Hackern keine Lücke lassen

Quer gelesen

- Zu den Cyberrisiken gehören Diebstahl, Beschädigung oder Verlust von Geräten und Daten.
- Prävention durch Updates, Backups und Sensibilisierung schützt vor Cyberangriffen, Versicherungen vor den Folgen.
- Bei Angriffen ist eine vorgängig durchdachte, schnelle Reaktion wichtig, um den Schaden zu minimieren.

Der Schutz vor Cyberangriffen beginnt mit starken Passwörtern. Ein sicheres Passwort ist mindestes 12 Zeichen lang und besteht aus einer Kombination von Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen (siehe QR-Code). Bild: Chat-GPT

Die Digitalisierung revolutioniert die Landwirtschaft, bringt aber auch Risiken mit sich. Cyberangriffe, Datenverluste und technische Abhängigkeiten stellen Betriebe vor neue Herausforderungen. Es gibt jedoch Massnahmen, mit denen man das Risiko eines Hackerangriffs verringern kann.

Text: Maurus Renggli

Softwares für Betriebs- und Herdenmanagement erleichtern die Büroarbeit, Melk- und Fütterungsroboter unterstützen die Arbeit im Stall und GPS-gesteuerte Maschinen helfen bei Feldarbeiten. Die Automatisierung und Digitalisierung haben den Arbeitsalltag in der Landwirtschaft bereits grundlegend verändert. Immer häufiger wird auch der Einsatz von künstlicher Intelligenz (KI) eine Rolle spielen, beispielsweise für das Monitoring von Maschinen oder Unkrauterkennung bei Spritz- und Hackarbeiten.

Maurus Renggli
Agrisano Stiftung, Fachspezialist landw. Versicherungswesen

Zugleich steigt aber auch die Abhängigkeit von diesen Technologien und die damit verbundenen Risiken.

Bedrohung steigt rasant

Zu den Cyberrisiken gehören Diebstahl, Beschädigung oder Verlust von Geräten und Daten. Mithilfe eingeschleuster Software wird der Zugriff auf Geräte gesperrt oder die darauf enthaltenen Daten verschlüsselt, um anschliessend ein Lösegeld für die Wiederherstellung zu verlangen (Ransomware). Datenverluste und Produktionsausfälle können zu Ertragseinbussen und zu Reputationsschäden gegenüber Abnehmern, Lieferanten und Kunden führen. Auch Haftpflichtschäden und rechtliche Auseinandersetzungen sind möglich.

Die geschätzten jährlichen Kosten durch Cyberkriminalität belaufen sich weltweit auf circa 600 Milliarden Franken. Zum Vergleich: Das Schweizer Bruttoinlandprodukt betrug im Jahr 2023 über 803 Milliarden Franken. In der Schweiz haben sich die beim Bundesamt für Cybersicherheit (BACS) gemeldeten Vorfälle im ersten Halbjahr 2024 im Vergleich zur Vorjahresperiode von rund 15 700 auf 34 700 mehr als verdoppelt.

Gefahren für die Landwirtschaft

Cyberangriffe betreffen nicht nur Grossunternehmen, sondern auch KMU-Betriebe und Privatpersonen. Branchen, die noch in der digitalen Transformation stecken, sind davon besonders betroffen. Dazu gehört auch die Landwirtschaft, da die vorhandene Vernetzung von Maschinen und Systemen Angriffsfläche bietet. Dies zeigt sich

Deckungsumfang einer guten Cyberversicherung

- 24/7-Krisenmanagement-Service
- Kosten für den Ersatz der Hardware und die Wiederherstellung von Daten
- Ertragsausfall und Mehrkosten infolge von Schäden an Hardware, Software oder Daten
- Ertragsausfall aufgrund von Reputationsschäden
- Vergütungen bei Cyberdiebstählen und Erpressungszahlungen
- Kampagnenkosten
- Haftpflichtdeckungen inklusive Medienhaftpflicht
- Rechtsbeistand sowie die Übernahme von Bussen

Angriffsflächen vermeiden

- **Sensibilisierung:** Bewusstsein bei sich selbst und den Mitarbeitenden fördern. Die häufigsten Cyberbedrohungen sind betrügerische Anrufe oder E-Mails im Namen von vermeintlichen Behörden, falsche Stellenangebote und Ransomware-Angriffe. Daher sollten Anhänge in E-Mails oder Links auf Websites auf ihre Plausibilität geprüft werden.
- **Regelmässige Updates:** Betriebssysteme und Software sollten aktuell gehalten werden, um Sicherheitslücken zu schliessen.
- **Passwortmanager nutzen:** Passwortmanager generieren und speichern starke Passwörter und erhöhen so die Sicherheit. Eine Erleichterung im Arbeitsalltag ist zudem die automatische Abfüllung der Benutzernamen und Passwörter.
- **Backup-Routine:** Daten sollten regelmässig gesichert werden, um sie im Ernstfall schnell wiederherstellen zu können. Dazu sollten unabhängige Sicherungssysteme wie eine externe Festplatte genutzt werden, die nur während des Abspeicherns des Backups mit dem Hauptnetzwerk verbunden ist.

anhand eines Praxisbeispiels aus dem Jahr 2024. Damals wurde ein Milchwirtschaftsbetrieb mit Melkroboter von Cyberkriminellen gehackt. Diese sperrten den Zugang zu wichtigen Daten wie die Besamungszeitpunkte und forderten Lösegeld in Höhe von 10 000 Franken.

Massnahmen auf Bundesebene

Der Bund treibt die Umsetzung der nationalen Cyberstrategie voran, um Bevölkerung und Wirtschaft für Cyberrisiken zu sensibilisieren und sie zu schützen. Speziell für die Landwirtschaft wurde eine Digitalisierungsstrategie entwickelt, einschliesslich eines Transformationsprogramms auf der Kommunikationsplattform DigiAgriFoodCH. Ziel ist es, den administrativen Aufwand zu verringern, die Datensicherheit zu erhöhen und den Ressourceneinsatz effizienter zu gestalten.

Prävention und Versicherungen

Wer digitale Technologien nutzt, sollte sich der damit verbundenen Risiken bewusst sein. Die Risikobeurteilung variiert je nach Betriebszweig und Digitalisierungsgrad. Zentrale Fragen sind: Welche Systeme könnten im eigenen Betrieb angegriffen werden und welche Auswirkungen hätte dies auf die Weiterführung des Betriebes? Auf dem Versicherungsmarkt werden mittlerweile verschiedene Lösungen angeboten, um Unternehmen – auch landwirtschaftliche Betriebe – gegen Cyberrisiken abzusichern (siehe Kasten).

Keine Abstriche bei der Deckung

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. In der Landwirtschaft ist die Verbreitung von Cyberversicherungen zurzeit noch verhältnismässig gering. Nur ein kleiner Teil der potenziellen Schäden ist durch Versicherungen abgedeckt, was den Handlungsbedarf bei Prävention und finanzieller Absicherung verdeutlicht.

«Im Falle eines Angriffs sollten Geräte sofort vom Netzwerk getrennt werden.»

Wie reagieren bei einem Angriff?

Im Falle eines Cyberangriffs sollten betroffene Geräte sofort vom Netzwerk getrennt werden. Zugänge sollten gesperrt und Passwörter geändert werden. Beweise wie Protokolldateien und E-Mails sind zu sichern und zu dokumentieren. Der Vorfall sollte dem BACS gemeldet und die Polizei informiert werden.

Es empfiehlt sich, IT-Sicherheitsbeauftragte oder – sofern eine Cyberversicherung besteht – deren Mitarbeitende hinzuzuziehen, um den Vorfall professionell zu bewältigen. Um besser auf einen Cyberangriff vorbereitet zu sein, sollten Szenarien durchgespielt und ein Notfallplan erstellt werden. Mit den kombinierten Massnahmen aus Prävention, Versicherungsschutz und staatlichen Initiativen kann die Cyberresilienz der Landwirtschaft in der Schweiz gestärkt werden. ■

Hier gehts zum Passwortcheck

qr.ufarevue.ch/passwort

Weiterführende Informationen

www.ncsc.admin.ch (BACS)
www.digiagrifood.ch