JANVIER 2022

Résumé de règlement – MR21-00033 – municipalité régionale de Durham

La municipalité régionale de Durham (la « région ») a signalé que le ou vers le 20 janvier 2021, une personne non autorisée avait obtenu accès à ses données au moyen de l'application de partage de fichiers Accellion FTA qu'elle utilisait.

Ayant établi que des renseignements personnels et des renseignements personnels sur la santé avaient été divulgués en l'occurrence, la région a signalé cette atteinte à la vie privée au Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (« CIPVP » ou « notre bureau »).

RÔLE DU CIPVP

Le CIPVP est l'organisme chargé de surveiller l'application des **lois ontariennes sur la protection de la vie privée**, lesquelles établissent des règles sur la collecte, l'utilisation, la divulgation, la protection et l'élimination de renseignements personnels et de renseignements personnels sur la santé par les institutions publiques et les fournisseurs de soins de santé de l'Ontario.

Lorsqu'une atteinte à la vie privée est signalée au CIPVP, notre bureau l'évalue pour s'assurer que l'organisation en question a pris des mesures raisonnables pour maîtriser l'incident, éviter qu'il ne se reproduise et aviser les personnes concernées. Nous déterminons également si, au moment de l'atteinte à la vie privée, l'organisation disposait de mesures de précaution raisonnables d'ordre administratif, technique et matériel

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

pour assurer la sécurité et la confidentialité des renseignements personnels et des renseignements personnels sur la santé dont elle avait le contrôle.

PORTÉE ET CONTEXTE DE L'ATTEINTE À LA VIE PRIVÉE

La cyberattaque signalée contre la région faisait partie de la vaste campagne menée par des cyberacteurs pour exploiter les vulnérabilités d'Accellion FTA à la fin de 2020 et au début de 2021[1], dans le but d'attaquer des organismes gouvernementaux et des entreprises privées du monde entier. Ces agissements se sont répercutés sur nombre d'organisations et de particuliers à travers le monde.

La région a fait savoir que le ou vers le 20 janvier 2021, d'après son enquête, une personne non autorisée avait obtenu accès à ses données en exploitant une vulnérabilité auparavant inconnue d'Accellion FTA. Cette personne a ensuite exfiltré des renseignements personnels et des renseignements personnels sur la santé contenus dans des documents qui avaient été acheminés à la région ou par celle-ci au moyen d'Accellion FTA.

La région a affirmé avoir pris connaissance de la cyberattaque le 25 mars 2021, lorsqu'elle a reçu une note de rançon sur cette affaire. Elle a confirmé avoir pris des mesures immédiates pour sécuriser ses systèmes et mener une enquête.

La région a signalé que les renseignements personnels ou renseignements personnels sur la santé d'environ 105 945 avaient été ou auraient pu avoir été touchés par l'atteinte à la vie privée. Selon la région, ces renseignements étaient variés et comprenaient : noms, dates de naissance, coordonnées, sexe, identité des parents ou tuteurs, lieux de travail, antécédents professionnels, renvois à des programmes d'aide aux employés, numéros d'immatriculation scolaire de l'Ontario, écoles, années d'études, renseignements sur les cours, systèmes scolaires, citoyenneté, religions, renseignements financiers, numéros de rôle d'impôt foncier, occupation/statut de locataire, renseignements sur le véhicule, pièces d'identité délivrées par le gouvernement, participation à un programme d'intervention auprès des partenaires violents, ordonnances judiciaires, noms d'agents de probation, numéros d'identité de membres et/ou prestations du programme Ontario au travail/POSPH, renvois, dossiers d'immunisation, numéros de carte Santé, admissibilité aux vaccins, résultats d'analyses en laboratoire, soins de santé reçus et renseignements sur les demandes d'ambulance.

1 Voir l'avis conjoint de cybersécurité **Exploitation of Accellion File Transfer Appliance - AA21-055A** du 24 février 2021. Cet avis était le fruit des efforts conjugués des responsables de la cybersécurité d'Australie, de Nouvelle-Zélande, de Singapour, du Royaume-Uni et des États-Unis.

Après cette attaque, la région a fait savoir qu'une partie des données touchées par l'atteinte à la vie privée avait été publiée sur le Web caché, y compris des renseignements personnels et des renseignements personnels sur la santé.

MAÎTRISE

La région a précisé qu'après qu'elle eut découvert l'atteinte à la vie privée, ses équipes de TI, en collaboration avec le fournisseur de l'application Accellion FTA, Accellion (maintenant appelé Kiteworks), ont pris des mesures immédiates pour sécuriser ses systèmes. La région a également confirmé avoir signalé la cyberattaque à la police.

NOTIFICATION

La région a confirmé avoir publié des renseignements sur l'atteinte à la vie privée sur son site Web et envoyé des avis écrits à presque toutes les personnes dont des renseignements personnels ou des renseignements personnels sur la santé auraient pu avoir été touchés par l'incident de cybersécurité[2]. Elle a également mis sur pied un centre d'appels pour répondre aux questions sur cette affaire, et offert des services gratuits de surveillance du crédit aux personnes dont des renseignements financiers avaient été touchés par l'atteinte à la vie privée.

MESURES DE PRÉCAUTION ET MESURES CORRECTIVES

La région a confirmé qu'elle était responsable de la gestion des utilisateurs et des correctifs pour l'application Accellion FTA. Elle a également fait savoir que sauf dans des circonstances limitées lorsqu'elle avait besoin de soutien technique, Accellion n'avait pas accès à ses données.

Au moment de l'atteinte à la vie privée, la région semblait avoir mis en place des mesures raisonnables pour se protéger contre une cyberattaque de ce genre, c'est-à-dire une attaque contre ses dossiers de renseignements personnels et de renseignements personnels sur la santé au moyen d'une application de transfert de fichiers.

Par exemple, afin de protéger l'organisation contre une cyberattaque et d'assurer la sécurité de ses données, la région a confirmé qu'au moment de l'atteinte à la vie privée, elle avait mis en place un mécanisme lui permettant de rester informée des mises à jour d'Accellion FTA. De plus, la région a confirmé qu'elle avait adopté une procédure de gestion des correctifs pour s'assurer que les produits (y compris Accellion FTA) étaient corrigés régulièrement et dès que des correctifs ou des mises à

2 Cinq personnes ayant pu avoir été touchées par l'atteinte à la vie privée étaient décédées, et la région ne disposait d'aucun renseignement sur leurs représentants successoraux. La région a ajouté à ses dossiers des directives écrites afin d'aviser ces représentants advenant que ceux-ci communiquent avec elle au sujet de ces personnes décédées. La région a également ajouté une note semblable concernant trois personnes ayant pu avoir été touchées dont elle n'avait pas les coordonnées.

niveau de sécurité étaient disponibles. Au moment de l'atteinte à la vie privée, la région a confirmé avoir établi une procédure précise pour corriger rapidement, au besoin, les vulnérabilités critiques. En effet, la région a indiqué qu'elle s'était appuyée sur cette procédure relative aux vulnérabilités critiques pour mettre à niveau Accellion FTA à plusieurs reprises au début de 2021. La région a également confirmé avoir mis en place une politique de conservation des informations téléchargées dans l'application afin de minimiser les répercussions possibles d'une attaque impliquant Accellion FTA.

En outre, la région a indiqué qu'elle avait pris les mesures proactives suivantes pour se protéger des cyberattaques :

- les employés reçoivent une formation sur les rançongiciels et la cybersécurité (avec notamment des simulations d'attaques par hameçonnage);
- un logiciel antivirus effectue des analyses en temps réel des appareils des utilisateurs finaux et des serveurs;
- les comptes utilisateurs sont assortis de privilèges et de droits d'accès, de sorte que les titulaires peuvent accéder uniquement aux renseignements nécessaires à leurs fonctions;
- une copie de sauvegarde des fichiers électroniques est effectuée régulièrement et vérifiée pour confirmer que les fichiers peuvent être récupérés.

Comme cette attaque a fait intervenir l'exploitation d'une vulnérabilité jusque-là inconnue (une exploitation du jour zéro), les mesures prises par la région pour se protéger d'une cyberattaque auraient été insuffisantes pour empêcher l'atteinte à la vie privée dont il est question dans cette affaire. La région a expliqué qu'Accellion l'avait informée de cette vulnérabilité d'Accellion FTA le 22 janvier 2021, deux jours après la cyberattaque. La région a indiqué qu'après avoir pris connaissance de cette vulnérabilité, elle a désactivé Accellion FTA le jour même jusqu'au 25 janvier 2021, date à laquelle un correctif était disponible et a été appliqué avec succès. Cependant, le mécanisme permettant à la région de recevoir des mises à niveau pour Accellion FTA et sa procédure de gestion des correctifs ne lui ont pas permis de se protéger de la cyberattaque qui avait déjà eu lieu à son insu.

En réaction à cette atteinte à la vie privée, la région a convenu d'instaurer des exigences de journalisation pour surveiller ou déceler les événements de sécurité (comme l'exfiltration de données) liés à toutes les applications de partage de fichiers qu'elle utilise. Cette mesure aidera la région à déceler et à comprendre mieux et plus rapidement les incidents de cybersécurité et à s'en rétablir. La région a également précisé qu'elle avait cessé d'utiliser Accellion FTA.

CONCLUSION

Les renseignements personnels et les renseignements personnels sur la santé touchés par cette atteinte à la vie privée étaient très délicats.

Dans l'ensemble, au moment de cette atteinte à la vie privée, la région semblait avoir mis en place un certain nombre de mesures de précaution raisonnables pour se protéger d'une cyberattaque de ce genre. En réponse à l'atteinte à la vie privée, la région a accepté de prendre d'autres mesures raisonnables pour mieux déceler et gérer les incidents de cybersécurité à l'avenir.

Après avoir examiné les circonstances de cette atteinte à la vie privée et les mesures prises par la région, l'analyste a estimé qu'aucun autre examen n'était nécessaire.

POST-SCRIPTUM

Le CIPVP travaille sans relâche pour résoudre les atteintes à la vie privée qui sont signalées à notre bureau et affiche un taux de réussite très élevé. Cette réussite est attribuable aux organisations qui se prêtent à notre processus et à leur volonté de prendre en considération les recommandations de notre bureau.

À notre époque, les cyberattaques sont de plus en plus fréquentes. Bien que toutes ne puissent être évitées, cette affaire devrait rappeler clairement l'importance non seulement de bien réagir aux cyberattaques, mais aussi de s'assurer que des défenses solides et à jour sont en place pour identifier et atténuer le risque d'attaque. Il faut notamment être vigilant lors de la sélection des logiciels et des autres technologies.

Au moment de cette atteinte à la vie privée, Accellion FTA, un logiciel patrimonial, était toujours pris en charge par le fournisseur. Après cet incident, la région a indiqué avoir transféré les utilisateurs vers d'autres applications de partage de fichiers. Si la migration des systèmes patrimoniaux vers de nouveaux systèmes constitue un défi pour toutes les organisations, il est important de suivre les progrès technologiques afin de tirer profit des mesures de sécurité les plus récentes.

Pour obtenir de plus amples renseignements, consultez les documents suivants du CIPVP :

- **Votre vie privée et le Bureau du commissaire à l'information et à la protection de la vie privée**
- **Les renseignements sur votre santé et votre vie privée**
- **Le vol d'identité : un crime de situation**
- **Déposer une plainte concernant la protection de la vie privée**
- **Déposer une plainte concernant la protection de la vie privée en matière de santé**
- **Se protéger contre les rançongiciels** (en anglais)

- **Se protéger contre l'hameçonnage**
- **Le télétravail pendant la pandémie de COVID-19**
- **Planning For Success: Privacy Impact Assessment Guide** (en anglais)
- **La communication de renseignements personnels sur la santé par courriel**
- **Considérations relatives à la protection de la vie privée et à la sécurité dans le contexte des visites de soins de santé virtuelles**
- **Feuille-info : Le transfert sécuritaire de renseignements personnels sur la santé**

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario