bitkom

Cyberresilienz in der Landwirtschaft

Whitepaper | Landwirtschaftliche Betriebe besser gegen Cyberattacken schützen

Herausgeber
Bitkom e. V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartnerin
Jana Moritz | Referentin Digital Farming & Food Tech
T 030 27576-443 | j.moritz@bitkom.org

Verantwortliches Bitkom-Gremium
AK Landwirtschaft

Autorinnen
Sarah Hanuschik | Research Analyst | Deutor
Jana Moritz | Referentin Digital Farming & Food Tech | Bitkom

Layout

Lea Joisten | Bitkom

Titelbild
© Daniel Hurst – stocksy.com

Inhalt

1 Einleitung

Durch die zunehmende Digitalisierung gewinnt der Aspekt der Cyber- und IT-Sicherheit in der Landwirtschaft immer mehr an Bedeutung. Laut einer repräsentativen Studie des Bitkom aus dem Jahr 2022 nutzen bereits 79 Prozent der Betriebe mindestens eine digitale Technologie. Jeder sechste Betrieb plant, innerhalb der nächsten 12 Monate in digitale Technologien und Anwendungen zu investieren.[1] Unzureichend geschützte digitale und vernetzte Systeme bieten jedoch Einfallstore für Hacker- oder Cyberangriffe mit potenziell schweren ökonomischen Folgen.

79 %

Der Landwirtinnen und Landwirte in Deutschland nutzen mindestens eine digitale Technologie bzw. ein digitales Verfahren.

Für die meisten Betriebe wiegen die Vorteile der Digitalisierung schwerer als die Bedenken. Insbesondere Zeitersparnis, körperliche Entlastung und eine umweltschonendere Produktion sind Gründe für den Einsatz digitaler Technologien. Derzeit spielen Aspekte der Cyber- und IT-Sicherheit beim Erwerb und Implementierung von digitalen Systemen und Prozessen keine große Rolle. Dabei sehen fast die Hälfte der Landwirtinnen und Landwirte (46 Prozent) die Sorge um ausreichende IT-Sicherheit als größte Hemmnisse bei der Digitalisierung der Landwirtschaft an.[1]

Insbesondere Bedrohungen aus dem Cyberraum sind für viele Nutzerinnen und Nutzer von digitalen Lösungen schwer einzuschätzen. Obwohl immer wieder Nachrichten über Hackerangriffe auf landwirtschaftliche Erzeugungs- und Verarbeitungssysteme auftauchen, ist das Bewusstsein für die Cyberbedrohungslage, insbesondere für den eigenen Betrieb, noch unzureichend vorhanden. Mangelndes Wissen im Umgang mit Cyberbedrohungen und Fragen der Verantwortlichkeit können zu einem Erstarren im Angesicht dieser Herausforderung führen. Dabei ist schnelles Handeln von immenser Wichtigkeit. Je früher sich Betriebe und Anbieter von digitalen Lösungen auf die mögliche Bedrohungslage einstellen, desto weniger kann ein Angriff anrichten.

Hersteller von digitalen Anwendungen tragen einen Teil der Verantwortung, indem sie Sicherheitslücken schließen und Nutzerinnen und Nutzer vor Angriffen schützen. Gerade die neuen Möglichkeiten von Cloud-Lösungen, bei denen die eigentliche Absicherung gegen Cyber-Angriffe vom Anbieter vorgenommen wird, und nicht mehr wesentlich beim Anwender selber erfolgt, bieten hier ein hohes Maß an zusätzlicher Sicherheit. Aber auch die Betriebe können durch Schulungen im Umgang mit Cyberbedrohungen und Konzepte für die Absicherung ihrer Systeme einen erheblichen Beitrag leisten.

Als Bitkom möchten wir das Bewusstsein für die Relevanz und Notwendigkeit von Cybersicherheit in der Landwirtschaft steigern. Mit diesem Whitepaper richten wir uns an Akteurinnen und Akteure aus der Praxis, Industrie und Politik und sprechen Handlungsempfehlungen für eine verbesserte Cyberresilienz in der Landwirtschaft aus.

1 Bitkom – Digitalisierung der Landwirtschaft 2022

2 Was bedeutet Cyberresilienz?

Die Resilienz bezeichnet die Fähigkeit eines Systems, trotz negativer Einflüsse von außen weiterhin funktionsfähig zu bleiben und sich möglichst schnell von Schäden zu erholen. In landwirtschaftlichen Systemen und Prozessen wird dieser Aspekt aufgrund der zunehmenden Globalisierung, Digitalisierung und Automatisierung immer wichtiger. Das Ziel ist dabei, Risiken zu minimieren und mögliche Schäden auf ein Minimum zu reduzieren, damit die Systeme und Prozesse schnellstmöglich wieder in ihren ursprünglichen Zustand zurückkehren können.

> Die Frage ist nicht, ob ein Unternehmen Opfer eines Cyberangriffs wird, sondern wie und warum.

Während das Konzept IT-Sicherheit hauptsächlich darauf abzielt, ein System wie einen Computer oder einen Clouddienst durch Werkzeuge wie Antivirenprogramme zu schützen, geht die Cybersicherheit einige Schritte weiter. Um im Falle eines Angriffs möglichst schnell wieder arbeitsfähig zu sein und Ertragsausfälle und Schäden zu minimieren, bedarf es einer gründlichen Vorbereitung, wie beispielsweise einer umfassenden Dokumentation aller relevanten Daten und Prozesse. Je sorgfältiger man in der Präventionsphase arbeitet, desto schneller kann man in der Reaktionsphase – also während eines Angriffs – handeln.

Die drei Phasen der Cybersicherheit

Präventionsphase	Reaktionsphase	Stabilisationsphase
▪ Risikomanagement ▪ Lagebeurteilung / Lagebild ▪ Technische und organisatorische Maßnahmen ▪ Awareness und Training	▪ Incidentmanagement (Projekt, Technisch) ▪ Krisenmanagement (geschäftlich, Versicherung) ▪ Kommunikationsmanagement (Behörden, Täter, Forensik, Soziale Medien, Internet etc..)	▪ Wiederherstellung der Geschäftstätigkeit mit hoher Cyber-Resilienz ▪ Vermeidung weiterer Angriffe ▪ Cybersichere Architektur- & Planung

Tabelle: Cyberstrategien für Unternehmen und Behörden; Michael Bartsch, Stefanie Frey, eigene Darstellung

Die Cyberresilienz beschreibt die Fähigkeit, optimal auf Angriffe zu reagieren, Schäden zu minimieren und schnellstmöglich zu einem funktionierenden System zurückzukehren. Auch wenn es dabei nur um Stunden geht, können diese Stunden entscheidend sein, ob beispielsweise eine Ernte noch gerettet werden kann oder die Lüftungsanlage im Schweinestall rechtzeitig wieder in Betrieb genommen wird.

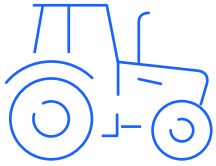
3 Bedrohungslage

Laut einer Bitkom-Studie aus dem Jahr 2021 stiegen die Schäden, die Unternehmen durch digitale Straftaten verursacht wurden, im Jahr 2020 auf 223 Mrd. Euro. Obwohl es keine expliziten Zahlen für den agrarwirtschaftlichen Sektor in Deutschland gibt, zeigen zahlreiche internationale Angriffe, dass auch hier mit einer Zunahme von Angriffen und Schäden gerechnet werden muss. Die größte Gefahr besteht durch skalierte Angriffe auf einen Landtechnikhersteller und dessen auf den Betrieben im Einsatz befindliche Technik.

86 %

der Unternehmen in Deutschland haben 2020 einen Schaden durch Cyberangriffe erlitten. (aus Bitkom Wirtschaftsschutz 2021)

Was kann passieren?



Traktoren mit digitaler Steuerungstechnik werden fahrunfähig gemacht.

Ein zu hoch dosiertes Pflanzenschutzmittel, das digital bestimmt wird, zerstört die Ernte.

Ein lahmgelegter Melkroboter führt zu verzögerten Arbeitsabläufen auf dem Milchviehbetrieb.

Cyberangriffe werden zunehmend so konzipiert, dass sie nicht nur auf einzelne Unternehmen abzielen, sondern auf Lieferketten und Wertschöpfungsketten. Dadurch hat eine Cyberattacke in der Regel multiple Auswirkungen. Ein Angriff auf eine Molkerei kann schnell zu Problemen beim Milchviehbetrieb führen, dessen Milch nicht mehr abgeholt werden kann, oder beim Lebensmitteleinzelhandel, dem keine Ware mehr geliefert wird. Es ist daher umso wichtiger, dass sich alle Akteure innerhalb der Lieferkette angemessen absichern, um eine reibungslose Prozesskette aufrechtzuerhalten.

4 Handlungsempfehlungen

4.1 Anwenderinnen und Anwendern

Unabhängig davon, wie gut ein System geschützt ist, kann ein Klick auf den falschen Link Cyberkriminellen Tür und Tor öffnen. Anwenderinnen und Anwender sollten sich ihrer Verantwortung bewusst sein und auch alle Nutzer des Netzwerks dafür sensibilisieren - das sind in landwirtschaftlichen Betrieben neben Angestellten oft auch Familienmitglieder. Eine Sicherung aller Systeme, die im Schadensfall noch abrufbar ist, ist elementar, um die wichtigsten Prozesse schnellstmöglich wieder zum Laufen zu bringen. Gerade in der Nutztierhaltung können Stunden, in denen eine Belüftungsanlage nicht läuft, über das Leben von Tieren entscheiden.

Für Landwirtinnen und Landwirte ist es daher essenziell, sich auf die eingesetzten Lösungen verlassen zu können. Bei der Auswahl des Anbieters sollte bereits auf ein erprobtes Cybersicherheitskonzept geachtet werden.

Um Systeme bestmöglich zu schützen, können Nutzerinnen und Nutzer folgende Maßnahmen ergreifen:

- **Beratungsangeboteim Bereich Cybersecurity wahrnehmen:** Ein Dienstleister unterstützt bei Trainings und Schulungen zur Erhöhung der Awareness bei Phishing-Angriffen, Identitätsdiebstahl sowie bei Maßnahmen zur Erhöhung der technischen und organisatorischen Sicherheit und dient auch als Ansprechpartner in Krisenzeiten.
- **Abschließen einer Cyberversicherung:** Diese übernimmt die Kosten, die bei der Wiederherstellung der Systeme im Falle eines Cyberangriffs entstehen, wie z. B. Aufwände für forensische Dienstleistungen und das Krisenmanagement. Da diese Leistungen oft an strenge Vorgaben gebunden sind, die das Unternehmen erfüllen muss, um den vollen Versicherungsschutz zu erhalten, empfiehlt sich hier die Unterstützung durch Cyber-Expertinnen und -Experten.
- **Nutzung von Cloud-Services:** Hier übernimmt der Anbieter einen Teil der Verantwortung für die Sicherheit. Und im Fall der Fälle kann die Landwirtin, der Landwirt, kurzfristig über einen anderen Computer unmittelbar weiterarbeiten und somit auch im Krisenfall ortsunabhängig auf wichtige Daten und Anwendungen zugreifen.

Daher benötigen Nutzer von digitalen Lösungen dauerhafte Unterstützung von Experten für Cybersicherheit, die sich um alle Phasen eines Angriffs kümmern und Spezialisten für Prävention, Reaktion und Stabilisierung sind. Zu den Dienstleistungen im Bereich der Cybersicherheit gehören neben dem Inzident- und Krisenmanagement auch Basisdienste, die schon vor dem Angriff dafür sorgen, dass das Unternehmen die Anforderungen einer Cyber-Versicherung erfüllt und gegenüber relevanten Cyber-Risiken gut aufgestellt ist. Individuelle, kundenspezifische Zusatzdienste sollten bei Bedarf

dazu gebucht werden. Dazu gehören zum Beispiel Schulungen für Mitarbeiterende, die über aktuelle Bedrohungen aufklären und ein Bewusstsein für Cybersicherheit schaffen, oder auch die Erstellung eines technischen Lagebildes, um eine zuverlässige Sicherheitsarchitektur gewährleisten zu können.

Die Stärkung digitaler Kompetenzen ist zudem von entscheidender Bedeutung, um die Cybersicherheit in der Landwirtschaft zu gewährleisten. Landwirtinnen und Landwirte müssen in der Lage sein, die Risiken zu erkennen, angemessene Schutzmaßnahmen zu ergreifen und im Falle eines Angriffs schnell zu reagieren. Dies erfordert eine stärkere Integration von digitalen Inhalten in der Aus- und Weiterbildung sowie verbesserte Informations- und Weiterbildungsangebote für Landwirtinnen und Landwirte.

4.2 Industrie

Hackerangriffe auf landwirtschaftliche Strukturen sind Angriffe auf die Versorgungsinfrastruktur und können weitreichende Folgen haben. Anbieter von digitalen Lösungen, sei es in der Innen- oder Außenwirtschaft, tragen somit eine besondere Verantwortung.

Im April 2022 warnte das FBI vor Ransomware-Attacken auf landwirtschaftliche Systeme[2]. Forschende der University of Cambridge betonen in ihrem im Februar 2022 veröffentlichten Paper die Bedeutung eines systemischen Verständnisses von Risiken und externen Effekten für den verantwortungsvollen Einsatz von künstlicher Intelligenz in der Landwirtschaft.[3]

Durch eine Erhöhung der (Cyber-)Sicherheit und der Fähigkeiten können Anbieter ihre Systeme bestmöglich schützen:

- **Cybersicherheit:** Hierunter fallen Maßnahmen zur Absicherung des Unternehmens gegen Cyberangriffe. Diese umfassen Präventions-, Reaktions- und Stabilisationsmaßnahmen, um einen erfolgreichen Cyberangriff zu erschweren und das Unternehmen schnell und mit minimalem Schaden durch die Krise zu bringen.
- **Fähigkeiten:** Cybersicherheit ist ein sich schnell entwickelnder Bereich, der viel Erfahrung und Know-how erfordert. Um eine bestmögliche Sicherheit zu gewährleisten, sollten Anbieter in entscheidenden Entwicklungsstufen externe Experten hinzuziehen.

2 ↗https://www.ic3.gov/Media/News/2022/220420-2.pdf
3 ↗https://www.nature.com/articles/s42256-022-00440-4

4.3 Politik & Verwaltung

1. **Verbesserung der Forschungslage**
   Laut einer im März 2022 im »International Journal of Disaster Risk Science« veröffentlichten Studie gibt es aktuell keine empirischen Untersuchungen, die sich mit der Resilienz und Vorbereitung auf Katastrophen im Bereich der Landwirtschaft im Allgemeinen und insbesondere für landwirtschaftliche IT-Systeme befassen[4]. Die unzureichende Forschungslage und die damit einhergehende mangelnde Datenlage erschweren die Identifikation von Risikofaktoren und möglichen Maßnahmen. Es bedarf daher Fördermaßnahmen, die die Digitalisierung und Cybersicherheit gleichermaßen vorantreiben.

2. **Verbesserung der Datenlage zu Cyberangriffen**
   In Deutschland fehlen generell Daten zu Cyberangriffen, da diese Fälle nicht meldepflichtig sind. Es ist nicht bekannt, wie viele Unternehmen betroffen sind und welcher Schaden entstanden ist. Eine flächendeckende Risikobewertung von landwirtschaftlichen Unternehmen und ihrer Prozessketten ist erforderlich, um Schwachstellen zu identifizieren und gezielte Maßnahmen zu ergreifen.

3. **Schaffung unbürokratischer Meldemöglichkeiten**
   Um die effektive Bekämpfung von Cyberangriffen in der Landwirtschaft zu gewährleisten, ist es von großer Bedeutung, den bürokratischen Aufwand im Zusammenhang mit der Meldung und Bearbeitung von Cyberangriffen deutlich zu reduzieren. Landwirtinnen und Landwirte müssen in der Lage sein, solche Vorfälle schnell und unkompliziert zu melden, um eine schnelle Reaktion und Unterstützung seitens der zuständigen Behörden und Fachleute zu ermöglichen. Dies erfordert eine Vereinfachung der Meldeverfahren und die Schaffung von klaren, benutzerfreundlichen Kanälen für die Kommunikation von Cyberangriffen. Eine effiziente Meldungsstruktur trägt dazu bei, dass Informationen über Cyberangriffe zeitnah erfasst werden können, um präventive Maßnahmen zu ergreifen, weitere Schäden zu minimieren und die Sicherheit in der Landwirtschaft zu stärken.

4. **Aufklärung und Informationskampagne**
   Um das Bewusstsein für Cybersicherheit in der Landwirtschaft zu stärken, ist die Durchführung einer umfassenden Aufklärungs- und Informationskampagne von großer Bedeutung. Landwirtinnen und Landwirte sollten über die bestehenden Risiken und Bedrohungen im Bereich der Cybersicherheit informiert werden. Diese Aufklärungskampagne sollte praxisnahe Beispiele, Fallstudien und Best Practices enthalten, um den Landwirtinnen und Landwirten ein besseres Verständnis für potenzielle Angriffsszenarien zu vermitteln. Darüber hinaus sollten Schulungen und Workshops angeboten werden, um ihnen das nötige Wissen und die Fähigkeiten zur Erkennung und Abwehr von Cyberangriffen zu vermitteln. Eine breit angelegte Informationskampagne in der Landwirtschaftsgemeinschaft wird das Bewusstsein für Cybersicherheit erhöhen und dazu beitragen, dass Landwirtinnen und Landwirte proaktiv Maßnahmen ergreifen, um ihre Betriebe vor Cyberbedrohungen zu schützen.

4 ↗Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers

5 Fazit

Die Digitalisierung bietet der Landwirtschaft immense Chancen, um Prozesse effizienter zu gestalten und die Erträge zu steigern. Jedoch birgt die Nutzung von digitalen Technologien auch Risiken, insbesondere im Bereich der Cybersicherheit. Hackerangriffe können nicht nur zu Umsatzeinbußen führen, sondern auch die Versorgungsinfrastruktur eines Landes gefährden.

Aktuell gibt es eine mangelnde Forschungs- und Datenlage bezüglich der Resilienz landwirtschaftlicher IT-Systeme. Es bedarf daher Fördermaßnahmen, die die Digitalisierung und Cybersicherheit in gleichem Maße vorantreiben und im nächsten Schritt sogar Normierungen für den Bereich der IT-Kommunikation in der Landwirtschaft zu schaffen. Damit könnte das Vertrauen in der digitalen Landwirtschaft ausgebaut und gestärkt werden.

Eine flächendeckende Risikobewertung von landwirtschaftlichen Unternehmen und deren Prozessketten ist nötig, um Schwachstellen zu identifizieren und zielgerichtete Maßnahmen einzuleiten.

Es ist zudem von großer Bedeutung, dass Landwirtinnen und Landwirte sich stärker bewusst zu werden, dass sie potenzielle Ziele für Hackerangriffe sein können und entsprechende Maßnahmen ergreifen, um sich effektiv dagegen zu schützen.

Insgesamt muss ein Gleichgewicht zwischen der Nutzung digitaler Technologien und der Gewährleistung von Cybersicherheit gefunden werden, um die Chancen der Digitalisierung in der Landwirtschaft bestmöglich zu nutzen und gleichzeitig die Versorgungsinfrastruktur eines Landes zu schützen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom