Un faux sentiment de cybersécurité?

8 décembre 2021

Auteurs

Eric Lavallée

Associé, Agent de marques de commerce Associé, et Avocat

Selena Lu

Associée, Avocate

Les rançongiciels ont fait tellement de ravages dans les dernières années que plusieurs en oublient les autres risques liés à la cybersécurité. Pour certains, le fait de ne pas détenir de renseignements personnels les immunise contre les pirates informatiques et les cyberincidents. Pour d'autres, tant que leurs ordinateurs continuent de fonctionner, c'est qu'il n'y a aucun logiciel malveillant qui y réside. Malheureusement, la réalité est toute autre.

Une nouvelle tendance se dessine à l'horizon, où l'on voit des logiciels malveillants déployés pour détourner de l'information confidentielle, notamment des secrets commerciaux, pour les vendre par la suite à des tiers ou les divulguer au public[1].

Les médias ont abondamment discuté du logiciel *Pegasus* utilisé pour épier des journalistes et des opposants politiques à travers le monde, au point où les autorités des États-Unis ont décidé de l'inclure dans leur liste d'interdictions[2]. Mais l'utilisation de logiciels espions n'est pas limitée à la sphère politique.

Récemment, un tribunal californien a condamné une société américaine, 24[7].ai, à payer 30 millions de dollars à une de ses concurrentes, Liveperson[3]. C'est qu'un logiciel de 24[7].ai était installé côte à côte avec le logiciel de Liveperson sur des systèmes de clients mutuels. Liveperson alléguait dans sa poursuite que 24[7].ai installait des logiciels espions capturant de l'information confidentielle de l'application Liveperson. De plus, les logiciels que 24[7].ai auraient installés faisaient disparaître certaines fonctionnalités de l'application de Liveperson, notamment le bouton activant la fonction de clavardage. Ce faisant, 24[7].ai aurait interféré dans la relation entre Liveperson et ses clients. Cette saga judiciaire se poursuit d'ailleurs, puisqu'un autre procès devra avoir lieu relativement aux secrets commerciaux d'une cliente de Liveperson[4].

Ce litige illustre bien que la cybersécurité concerne non seulement les renseignements personnels, mais aussi les secrets commerciaux et même le bon fonctionnement des logiciels d'entreprise.

Plusieurs précautions peuvent être prises pour diminuer les risques d'incidents de cybersécurité. Des politiques internes robustes à tous les niveaux dans l'entreprise aident à maintenir un cadre sécuritaire pour les opérations des entreprises. Combinées à une sensibilisation des employés aux enjeux juridiques et commerciaux de la cybersécurité, ces politiques peuvent être des ajouts importants aux meilleures pratiques en informatique. Par ailleurs, la sensibilisation des employés facilite l'adoption de meilleures pratiques, notamment des investigations systématiques des anomalies de fonctionnement et l'utilisation de méthodes de programmation protégeant les secrets commerciaux de l'entreprise. Qui plus est, il peut être opportun de s'assurer que les contrats avec des clients accordent aux fournisseurs informatiques des accès permettant les suivis nécessaires pour assurer la sécurité des deux parties.

Finalement, il faut se rappeler que le conseil d'administration doit faire preuve de soin, de diligence et de compétence tout en veillant à l'intérêt supérieur de l'entreprise. Les administrateurs pourraient être tenus personnellement responsables s'ils manquent à leurs obligations de veiller à ce que des mesures adéquates soient mises en place pour prévenir des cyberincidents, ou s'ils font fi des risques et font preuve d'aveuglement volontaire. Ainsi, les membres du conseil d'administration doivent faire preuve de vigilance et être formés et sensibilisés en matière de cybersécurité afin de pouvoir intégrer celle-ci dans leur gestion des risques.

Dans une ère où la propriété intellectuelle est devenue l'actif le plus important d'une société, il va de soi qu'il est primordial de mettre en place les outils technologiques, mais aussi les procédures et les politiques requises pour bien la protéger!

N'hésitez pas à faire appel aux services de Lavery pour vous conseiller sur les aspects juridiques de la cybersécurité.

---

1. voir notamment Carly Page, This new Android spyware mascarades as legitimate apps, *Techcrunch*, 10 novembre 2021, en ligne : https://techcrunch.com/2021/11/10/android-spyware-legitimate-apps; Carly Page, FBI says ransomware groups are using private financial information to further extort victims, *Techcrunch*, 2 novembre 2021, en ligne : https://techcrunch.com/2021/11/02/fbi-ransomware-private-financial-extort.
2. Frank Gardener, NSO Group: Israeli spyware company added to US trade blacklist, *BBC News,* 3 novembre 2021, en ligne: https://www.bbc.com/news/technology-59149651.
3. Thomas Claburn, Spyware, trade-secret theft, and $30m in damages: How two online support partners spectacularly fell out, *The Register,* 18 juin 2021, en ligne: https://www.theregister.com/2021/06/18/liveperson_wins_30m_trade_secret.
4. Blake Brittain, LivePerson wins $30 million from [24]7.ai in trade-secret verdict,*Reuters,* 17 juin 2021, en ligne: https://www.reuters.com/legal/transactional/liveperson-wins-30-million-247ai-trade-secret-verdict-2021-06-17.