Praeventio

Assurance responsabilité professionnelle Barreau

Mars 2025

Judith Guérin
Coordonnatrice aux activités de prévention
judith.guerin@farpbq.ca

Émilie Chevrier
Avocate aux activités de prévention
emilie.chevrier@farpbq.ca

Clé USB et responsabilité professionnelle

Une clé USB trouvée par hasard ou remise lors d'une rencontre professionnelle peut paraître inoffensive. Pourtant, elle peut aussi être la porte d'entrée d'une cyberattaque. Virus, logiciels espions, fichiers truqués : en une seule connexion, ces menaces peuvent se matérialiser et compromettre les données sensibles de votre cabinet ou de votre clientèle.

D'ailleurs, en 2024, le groupe de cyberespionnage Mustang Panda a utilisé cette méthode pour infiltrer des entreprises du secteur maritime en Europe. Les clés USB infectées auraient potentiellement été distribuées lors d'événements et salons professionnels. Cet exemple démontre à quel point ces attaques sont toujours d'actualité.

Pour les avocats, de telles intrusions peuvent être lourdes de conséquences : pertes de données, interruption d'affaires, atteinte à la réputation, violation du secret professionnel ou du privilège relatif au litige.

Or, les dommages liés aux cyberrisques ne sont pas couverts par la police d'assurance émise par le Fonds d'assurance (art. 1.15, 1.16 et 2.04 m) de la police).

Afin de limiter les risques de faire face à une situation similaire, voici quelques suggestions :

- Avant d'accéder au contenu d'une clé USB, utilisez un ordinateur dédié à l'analyse des fichiers et isolé du reste de votre réseau (communément appelé station blanche). Ainsi, vous évitez tout risque d'infection et préservez la confidentialité de vos données;

- Vérifiez que l'antivirus de votre ordinateur est à jour. Ce dernier devrait également être configuré pour analyser les périphériques USB connectés avant d'accéder à leur contenu;

- Désactivez la fonction « lecture automatique » sur votre ordinateur puisque cette dernière peut permettre l'exécution systématique de fichiers malveillants présents sur une clé USB non sécurisée;

- Faites quotidiennement des sauvegardes de votre système informatique au complet (ordinateurs, disques durs externes, serveurs, etc.);

- La formation demeure l'une des manières les plus efficaces de combattre la cybercriminalité. Pour cette raison, sensibilisez l'ensemble du personnel sur les risques liés à l'utilisation de clés USB;

- Élaborez une politique claire quant à l'utilisation de matériel informatique, incluant les clés USB ou autres périphériques externes;

- En cas de doute sur la fiabilité d'une clé USB, contactez votre équipe informatique. Elle pourra vous aider à confirmer le caractère sécuritaire de cette dernière.

En suivant ces recommandations simples, vous réduirez les risques d'infection de vos ordinateurs par des clés USB potentiellement dangereuses, protégeant ainsi les données sensibles de votre cabinet et de votre clientèle.

Dans tous les cas, il est approprié que les avocats souscrivent à une assurance cyberrisques. À cet égard, la Corporation de services du Barreau du Québec a conclu une entente avec un assureur pour offrir aux membres en règle du Barreau du Québec la possibilité de souscrire à une telle assurance.

Références :

Alexandre Boero, « Des clés USB infectées déguisées en goodies? L'improbable infiltration de hackers dans le fret maritime, Clubic, Cybercriminalité, 12 octobre 2024, en ligne : https://www.clubic.com/actualite-540278-des-cles-usb-infectees-deguisees-en-goodies-l-improbable-infiltration-de-hackers-dans-le-fret-maritime.html (Page consultée le 28 février 2025).

Centre canadien pour la Cybersécurité, « Conseils de sécurité pour les dispositifs périphériques – ITSAP.70.015 », Mai 2024, en ligne : https://www.cyber.gc.ca/sites/default/files/itsap.70.015-f.pdf (Page consultée le 6 février 2025).

Orange Cyberdefense, « Infection par clé USB : comment s'en protéger? », Insight Blog, 31 août 2023, en ligne : https://www.orangecyberdefense.com/fr/insights/blog/infection-par-cle-usb-comment-sen-proteger#:~:text=l'%C3%A9quipement%20incrimin%C3%A9.-,Limiter%20les%20risques%20d'infection%20par%20cl%C3%A9%20USB%20avec%20Malware,Malware%20Cleaner%20d'Orange%20Cyberdefense. (Page consultée le 6 février 2025).

Commissariat à la protection de la vie privée du Canada, « Conseils à l'intention des institutions fédérales sur l'utilisation des dispositifs de stockage portatifs », 25 mars 2014, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels/aide-pour-l-application-de-la-loi-sur-la-protection-des-renseignem (Page consultée le 6 février 2025).

Yvette Bonnet, « Alerte attaque USB : Des moyens simples pour protéger les USB contre les attaques », Wondershare, Recoverit, en ligne : https://recoverit.wondershare.fr/usb-recovery/prevent-usb-attack.html (Page consultée le 6 février 2025).