Assemblée générale annuelle de 2004 de la FCA

27 février, 10 h 30 – 12 h 30

Commandité par :

Scotiabank®

Résumé : Aperçu de l'atelier sur la cybersécurité dans le secteur canadien de l'agriculture

Lors de l'atelier, les participants ont exploré les menaces pressantes en matière de cybersécurité auxquelles est confronté le secteur canadien de l'agriculture. L'atelier visait à renforcer les connaissances de base, à évaluer des scénarios réels d'atteinte à la sécurité et à définir des stratégies de réponse et d'atténuation efficaces pour se protéger contre de futurs cyberincidents. Un thème récurrent tout au long de l'atelier était le défi de discuter ouvertement de la cybersécurité et le besoin critique d'un engagement proactif de lutte contre la cybercriminalité.

Signaler un cyberincident - Centre canadien pour la cybersécurité

La cybersécurité et votre entreprise agricole - agriculture.canada.ca

Panélistes :

- Merina Johnston, directrice principale, Stratégie et projets, Agriculture canadienne, Banque Scotia
- Ali Dehghantanha, Chaire de recherche du Canada en cybersécurité et les renseignements sur les menaces
- Katherine MacDonald, Directrice générale, Gestion stratégique, Direction générale des systèmes d'information à Agriculture et Agroalimentaire Canada
- Charles-Félix Ross, directeur exécutif, Union des producteurs agricoles
- Janos Botschner, consultant principal, HumInsight

Thèmes clés :

Le système alimentaire canadien n'est pas suffisamment préparé aux cyberattaques, alors que la numérisation accroît sa vulnérabilité

Le secteur est confronté à des risques croissants d'attaques perpétrées au moyen de rançongiciels, où les pirates informatiques verrouillent et volent des informations et exigent une rançon pour les débloquer. Les petites et moyennes entreprises (PME) du secteur agricole sont particulièrement vulnérables en raison des nombreux points d'entrée que peuvent utiliser les pirates. L'attrait croissant de l'agriculture pour les pirates informatiques s'explique par son évolutivité par rapport aux grandes entreprises. Le rôle du secteur en tant qu'infrastructure

critique et son empreinte numérique croissante en font une cible de choix, avec des menaces documentées venant d'entités étrangères situées notamment en Iran, en Corée du Nord et en Russie, motivées par des raisons financières ou malveillantes. Les avancées technologiques, y compris l'IA, sont des armes à double tranchant, offrant de nouvelles opportunités à exploiter aux cybercriminels.

Un appel urgent est lancé aux agriculteurs pour qu'ils signalent les cybercrimes, avec l'appui assuré d'Agriculture et Agroalimentaire Canada (AAC), soulignant la nécessité d'une approche collective de la cybersécurité.

Incident de cybersécurité à l'UPA

Une brèche de sécurité informatique survenue pendant une période de vacances a révélé la vulnérabilité de l'Union des producteurs agricoles (UPA), affectant de nombreuses organisations et de nombreux systèmes. Cet incident a mis en évidence la nécessité de disposer d'un plan d'intervention complet, **comprenant des stratégies juridiques, informatiques, de négociation et de communication.** Il était clair qu'il faut mettre l'accent sur des stratégies prédéfinies, l'évaluation des risques et la prise de mesures de cybersécurité solides telles que la surveillance du web et l'analyse des vulnérabilités.

Il faut agir rapidement pour mettre en œuvre de solides pratiques de cybersécurité dans toutes les associations agricoles, mais il est nécessaire aussi de favoriser une culture de sensibilisation et d'intégration stratégique de la cybersécurité dans le cadre de l'exploitation du secteur. Pour renforcer la cyberpréparation et la résilience, Community Safety Knowledge Alliance (CSKA),dans le cadre de son projet Cybersécurité dans l'agriculture canadienne a créé des outils gratuits pour les producteurs afin d'améliorer la gestion des risques de l'entreprise agricole et la cyberhygiène au sein de l'exploitation.

Mesures de base pour rendre votre exploitation agricole plus sûre sur le plan informatique

La CSKA recommande une approche adaptative pour renforcer la cyberrésilience de l'agriculture canadienne en créant une capacité en réseau pour une collaboration et un soutien durables. Ce concept est connu sous le nom de « Cyber Barn Raising » (Action agricole collective pour la cybersécurité). Il englobe quatre domaines d'activité couvrant la chaîne de valeur agroalimentaire et son écosystème :

- Soutien à la cybersécurité dans les exploitations agricoles centré sur les producteurs
- Partenariats publics-privés
- Développement des capacités du personnel
- Gouvernance renforcée pour renforcer la confiance

Le cadre et les recommandations de renforcement de la cyberrésilience de l'agriculture canadienne sont disponibles à l'adresse suivante : Cyber Barn Raising.