Guide sur la protection de la vie privée

Sollio Agriculture LP (« Sollio AG ») et Agronomy Compagny of Canada (« Agromart ») sont heureux de vous aviser qu'un règlement a été conclu dans le cadre d'un recours collectif se rapportant à une atteinte à la sécurité survenue en 2020 à la suite d'une cyberattaque.

Vous trouverez plus de renseignements sur le règlement en consultant les pages suivantes (en anglais seulement) :

https://www.foremancompany.com/agromart-sollio-privacy-breach ou

https://waddellphillips.ca/class-actions/sollio-ag-and-agromart-class-action/

Sollio AG et Agromart profitent de cette occasion pour vous rappeler l'importance de la sécurité des données dans le secteur agricole au Canada et vous faire part des enseignements qui en ont été tirés et des améliorations qui ont récemment été implantées afin de rendre nos systèmes plus sécuritaires.

Sécurité électronique et protection de la vie privée dans le secteur agricole au Canada

La protection de la vie privée et la sécurité des données sont des priorités grandissantes pour tous les secteurs. Toutes les organisations, quelle que soit leur taille, ont un rôle à jouer pour s'assurer que les appareils et les données qu'elles emploient pour effectuer leur travail sont sécurisés. Plus important encore, des pratiques robustes en matière de sécurité des données et de protection de la vie privée favorisent un sentiment de confiance entre les organisations et les particuliers qui leur communiquent leurs renseignements.

La protection de la vie privée et la sécurité des données sont particulièrement importantes pour le secteur agricole, un milieu dans lequel l'adoption de technologies connectées a fortement crû au cours des dernières années. Que l'on pense aux téléphones intelligents, aux logiciels de gestion agricole ou encore, aux équipements agricoles connectés et à guidage GPS, la totalité du secteur agricole repose sur différentes formes de systèmes compatibles avec Internet ou connectés. Il est essentiel que chaque acteur du secteur agricole utilise de manière sécuritaire des appareils et des systèmes, et qu'il s'assure que les appareils et les systèmes sont dotés de mesures de protection appropriées afin de préserver autant que possible la sécurité des utilisateurs. De plus, à l'instar de tout autre équipement, les appareils et les systèmes connectés doivent être entretenus de façon appropriée, et leurs systèmes et mesures de sécurité doivent être vérifiés régulièrement et tenus à jour.

Si les appareils et les systèmes deviennent désuets ou ne sont pas adéquatement entretenus ou sécurisés, ceux-ci deviennent des cibles de choix pour les criminels cherchant à commettre des cyberattaques. Les cyberattaques peuvent prendre différentes formes. Au cours des dernières années, elles sont devenues plus destructives; dans plusieurs cas, des criminels ont rendu des ordinateurs et des appareils inutilisables, parfois au point d'empêcher complètement des entreprises de fonctionner. Dans le pire scénario, les criminels volent les données, verrouillent l'accès aux systèmes informatiques et aux appareils des organisations, puis exigent une rançon en échange de la suppression des données et du déverrouillage des ordinateurs et des appareils. Ces rançons sont parfois élevées : entre 2021 et 2022, la rançon moyenne a doublé, s'élevant à plus de 1,5 million de dollars. Cette menace pèse sur les organisations de grande taille, mais également sur les petites entreprises.

Dans tous les cas, les incidents de cybersécurité visant des entreprises sont coûteux et chronophages à régler, et il peut être très dispendieux de restaurer les systèmes et les données. Dans le secteur agricole, cela peut également mener à des préoccupations plus générales en matière de sécurité alimentaire. Des rapports font état d'incidents de cybersécurité qui semblent mettre en cause des formes d'espionnage du marché agricole canadien. Le Canada fait partie des principaux producteurs et exportateurs agricoles mondiaux. Notre marché a une grande valeur et nous avons tous un rôle à jouer afin de protéger les données et les renseignements du secteur agricole canadien.

Comment les criminels attaquent-ils les organisations?

Les criminels peuvent attaquer les organisations de différentes façons :

Compromission de l'adresse courriel professionnelle : Une compromission de l'adresse courriel professionnelle survient lorsqu'un criminel obtient l'accès au compte de courriel d'une victime, souvent pour voler des renseignements sensibles entreposés dans le compte ou comme ruse pour faire en sorte que l'utilisateur redirige des fonds vers le compte bancaire du criminel (généralement en se faisant passer pour un vendeur ou un autre bénéficiaire). Les criminels compromettent parfois des comptes de courriel en envoyant à l'utilisateur un courriel d'hameçonnage. Un courriel d'hameçonnage est un courriel qui peut sembler légitime, mais qui contient un hyperlien ou un code QR qui dirige l'utilisateur vers une page Web sur laquelle il lui est demandé d'entrer ses justificatifs d'identité. Un criminel peut également utiliser son accès au compte de courriel de l'utilisateur pour envoyer d'autres courriels d'hameçonnage à partir de celui-ci, dans le but que d'autres personnes divulguent leurs justificatifs d'identité (cette méthode étant appelée « hameçonnage latéral »).

Soyez vigilants lorsque vous ouvrez des courriels provenant d'expéditeurs inconnus ou lorsqu'il vous est demandé dans un courriel d'ouvrir des liens ou de cliquer sur un document. Bien qu'un courriel puisse sembler provenir d'une source légitime, vous devriez vérifier l'adresse courriel, ce que vous pouvez faire en survolant l'adresse avec votre curseur. Méfiez-vous si vous ne connaissez pas l'adresse courriel de l'expéditeur. Les erreurs typographiques ou les structures de phrases inhabituelles sont également des signaux d'alarme d'hameçonnage potentiel.

Exploitation des vulnérabilités d'un système ou d'un appareil : Les criminels peuvent également avoir accès aux systèmes informatiques et aux appareils connectés en exploitant les vulnérabilités du système ou de l'appareil. Même si les fabricants et les développeurs de logiciels veillent à ce que leurs systèmes respectent certaines exigences minimales en matière de sécurité, ils découvrent souvent des vulnérabilités après la commercialisation de leurs produits. Pour corriger ces vulnérabilités, ils publient des « correctifs » que les utilisateurs peuvent télécharger et installer avant que les criminels attaquent leur système non corrigé. Dans de rares cas, les criminels découvriront et exploiteront de nouvelles vulnérabilités avant que le fabricant ou le développeur de logiciels (ou le grand public) s'en rende compte. Ces vulnérabilités se nomment « vulnérabilités de jour zéro ». Il est par conséquent important de mettre à jour votre logiciel afin d'incorporer les derniers correctifs dès que ceux-ci sont disponibles. Encore une fois, les appareils et systèmes logiciels plus vieux comportent souvent un degré de vulnérabilité qui leur est propre, particulièrement s'il existe un risque que les correctifs ou les mises à jour n'aient pas été régulièrement effectués. Les pirates sophistiqués comprennent ce risque et l'utilisent à leur avantage.

Rançongiciel : Les courriels d'hameçonnage et les compromissions d'adresses courriel professionnelles ainsi que les appareils non sécurisés peuvent également être utilisés pour installer un logiciel malveillant sur l'ordinateur ou un autre appareil d'un utilisateur, ce qui entraîne un deuxième type courant d'attaque appelée **rançongiciel**. Le rançongiciel est un logiciel malveillant qui verrouille (« chiffre ») les fichiers ou les systèmes d'un utilisateur. Les rançongiciels peuvent être installés de diverses façons, notamment au moyen d'un courriel d'hameçonnage ou d'un compte d'utilisateur compromis ou de façon moins courante, par clé USB. Avant de mettre en place un rançongiciel, les pirates vont souvent voler les données et supprimer les sauvegardes de données. Comme mentionné précédemment, les groupes derrière un rançongiciel exigeront une rançon en échange de la suppression des données volées et du déverrouillage (« déchiffrement ») des fichiers ou des systèmes.

Comment Sollio AG et Agromart protègent vos renseignements

Les mesures de sécurité mises en place par Sollio AG et Agromart et chaque membre du secteur agricole sont essentielles afin d'assurer la sécurité de toute personne et de ses renseignements. Sollio AG et Agromart ont mis en place les types de mesures de sécurité suivantes afin d'atténuer le risque entourant les données que vous leur communiquez :

- désigner un chef de la protection des renseignements personnels chargé de la direction des politiques et des pratiques en matière de protection de la vie privée et de sécurité au sein de nos organisations et de l'obligation d'en rendre compte;
- mettre en place l'authentification multifacteur pour l'ensemble des services externes et des services administratifs internes;
- migrer l'entièreté de l'infrastructure vers un service infonuagique protégé par l'authentification multifacteur et un accès conditionnel;
- s'assurer que chaque site d'entreprise est sur son propre réseau;
- implanter un gestionnaire de mots de passe d'entreprise et renforcer la politique en matière de mot de passe;
- mettre en place une nouvelle génération d'antivirus/de plateforme de détection et de réponse (EDR) et passer en revue la configuration du pare-feu;
- implanter un service de prévention de la perte des données pour se protéger contre l'exfiltration de données et améliorer le contrôle des bases de données et des fichiers essentiels;
- implanter des alertes pour les comptes administrateur, notamment des alertes en cas de tentative de connexion échouée et d'activités inhabituelles;
- procurer de la formation et déployer des campagnes de sensibilisation sur la cybersécurité.

Que peuvent faire les particuliers ainsi que votre entreprise agricole pour aider à prévenir les cyberattaques?

Il est important que l'ensemble des organisations accorde une grande importance à la protection de la vie privée et à la sécurité des données. Nous avons énuméré quelques conseils ci-dessous afin de vous aider à vous assurer que vos pratiques en matière de protection de la vie privée et de sécurité des données sont robustes et que vous êtes protégé contre les cybercriminels :

- **Ayez recours à des mesures de sécurité éprouvées :** des mesures telles que des mots de passe robustes modifiés régulièrement, des gestionnaires de mots de passe et l'authentification multifacteur contribueront grandement à sécuriser

- vos données. La combinaison de ces mesures avec d'autres étapes courantes de sécurité des données comme le fait de tenir à jour ses logiciels, le chiffrement des données sensibles entreposées et transmises et l'utilisation de logiciels de surveillance de programmes malveillants (comme des logiciels « de détection et de réponse ») aideront à contrecarrer plusieurs risques de cybersécurité.

  Un mot de passe robuste combine des lettres majuscules et minuscules, des chiffres et des symboles. Il peut s'agir d'un mot ou d'une phrase que vous seul connaissez dans laquelle vous remplacez des lettres par des chiffres, par exemple « R0verestm0nchien^ ».

- **Investissez dans la formation en matière de cybersécurité :** malheureusement, l'erreur humaine est l'un des risques de cybersécurité les plus fréquents auquel tous sont exposés. Investir dans de la formation qui fait mention des risques les plus courants comme l'hameçonnage et le rançongiciel est important. Des programmes de formation gratuits sont disponibles en ligne, comme celui offert par le gouvernement du Canada à l'adresse https://www.cyber.gc.ca/fr/education-communaute/carrefour-apprentissage/cours/625-cybersecurite-pour-petites-moyen-entreprises.

- **Mettez hors service les appareils et les comptes qui ne sont plus utilisés :** les appareils et les comptes désuets ou ne faisant plus d'objet d'une surveillance qui ne reçoivent plus les mises à jour de sécurité peuvent constituer une porte d'entrée à votre système facilement accessible pour les pirates. Envisager de mettre à jour régulièrement ou de mettre hors service ces appareils et ces comptes.

- **Conserver des sauvegardes de données, y compris des sauvegardes qui ne sont pas connectées ou qui ne peuvent pas être modifiées :** si vous êtes victime d'une attaque, le fait d'avoir des sauvegardes récentes et sécurisées est une étape importante pour s'assurer que votre organisation peut rapidement reprendre ses activités.

- **Segmenter votre réseau :** si votre organisation doit utiliser des appareils qui ne sont pas sécurisés, consulter des professionnels de l'informatique au sujet de la segmentation de votre réseau afin de vous assurer que vos systèmes essentiels n'interagissent pas avec les appareils non sécurisés.

- **Consultez des experts :** si vous n'êtes pas certain des étapes à prendre ou des façons de sécuriser vos systèmes, consultez des experts en sécurité informatique. Ceux-ci seront en mesure de vous aider à mettre en place des mesures de sécurité des données adéquates pour vos systèmes.

Où puis-je en apprendre davantage à propos de la cybersécurité?

Vous pouvez obtenir plus de renseignements au sujet des pratiques de protection de la vie privée et de sécurité des données en consultant les ressources suivantes :

Centre antifraude du Canada, *Protégez-vous contre les fraudes* : https://antifraudcentre-centreantifraude.ca/protect-protegez-fra.htm.

Community Safety Knowledge Alliance, *Cyber Security Capacity in Canadian Agriculture*: https://cskacanada.ca/projects/strengthening-the-cyber-security-capacity-of-canadas-agricultural-sector/ (en anglais seulement).

Gouvernement du Canada (Agriculture et Agroalimentaire Canada), *La cybersécurité et votre entreprise agricole* : https://agriculture.canada.ca/fr/programmes/outils-gestion-risques-finances-agricoles/cybersecurite-votre-entreprise-agricole.

Ali Dehgnantanha, Hadis Karimipour, Amin Azmoodeh, *Cybersecurity in Smart Farming: Canada Market Research*: https://arxiv.org/abs/2104.05183 (en anglais seulement).

Dr. Taylor Reynolds (Massachusetts Institute of Technology, Internet Policy Research initiative) *Cybersecurity for Agriculture*: https://www.usda.gov/sites/default/files/documents/S22_Taylor_Connectivity-in-Rural-America.pdf (en anglais seulement).