i-SIGMA™

Home of NAID & PRISM International

L'honorable sénateur Tony Dean
Président, Comité sénatorial permanent de la sécurité
nationale, de la défense et des anciens combattants
Sénat du Canada
Ottawa (Ontario)
K1A 0A4

Le 30 octobre 2024

Monsieur le Sénateur,

Tandis que votre comité examine le projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois, i-SIGMA souhaite attirer votre attention sur un aspect souvent négligé de la cybersécurité : s'assurer que tous les renseignements personnels et autres données de nature délicate sont effacés des appareils électroniques mis au rebut.

Pour vous remettre en contexte, l'entité i-SIGMA a été créée en mai 2018 à la suite de la fusion de la National Association for Information Destruction (NAID) et de PRISM International (Professional Records and Information Services Management). La NAID a toujours été l'association internationale de surveillance des opérateurs de déchiquetage sécurisé et, grâce à notre association avec PRISM International, nous représentons désormais les quatre piliers de la gestion des documents et de l'information, à savoir le stockage des documents et des renseignements physiques, la protection des données et l'entreposage des supports médias, la numérisation et le balayage ainsi que les services de destruction des documents et des renseignements confidentiels. À ce titre, i-SIGMA est l'association-cadre qui chapeaute ces pratiques professionnelles en matière de protection de la vie privée et qui promeut la gestion appropriée du cycle de vie de l'information, une activité essentielle dans l'environnement réglementaire d'aujourd'hui.

Dans le cadre de nos efforts constants pour tenir les gouvernements informés des questions émergentes concernant la protection de la vie privée et la sécurité publique, i-SIGMA et ses associations homologues du monde entier mènent régulièrement des recherches sur les facteurs de risque en matière de protection de la vie privée et de sécurité.

À titre d'exemple, vous trouverez ci-joint un communiqué de presse de l'une de nos associations fondatrices détaillant les résultats de la plus grande étude réalisée à ce jour sur la présence de renseignements personnels identifiables sur les appareils électroniques vendus sur le marché des biens d'occasion. L'étude a révélé que 40 % des appareils revendus par l'intermédiaire de marchés accessibles au public contenaient des renseignements personnels.

…/2

Pour garantir la crédibilité du processus, l'étude a été réalisée par un laboratoire judiciaire indépendant. Il est toutefois alarmant de constater que l'étude a été menée en faisant uniquement appel à des méthodes de récupération de base, et non à des méthodes de criminalistique perfectionnées; autrement dit, n'importe qui serait capable d'accéder à ces renseignements. Parmi les données récupérées, on retrouvait des renseignements sur la carte de crédit, des coordonnées, des noms d'utilisateur et des mots de passe, des données personnelles et d'entreprises ainsi que des renseignements fiscaux. Les appareils examinés étaient des téléphones portables, des tablettes et des disques durs.

i-SIGMA estime que cette étude montre à quel point il importe a) de veiller à ce que les particuliers et les organisations prennent des mesures pour s'assurer que tous les renseignements personnels sont effacés de leurs appareils avant de s'en départir sur le marché de la revente ou du recyclage; et b) que les entreprises du domaine du recyclage ou de la revente d'appareils électroniques respectent les normes de l'industrie relatives à la suppression adéquate des données.

Nous pensons que les résultats de l'étude ont également permis de cibler des moyens inhabituels de commettre des cybercrimes et, éventuellement, de lancer des cyberattaques. Ce risque ne peut qu'augmenter avec la multiplication des appareils électroniques en circulation, ce qui signifie également que davantage d'appareils finissent par être envoyés au recyclage ou au rebut. À vrai dire, une personne n'a pas besoin d'être un pirate informatique accompli pour faire tomber un système lorsqu'elle peut simplement obtenir tous les renseignements dont elle a besoin à même de vieux ordinateurs et téléphones, ainsi que de vieilles tablettes, etc.

Ni les particuliers ni les entreprises ne sont à l'abri de ce type de menace. Si les grandes entreprises ont probablement mis en place des systèmes rigoureux pour s'assurer que les appareils électroniques mis au rebut ne contiennent plus de données, ce n'est pas forcément le cas des petites entreprises. Les cybercriminels ciblent souvent le maillon le plus faible du système, et ce maillon pourrait bien être les appareils mis au rebut par les petites entreprises, que l'on retrouve sur le marché des biens d'occasion (et qui sont parfois même simplement laissés sur le trottoir).

En ce qui concerne le projet de loi C-26, selon les conclusions les plus pertinentes que nous pouvons tirer de notre travail, il faudrait s'assurer que les programmes de cybersécurité qui seront exigés en vertu de la loi comprennent des dispositions relatives au retrait de tout renseignement personnel des vieux appareils électroniques ou de tout autre renseignement susceptible de présenter un cyberrisque. De façon générale, il s'agit d'un domaine de la cybersécurité que l'ensemble des particuliers, des entreprises et des autres organisations devront garder à l'esprit à mesure que de plus en plus d'appareils électroniques entreront sur le marché, et qu'ils en sortiront à la fin de leur cycle de vie. Par ailleurs, comme notre organisation le répète depuis des décennies : la sécurité des renseignements dépend du maillon le plus faible de ce cycle de vie, et, trop souvent, nous accordons peu d'attention à la fin de ce cycle de vie.

Pour renchérir sur ce point, prenons le cycle de vie d'un document papier contenant des renseignements financiers, des données de sécurité ou des renseignements personnels de nature délicate. Une organisation se doit de mettre en place des mesures de protection tout au long du cycle de vie d'un tel document, notamment des systèmes de stockage sûrs, des

…/3

politiques claires sur les exigences de conservation et, enfin, des protocoles de destruction et d'élimination sûrs lorsqu'il n'est plus nécessaire de conserver ces renseignements. À cette dernière étape, vous ne vous permettriez pas de jeter le document à la poubelle ni de l'envoyer au recyclage, car il contient des renseignements qui pourraient s'avérer précieux pour quiconque les volerait. Si une personne s'en débarrassait négligemment de cette façon, tous les efforts réalisés pour protéger ces renseignements pendant la phase utile de leur cycle de vie seraient réduits à néant. Voilà pourquoi il faut prêter attention à la fin du cycle de vie; cette phase est tout aussi importante que les autres.

Prenons maintenant ce même document et supposons qu'il n'a toujours existé qu'en format électronique. Les gens ont l'habitude de protéger leurs mots de passe et de verrouiller leurs appareils, mais les petites entreprises savent-elles ce qu'il faut faire des vieux appareils électroniques? Il s'agit d'un volet complexe du processus de destruction de l'information; les initiatives maison visant à nettoyer des appareils s'avèrent souvent insuffisantes, car il est encore possible de récupérer l'information. Ainsi, lorsque des particuliers et des organisations se débarrassent de leurs appareils électroniques, c'est un peu comme s'ils mettaient une boîte contenant des données financières ou de sécurité de nature délicate directement sur le trottoir.

Ce genre de situation ne relève pas du tout de la fiction. En 2010, un audit mené par le commissaire à la protection de la vie privée du Canada a permis de constater que les ordinateurs du gouvernement fédéral donnés au « Programme des ordinateurs pour les écoles » contenaient une quantité alarmante de renseignements personnels de nature délicate[1].

Nous espérons que ces renseignements vous seront utiles, et nous attendons avec impatience les délibérations sur le projet de loi C-26. Merci de nous avoir accordé de votre temps.

Cordialement,

Tony Perrotta
Directeur, Canada, i-SIGMA
www.isigmaonline.org

CC : Membres, Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants
Madame Ericka Paajanen, greffière du Comité

[1] https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/verifications/ar-vr_pidp_2010/

POUR DIFFUSION IMMÉDIATE :

Communiqué de presse : La plus grande étude réalisée à ce jour a révélé que des renseignements personnels identifiables ont été trouvés sur 40 % des appareils usagés

Phœnix, Arizona, 24 mars 2017 – La National Association for Information Destruction® (NAID®) a annoncé aujourd'hui les résultats de la plus grande étude réalisée à ce jour sur la présence de renseignements personnels identifiables (RPI) sur des appareils électroniques vendus sur le marché de l'occasion. L'étude a révélé que 40 % des appareils revendus dans les canaux de revente accessibles au public contenaient des RPI. La NAID a mandaté CPR Tools, Inc. pour analyser les appareils usagés, qui comprenaient des disques durs, des téléphones portables et des tablettes usagés.

L'état actuel du stockage électronique a permis à presque chaque adulte de posséder un dispositif de stockage de données. « Le stockage de données étant intégré à presque tous les aspects de la technologie actuelle, il en va de même pour la probabilité d'un accès non autorisé ou involontaire à ces données » [TRADUCTION], déclare John Benkert, PDG de CPR Tools. Il ajoute : « Les sites de vente aux enchères, de revente et de recyclage ont créé une source de revenus pratique grâce aux appareils d'occasion. Cependant, la véritable valeur réside dans les données que le public laisse involontairement sur les appareils. » [TRADUCTION]

Bien que des études similaires aient été menées au cours de la dernière décennie, l'étude de la NAID est unique dans la mesure où le processus de récupération utilisé pour localiser les données sur plus de 250 appareils n'était, par sa nature, ni complexe ni exigeant une formation avancée en criminalistique. Toutes les méthodes ont fait appel à des logiciels contributifs téléchargeables.

Robert Johnson, PDG de la NAID, souligne que, même si les résultats de cette étude montrent une diminution des données trouvées par rapport aux études précédentes, la « NAID n'a utilisé que des mesures de base pour extraire les données; imaginez si nous avions demandé à notre agence de criminalistique d'explorer réellement en profondeur! » Il poursuit en laissant entendre que « la proportion équivalant à 40 % est horrible quand on pense aux millions d'appareils qui sont recyclés chaque année » [TRADUCTION].

Les RPI récupérés comprenaient des renseignements sur la carte de crédit, des coordonnées, des noms d'utilisateur et des mots de passe, des données personnelles et d'entreprises, des renseignements fiscaux, etc. Alors que les téléphones portables contenaient le moins de RPI récupérables (avec 13 %), les tablettes ont révélé des résultats particulièrement inquiétants, avec un taux de 50 %. Des RPI ont également été retrouvés sur 44 % des disques durs. Au total, 40 % des appareils contenaient des RPI. L'étude a inclus des appareils ayant été utilisés à la fois dans des environnements commerciaux et personnels.

M. Johnson souligne que les résultats ne constituent en aucun cas une forme d'accusation à l'encontre des services commerciaux dignes de confiance qui proposent des services sécurisés d'effacement des données. « Nous savons, grâce aux audits que nous effectuons régulièrement auprès des fournisseurs de services certifiés de la NAID, que, lorsque l'effacement est effectué correctement, ce processus est fiable et efficace. Le problème réside dans les fournisseurs de services qui ne sont pas qualifiés et, trop souvent, dans les entreprises et les particuliers qui pensent pouvoir accomplir cette tâche par eux-mêmes. » [TRADUCTION]

À PROPOS DE LA NAID

La National Association for Information Destruction (NAID) est l'organisme de surveillance international et l'association professionnelle à but non lucratif du secteur de la destruction sécurisée, qui représente actuellement plus de 1 900 sites membres dans le monde. La NAID plaide en faveur de l'établissement d'une norme de bonnes pratiques appliquée par l'ensemble des gouvernements, par les prestataires de services ainsi que par les fournisseurs de produits, d'équipements et de services destinés aux entreprises spécialisées dans la destruction. La mission de la NAID consiste à promouvoir la destruction appropriée des renseignements supprimés au moyen d'activités éducatives et à encourager l'externalisation des besoins en matière de destruction à des sous-traitants qualifiés. Pour en savoir plus, prière de visiter le site http://www.naidonline.org/ ou de nous suivre sur Twitter et Facebook à @NAIDonline.