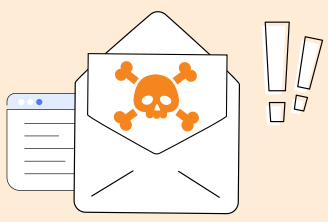
CYBERSÉCURITÉ : UNE ÉTUDE DE CAS DANS LE SECTEUR LAITIER

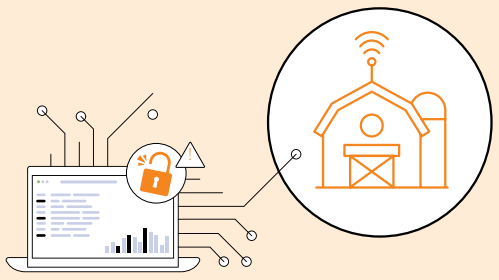
Les agroentreprises de toutes tailles sont vulnérables aux cyberincidents. Voici un exemple de la façon dont une attaque par hameçonnage pourrait avoir une incidence sur votre entreprise et de ce que vous pouvez faire pour la protéger.

Alex, propriétaire d'une **petite exploitation laitière**, reçoit un **courriel supposément de la banque** sur son ordinateur d'entreprise.

Le courriel indique que le **compte bancaire d'Alex a été bloqué**. Voulant le réactiver, **Alex clique sur le lien**.



Malheureusement, le **courriel et le lien sont frauduleux**. Au lieu de mener au site web de la banque, le lien télécharge un rançongiciel sur l'ordinateur d'Alex.



L'ordinateur portable d'Alex est **connecté à l'ensemble du réseau de l'exploitation**. Le rançongiciel se propage rapidement et crypte toutes les données de l'exploitation.

Cette attaque a de graves conséquences

Trayeuses automatiques

Le rançongiciel **arrête** les trayeuses autonomes, ce qui **perturbe** le programme de traite et a des **répercussions** sur la santé des vaches et la production de lait.

Perturbation de la chaîne d'approvisionnement

Toutes les **coordonnées** et les **communications** de la chaîne d'approvisionnement sont cryptées, ce qui interrompt les commandes et la distribution.

- Alex ne peut pas passer de commandes d'aliments pour animaux, de fournitures vétérinaires ou d'équipements, et ne peut pas recevoir de mises à jour sur les livraisons.
- Le processus de distribution est paralysé. Les livraisons de lait sont interrompues, les inventaires et l'état des commandes sont affectés.

Arrêt des activités

Les logiciels de gestion agricole et les dossiers essentiels sont **inaccessibles**, ce qui a des conséquences sur les activités de l'exploitation.

- L'exploitation ne peut pas communiquer avec ses partenaires ou gérer la logistique, ce qui entraîne des retards, des délais non respectés et une atteinte potentielle à la réputation.
- Alex ne peut pas accéder à ses courriels pour joindre les clients.
- Beaucoup de commandes sont retardées, des livraisons sont oubliées et la confiance des partenaires est érodée.

L'exploitation agricole d'Alex **ne dispose pas d'une équipe de TI ni d'une cyberassurance**. En l'absence de services de restauration en cas d'incident, Alex **sent une obligation de payer la rançon pour décrypter les données et reprendre ses activités**. Les pertes financières et les perturbations des activités sont dévastatrices.

La situation d'Alex aurait pu être atténuée

- Alex et **les employés auraient dû être formés** pour reconnaître les courriels d'hameçonnage et éviter de cliquer sur des liens suspects.
- **Des logiciels antivirus et anti-logiciels malveillants** auraient pu détecter et bloquer le rançongiciel avant qu'il ne se propage.
- **La segmentation du réseau** peut empêcher la propagation des logiciels malveillants.
- **Des sauvegardes régulières** sur un site isolé, hors réseau, auraient permis à Alex de restaurer plus facilement les systèmes. La sauvegarde des données crée des copies des informations importantes, et le stockage séparément du système principal, p. ex. sur un disque dur externe ou un service sécurisé en nuage, renforce le degré de sécurité.
- **Une cyberassurance** peut fournir un soutien financier et un accès à des services professionnels d'intervention en cas d'incident.
- **Les interventions en cas d'incident** permettent de s'assurer que tous les employés savent comment réagir en cas de cyberincident.

Soyez vigilant pour protéger votre entreprise

Visitez notre **site web** pour plus de renseignements

agriculture.canada.ca/cybersecurite-entreprise-agricole

Agriculture et Agroalimentaire Canada
Agriculture and Agri-Food Canada
Canada