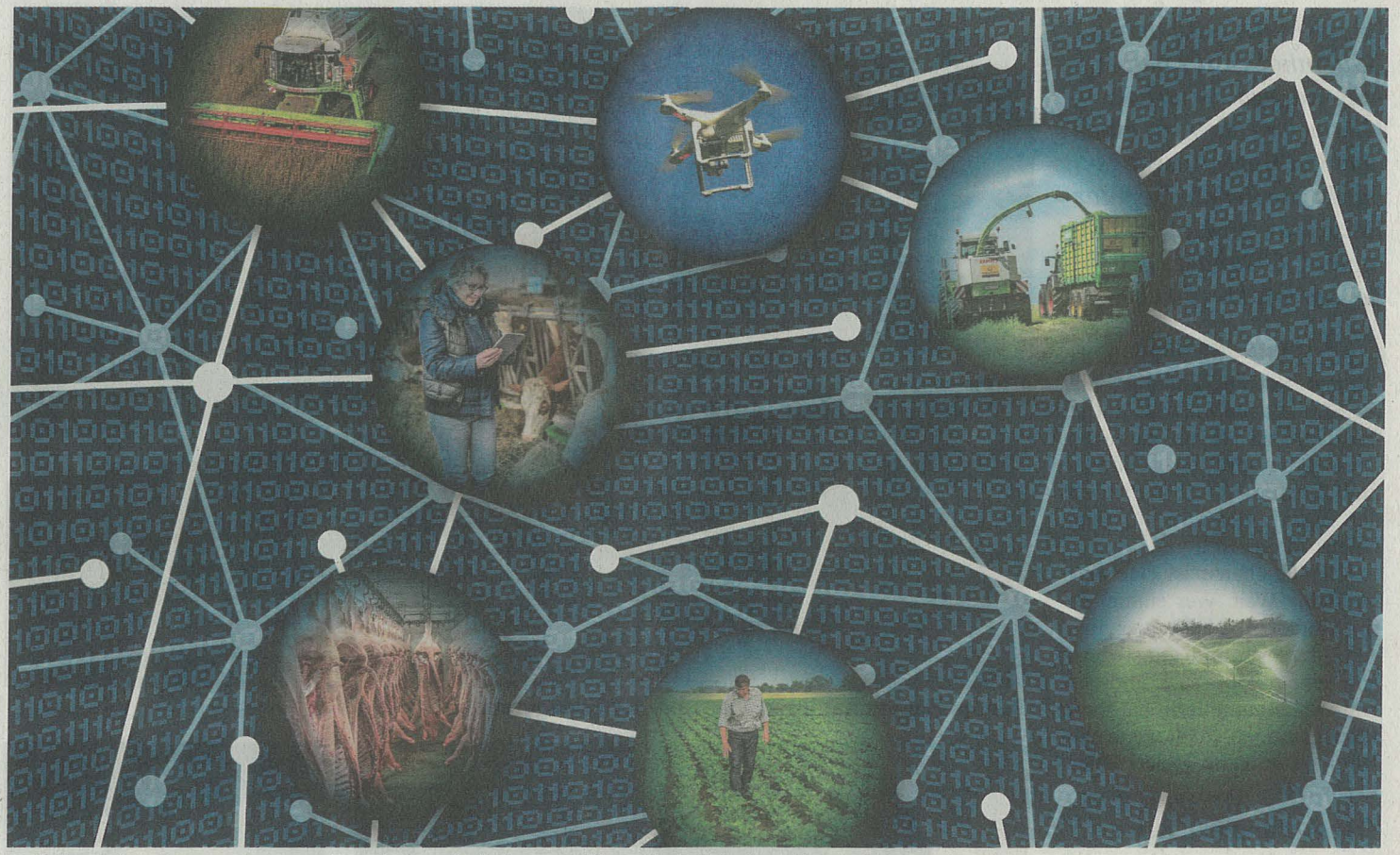
CYBERKRIMINALITÄT: Angriffsfläche bieten nicht nur grosse Smart-Farming-Betriebe

Das Risiko für einen Angriff minimieren

Gezielte Attacken auf Computersysteme können Betriebsabläufe erheblich stören. Treffen kann es jeden. Sorgfalt bei der Datensicherheit hilft dem vorzubeugen, eine Cyberversicherung hilft im Schadensfall.

MARCELLO MARRA*

«Chancen und Risiken der Digitalisierung in der Landwirtschaft» war Thema eines Kurses, den die Agrisano kürzlich in Windisch AG durchführte. Agroscope informierte über den aktuellen Stand der Forschung, während Hersteller und Anwender von Stalltechnik und Farmmanagementsystemen aus der Praxis berichteten. Das Themenspektrum umfasste auch mögliche Auswirkungen auf die Arbeitssicherheit sowie Cyberversicherungen.



Gefahren in einer vernetzten Landwirtschaft lauern überall. *(Bild: Agrarfoto)*

Datensicherheit

Gefahren in einer vernetzten Landwirtschaft lauern überall. *(Bild: Agrarfoto)*

Datensicherheit

Welche Systeme könnten im eigenen Betrieb angegriffen werden, welche Auswirkungen hätte dies, und wie reagiert man im Ernstfall? sind Fragen, die sich jeder stellen sollte. Manche Massnahmen sind aufwendig und mit höheren Kosten verbunden, andere sind ganz leicht umzusetzen. Zum Beispiel die Passwortverwaltung. Die Nutzung verschiedener Passwörter, idealerweise mit einem Passwortmanager, ist eine kosteneffiziente und sehr wirkungsvolle Methode, um die Sicherheit digitaler Systeme zu erhöhen. Dies betrifft nicht nur Passwörter für kritische Infrastrukturen, sondern auch jene für den PC im Stall oder das eigene Smartphone. Ein weiterer entscheidender Aspekt ist die regelmässige Datensicherung (Backup). Sicherungskopien sollten offline, also auf einem externen Medium, an einem separaten Ort aufbewahrt werden.

Eine häufige Schwachstelle für Schadprogramme ist veraltete Software. Um dieses Risiko zu verringern, sollten alle Computer und Server so konfiguriert sein, dass sie automatisch Sicherheitsupdates erhalten.

Aufmerksam bleiben

Auch die Sensibilisierung der Mitarbeitenden ist wichtig, um beispielsweise nicht Opfer von Phishing-Angriffen zu werden. Bei diesen Attacken wird versucht, persönliche Informationen durch betrügerische E-Mails oder Websites zu erlangen. Manche sind leicht erkennbar, da sie viele Rechtschreibfehler enthalten. Andere sind fehlerfrei und täuschend echt im Layout bekannter Firmen gestaltet. Deshalb sollte man immer prüfen, ob die Absenderadresse seriös ist und der Inhalt der Nachricht Sinn ergibt. Im Zweifel sollte man keine Links oder Anhänge anklicken. Ein gut eingestellter Spamfilter kann ebenfalls hilfreich sein.

Viele Angriffspunkte

Jedes Smartphone und jeder PC sind potenzielle Angriffspunkte. Im Bereich Smart Farming können Melk-, Fütterungs- und Entmistungsroboter betroffen sein. Anfällig für Cyberangriffe – verbunden mit einer Störung der Betriebsabläufe – sind auch Traktoren, da sie zunehmend vernetzt sind. Cyberangriffe können unmittelbare finanzielle Folgen haben (z. B. Lösegeldforderungen oder Einbussen aufgrund eines Betriebsunterbruchs).

Anfällig für Cyberangriffe sind auch Traktoren, da sie zunehmend vernetzt sind.

Was Versicherungen bieten

Diffuser und somit schwieriger zu beziffern sind Reputationsschäden, die beispielsweise durch Virusversand an Kunden verursacht werden oder durch Angriffe auf Social-Media-Accounts, die wiederum zu vernichtender Kritik (sog. Shitstorms) führen können.

Vorbeugende Massnahmen im Bereich Datensicherheit sind zentral und reduzieren das Schadenspotenzial am effektivsten. Cyberversicherungen kommen ins Spiel, wenn trotzdem ein Schaden entsteht. Für Versicherer sind Cyberversicherungen ein relativ neuer Bereich, und die angebotenen Lösungen unterscheiden sich nicht nur in Bezug auf die Prämien. Auch die Deckungen variieren stark. Abstriche beim Deckungsumfang sind zu vermeiden. Um Kosten zu sparen, wird empfohlen, stattdessen den Selbstbehalt auf ein für den Betrieb tragbares Mass zu erhöhen.

Wer gefährdet ist

Auf dem KMU-Portal des Seco finden sich unter der Rubrik «Trends» weiterführende Informationen zum Thema Cybersicherheit. Mittels eines Schnell-Checks kann man einfach herausfinden, ob die technischen, organisatorischen und mitarbeiterbezogenen Massnahmen ausreichend Schutz vor Cyberrisiken bieten. Denn für Cyberkriminelle sind nicht nur grosse Unternehmen interessant, sondern insbesondere auch leicht zu hackende Accounts von Privatpersonen oder KMU.

*Der Autor ist Fachspezialist Produkte und Support bei der Agrisano Stiftung in Brugg AG.

DAS DECKT EINE CYBERVERSICHERUNG AB

- 24/7-Krisenmanagement-Service
- Hardware-Ersatzkosten
- Daten-Wiederherstellungskosten
- Ertragsausfall und Mehrkosten infolge Hardware-/Software-/Datenschäden
- Ertragsausfall aus Reputationsschäden
- Vergütung bei Cyber-Diebstählen
- Vergütung von Erpressungszahlungen
- Kampagnen-Kosten
- Haftpflichtdeckung inklusive Medienhaftpflicht
- Rechtsbeistand und Bussenübernahme

CHECK FÜR KMU

Dieser Online-Fragebogen zeigt auf, ob die wichtigsten technischen, organisatorischen und mitarbeiterbezogenen Massnahmen für ein Mindestmass an Cybersicherheit umgesetzt werden.

FÜR DIE BAUERN?

Aktuell gibt es keine branchenspezifische Lösung. In der Schweiz bieten verschiedene grosse Versicherungsunternehmen Produkte an, die man bei Bedarf anhand des in diesem Beitrag genannten Deckungsumfangs miteinander vergleichen sollte.