En bref

- Les cyberrisques incluent le vol, les dommages ou la perte d'appareils et de données.
- Les mises à jour, les sauvegardes régulières et la sensibilisation sont des mesures préventives efficaces, tandis que les assurances couvrent les conséquences.
- En cas d'attaque, une réaction rapide et bien préparée peut minimiser les dégâts.

Pour se prémunir contre les cyberattaques, il s'agit de choisir des mots de passe hautement sécurisés. A cet effet, un mot de passe doit comporter au moins 12 caractères ainsi que tous les éléments suivants : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux (cf. code QR). Photo : ChatGPT

Si la digitalisation révolutionne le secteur agricole, elle apporte également son lot de risques: cyberattaques, pertes de données et dépendance technologique posent de nouveaux problèmes aux exploitations. Cependant, des mesures existent pour réduire le risque de piratage informatique.

Texte: Maurus Renggli

Les logiciels de gestion des exploitations et des troupeaux simplifient les tâches administratives, tandis que les robots de traite et d'alimentation assistent les agriculteurs·trices dans les étables. De plus, les machines guidées par GPS optimisent les travaux aux champs. Ces avancées ont déjà modifié en profondeur le quotidien des agriculteurs·trices. A l'avenir, l'intelligence artificielle (IA) jouera un rôle croissant, notamment pour le suivi des machines ou la reconnaissance des adventices lors des travaux de pulvérisation ou de binage. Cependant, la dépendance accrue à ces technologies s'accompagne de nouveaux risques.

Maurus Renggli
Fondation Agrisano, spécialiste en assurances agricoles

Une menace en constante augmentation

Les cyberrisques incluent le vol, les dommages ou la perte d'appareils et de données. Les logiciels malveillants, comme ceux de rançon (« ransomware »), bloquent l'accès aux appareils ou encryptent les données pour exiger une somme d'argent en échange de leur restitution. Les pertes de données ou de production qui en résultent peuvent entraîner une baisse des revenus et nuire à la réputation de l'exploitation auprès des client·es et des partenaires. Par ailleurs, des litiges juridiques ou des dommages liés à la responsabilité civile (RC) peuvent également survenir.

En 2023, les coûts mondiaux de la cybercriminalité étaient estimés à environ 600 milliards de francs, soit près des trois quarts du PIB suisse (803 milliards). En Suisse, les incidents signalés à l'Office fédéral de la cybersécurité (OFCS) ont presque doublé au premier semestre 2024, passant de 15 700 à 34 700 par rapport à l'année précédente.

Cyberrisques particuliers dans l'agriculture

Les cyberattaques ne visent pas seulement les grandes entreprises: les PME et les particuliers sont aussi concernés. Les secteurs en pleine transition digitale, comme l'agriculture, sont particulièrement vulnérables en raison de l'interconnexion croissante des machines et des systèmes. Le piratage d'une exploitation laitière équipée d'un robot de traite en 2024 témoigne de cette vulnérabilité accrue: les pirates informatiques ont bloqué l'accès à des données essentielles,

Etendue de la couverture d'une bonne cyberassurance

- Service de gestion de crises disponible 24/7
- Prise en charge des coûts pour le remplacement du matériel informatique et la restauration des données
- Compensation des pertes de revenus et des coûts supplémentaires dans le cas où le matériel informatique, les logiciels ou les données ont été endommagés
- Indemnisation des pertes de revenus liées aux atteintes à la réputation
- Remboursement en cas de vols de données ou de paiements liés à des cyber-extorsions
- Couverture des frais de campagnes de communication
- Couverture de la RC, (y c. RC du fait de publications dans les médias)
- Assistance juridique et prise en charge des amendes

Réduire les vulnérabilités

- **Sensibilisation :** il s'agit d'encourager la prise de conscience chez soi et auprès des collaborateurs·trices. Les menaces informatiques les plus courantes incluent les appels ou courriels frauduleux se faisant passer pour des autorités, de fausses offres d'emploi et les attaques par logiciel de rançon. Il est donc essentiel de vérifier la plausibilité des liens ou des pièces jointes contenus dans les courriels ou les sites Web.
- **Mises à jour régulières :** pour combler les failles de sécurité, il convient de maintenir les systèmes d'exploitation et les logiciels à jour.
- **Utilisation de gestionnaires de mots de passe :** les gestionnaires de mots de passe permettent de générer et de stocker des mots de passe robustes, augmentant ainsi la sécurité. Ils simplifient également le quotidien grâce au remplissage automatique des noms d'utilisateur et des mots de passe.
- **Routine de sauvegarde :** il est important de sauvegarder régulièrement les données pour pouvoir les restaurer rapidement en cas d'incident. A cet effet, il est recommandé d'utiliser des systèmes ad hoc indépendants, comme un disque dur externe, connecté au réseau principal uniquement lors de l'enregistrement des sauvegardes.

telles que les calendriers d'insémination, et exigé une rançon de 10 000 francs.

Mesures gouvernementales

La Confédération met en œuvre une stratégie nationale pour sensibiliser la population et les entreprises aux cyberrisques. Une stratégie de digitalisation spécifique à l'agriculture a également été développée, incluant un programme de transformation, par le biais de la plateforme de communication DigiAgriFoodCH. L'objectif est de réduire la charge administrative, d'améliorer la sécurité des données et d'optimiser l'utilisation des ressources.

Prévention et assurances

Toute personne utilisant des technologies digitales doit être consciente des risques qui y sont associés. Pour évaluer ces derniers, il convient de considérer le type d'exploitation et du niveau de recours aux technologies digitales ainsi que de se poser les questions clés suivantes : quels systèmes de l'exploitation pourraient être attaqués et quelles en seraient les conséquences sur le fonctionnement de celle-ci ? Sur le marché des assurances, diverses solutions sont proposées pour couvrir les risques liés à la cybercriminalité, y compris pour les exploitations agricoles (cf. encadré).

Bien choisir sa couverture

Les offres d'assurance varient non seulement en termes de primes, mais aussi en termes de couverture. Pour économiser tout en restant bien protégé, il est préférable d'ajuster la quote-part à un niveau supportable pour l'exploitation, plutôt que de réduire la couverture des risques (stratégie à éviter). Aujourd'hui, les cyberassurances restent peu répandues dans le secteur agricole, laissant une grande partie des dommages potentiels non couverts, une situation qui souligne l'importance de renforcer les mesures de prévention et de protection financière.

En cas de cyberattaque, les appareils doivent être immédiatement déconnectés du réseau.

Que faire en cas d'attaque ?

En cas de cyberattaque, les appareils concernés doivent être immédiatement déconnectés du réseau. De plus, les accès doivent être bloqués et les mots de passe, changés. Il est également crucial de sécuriser et documenter les preuves (fichiers journaux, courriels, etc.). Enfin, l'incident doit être signalé à l'OFCS et à la police.

Pour faciliter la gestion de la crise, il est recommandé de faire appel à un·e responsable de la sécurité informatique ou, si l'exploitation dispose d'une cyberassurance, à des expert·es mandatés par l'assureur. De même, il est avisé de simuler des scénarios d'attaque et d'élaborer un plan d'urgence afin de mieux se préparer. Combiner des mesures de prévention, des solutions d'assurance et des initiatives étatiques constitue la clé pour renforcer la résilience de l'agriculture suisse face aux cyberrisques. ■

Cliquez ici pour vérifier votre mot de passe

qr.ufarevue.ch/mot-de-passe

Informations complémentaires

www.ncsc.admin.ch/ncsc/fr/home.html (OFCS)

www.digiagrifood.ch/fr