure informatique et prenez les mesures de sécurité nécessaires afin de remédier aux failles identifiées.

Plusieurs outils publiés par des agences de cybersécurité nationale et européenne sont disponibles en ligne si vous souhaitez effectuer une partie de l'audit sans faire appel à un service externe (qui reste recommandé).

2) Formez et sensibilisez régulièrement votre personnel aux questions relatives à la cybersécurité et la protection des données à caractère personnel.

3) Développez en interne une stratégie de réponse aux cyberattaques et aux violations de données à caractère personnel.

4) Encadrez contractuellement et de manière adéquate vos relations avec les tiers afin de vous protéger en cas de défaillance de leur part.

5) Vérifiez vos contrats d'assurance et en fonction de la sensibilité des informations traitées par l'entreprise, **assurez-vous contre le cyber-risque.**

Ressources externes:

- ENISA, "Cybersecurity guide for SMEs - 12 steps to securing your business", disponible **ici**.
- ANSSI, "La cybersécurité pour les TPME/PME en 13 questions", disponible **ici**.
- CCB, "Cybersecurity guide for SMEs", disponible **ici**

Julie Lodomez
Avocate - Associée

et Cassandra Bockstael
Avocate

LawellMcMiller
Bruxelles - Paris
28, Avenue Marnix - 1000 Bruxelles
Belgique
+32 2 736 40 90
https://www.lawellmcm.com/

ALTA-JURIS INTERNATIONAL
Membre du réseau Alta Juris International
https://www.altajuris.com/