Resiliente Digitalisierung der kritischen Infrastruktur Landwirtschaft - mobil, dezentral, ausfallsicher

Christian Reuter[1], Wolfgang Schneider[2], Daniel Eberz[2],
Markus Bayer[1], Daniel Hartung[1], Cemal Kaygusuz[1]

Wissenschaft und Technik für Frieden und Sicherheit (PEASEC), TU Darmstadt[1]
Dienstleistungszentrum Ländlicher Raum Rheinhessen-Nahe-Hunsrück (DLR R-N-H)[2]

Zusammenfassung

Diese Arbeit befasst sich mit der zunehmenden Digitalisierung der kritischen Infrastruktur Ernährungswirtschaft und setzt den Fokus auf die dadurch resultierenden informationstechnologischen Folgen bezüglich der Angriffs- und Ausfallsicherheit der Landwirtschaft und von ihr abhängigen Sektoren. In diesem Kontext wird die Modernisierungen der Landmaschinen und deren Vernetzung sowie das Cloud-Computing analysiert und zu treffende Maßnahmen bezüglich einer resilienten Struktur erläutert. In vielen Bereichen wird dabei aufgezeigt, dass das Ausfallrisiko der Produktion zugunsten von Vorteilen wie Ertrags- und Qualitätssteigerung vernachlässigt wird. Dieser Beitrag plädiert für eine resiliente Digitalisierung in der Landwirtschaft mit gebrauchstauglichen Sicherheitslösungen, um keine zusätzlichen Aufwände für die Nutzer zu erzeugen und somit die praktische Sicherheit zu erhöhen.

1 Einleitung

Modernisierung und Digitalisierung der Ernährungswirtschaft schreiten immer weiter voran, während den informationstechnologischen Konsequenzen nicht ausreichend Beachtung geschenkt wird. Gegenwärtig stehen in der Landwirtschaft Produktivitätssteigerung, Umweltschutz und Qualitätssteigerung durch die digitale Vernetzung im Vordergrund. So gibt es bereits diverse Big Data Ansätze und Projekte, um beispielsweise das Verhalten der Feldwirtschaft mit dem vorrangigen Ziel der Ertrags- und Qualitätssteigerung zu analysieren. 66% der Landwirte sind der Überzeugung, dass die zunehmende Digitalisierung eine Chance für ihr Unternehmen bietet, wohingegen lediglich 13% Risiken sehen (Bitkom, 2016). Da die Ernährungswirtschaft ein Teil der kritischen Infrastruktur ist, sollte diese insbesondere in Hinsicht auf mögliche Angriffspotenziale und auf Ausfallsicherheit analysiert werden. Zudem zeigen Katastrophen, wie die des weitreichenden Stromausfalles vom 14. August 2003 in den USA

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2018 in
R. Dachselt, G. Weber (Hrsg.):
Mensch und Computer 2018 – Workshopband, 02.–05. September 2018, Dresden.
 https://doi.org/10.18420/muc2018-ws12-0330

und in Kanada, dass auch andere benachbarte Sektoren betroffen sein können. Damals kam es infolge eines Stromausfalles zu Problemen in der Nahrungsmittelversorgung, auf welche beide Länder nicht vorbereitet waren (Reuter, 2018). Die vorliegende Arbeit setzt sich daher mit der Ausfall- und Angriffssicherheit insbesondere in Bezug auf die Rolle der Landwirtschaft als zentraler Bestandteil der Ernährungswirtschaft kritisch auseinander. In Kapitel 2 wird zunächst die Fragestellung Landwirtschaft 4.0 - Chance oder Risiken thematisiert. In Kapitel 2.1 geht es um Problemstellungen im Bereich Cloud-Computing. Kapitel 2.2 beschäftigt sich mit der Landtechnik. Kapitel 2.3 schließlich widmet sich der möglichen Störanfälligkeit von Globalen Navigationssatellitensystemen. Ein Fazit zieht erste Schlussfolgerungen aus dem zuvor Gesagten. Besonderes Augenmerk wird im Rahmen dieser Studie auf die Schaffung von resilienten, d.h. widerstandsfähigen, Strukturen zur Eindämmung von Ausfallrisiken und gebrauchstauglichen Sicherheitslösungen gelegt.

2 Landwirtschaft 4.0 - Chance oder Risiko

Infrastrukturen sind für eine ausreichende Daseinsvorsorge und wirtschaftliche Entwicklung erforderlich. Kritisch ist eine Infrastruktur dann, wenn eine Störung erhebliche dauerhafte Auswirkungen auf das Wirtschaftswesen oder die öffentliche Sicherheit hätte. Nach der Definition der EU-Richtlinie 2008/114/EG können auch schon einzelne Teile von größeren Anlagen oder Systemen als kritisch bezeichnet werden (Europäische Union, 2008). **Ernährungswirtschaft** ist eine Infrastruktur zur Produktion und Distribution von Ernährungsgütern und umfasst viele unterschiedliche Glieder in der Wertschöpfungskette der Ernährungswirtschaft, sowohl die Primärproduktion mit den **landwirtschaftlichen Betrieben** als auch die Lebensmittelverarbeitung, sowie den Handel mit Lebensmitteln. In diesen Bereich fallen in Deutschland vor allem eine Vielzahl von kleinen und mittelständigen Unternehmen. Als drittgrößter Industriezweig trägt die Ernährungswirtschaft mit rund 7% zur gesamtwirtschaftlichen Wertschöpfung in Deutschland bei[1]. Die Ernährungswirtschaft ist folglich essentiell für den reibungslosen Ablauf im Staats- und Wirtschaftswesen. Nach der Verordnung zur Bestimmung **kritischer Infrastrukturen** gilt ein Landwirt als Betreiber kritischer Infrastruktur im Sektor Ernährung, sofern der Schwellenwert der Produktion von 434500 Tonnen Speisen oder 350 Millionen Liter Getränke pro Jahr überschritten wird (BMI, 2015).

Um die **Landwirtschaft 4.0** näher zu erläutern, ist es hilfreich den Begriff der Industrie 4.0 zu erklären. Die vierte industrielle Revolution, kurz **Industrie 4.0**, beschreibt einen neuen Ansatz der Steuerung und Organisation der Produktion mittels Vernetzung aller an der Produktion beteiligten Akteure und Maschinen sowie die Möglichkeit das aus diesen Daten gewonnene Wissen zu nutzen, um so flexibel wie möglich auf unerwartete Veränderungen zu reagieren (Bendel, 2018). Hierbei sind die intelligenten Maschinen zwar mit dem IT-System des Unternehmens vernetzt, arbeiten jedoch selbstständig und sind in der Lage, ihren eigenen Arbeitsablauf zu organisieren. Sie reagieren eigenständig auf Veränderungen im Produktionsprozess

[1] https://www.bll.de/embed/pb-flyer-wirtschaftskraft

und handeln dementsprechend. Der Fokus der deutschen Landwirtschaft, die wie bereits dargelegt als kritische Infrastruktur gilt, liegt insbesondere auf der präzisen und nachhaltigen Bewirtschaftung des Bodens. Dies soll künftig das **Smart Farming** durch Erhebung und Analyse von Prozess- und Sensordaten ermöglichen. Wann und wie oft ein Feld gedüngt werden muss, entscheiden intelligente Systeme individuell für den jeweiligen Boden in Abhängigkeit von fusionierten Informationen über Bodenbeschaffenheit, Vegetation, Sorten, Wetterbedingungen und anderen Parametern der pflanzlichen Produktion, um eine nachhaltige und effiziente Ressourcenverwendung zu generieren. Unerwartete Wetterveränderungen haben einen großen Einfluss auf die Sicherstellung des Ertrags. Um die Wetterentwicklung modellieren und abschätzen zu können, sind diese Massendaten von entscheidender Bedeutung. Durch die Vernetzung der gesammelten Wetterdaten sollen bevorstehende Stürme und Starkregenereignisse frühzeitig erkannt werden (Birnesser, 2017) – ähnlich wie Warn-Apps (Reuter, Kaufhold, Leopold, & Knipp, 2017). Nun stellen sich der Evolution im Sinne der Landwirtschaft 4.0 auch einige **Herausforderungen**. So gibt es in landwirtschaftlichen Räumen häufig keine ausreichende Internetversorgung, da eine flächendeckende Breitbandversorgung in dünn besiedelten Räumen kaum profitabel ist. Dies wäre bei der jetzigen Gesetzeslage nur mit einem großen finanziellen Aufwand seitens der Gemeinden umsetzbar. Die bislang nicht benötigte umfassende Qualifikation der Landwirte im Bereich der Informationstechnologie erschwert das Verständnis über die notwendigen Prozesse.. Eine weitere Herausforderung ist die Tatsache, dass die IT-Sicherheit langsamer voranschreitet als die Entwicklung der Landwirtschaft 4.0 (Martínez, 2016).

Bei Betrachtung der nationalen und internationalen **Literatur** fällt auf, dass die möglichen Folgen der digitalen Vernetzung landwirtschaftlicher Betriebsabläufe bezüglich der Verantwortung für die Sicherstellung der Ernährung der Bevölkerung bislang nicht hinreichend reflektiert wurden und nur sehr wenige Quellen existieren: Schneider (2017) beschäftigt sich mit der Datenhoheit und der Ausfallsicherheit von landwirtschaftlichen Betrieben. Ruggeri (2015) thematisiert das erhöhte Sicherheitsrisiko des ISOBUS-Systems, der zentralen Technik des Smart Farmings. Bezüglich der sicherheitskritischen Auseinandersetzung mit dem Global Positioning System (GPS), die nicht prinzipiell einen Bezug zur Landwirtschaft haben, weisen Hui und Na (2009) auf die Möglichkeit hin mit Störsendern das GPS Signal zu unterdrücken. Jafarnia-Jahromi et al. (2012) beschreiben hingegen das GPS-Spoofing, womit es möglich ist, ein vorhandenes GPS-Signal abzuändern oder zu überlagern.

2.1 Cloud-Computing – Datenschutz, Ausfallsicherheit

Cloud-Computing bedeutet, dass Daten nicht mehr vor Ort gespeichert werden, sondern auf Servern in Rechenzentren ausgelagert werden. Ein Vorteil liegt darin, dass die Daten durch lokale Störungen nicht verloren gehen können; der Nachteil besteht darin, dass die Datenschutzgesetze der Staaten sich sehr voneinander unterscheiden. Abbildung 1 veranschaulicht die Funktionsweise von Cloud-Computing in der Landwirtschaft. Schneider (2017) beschäftigt sich mit der Datenhoheit und der davon abhängigen Wertschöpfung von landwirtschaftlichen Betrieben: Essenziell für die Digitalisierung in der Landwirtschaft ist die Erhebung, Bearbeitung und Bewertung bzw. Auswertung von betriebsbezogenen Daten. Die Verwendung von

betriebseigenen Computern birgt dabei einige Schwierigkeiten: So muss die Rechnerinfrastruktur regelmäßig den neuen technologischen Entwicklungen angepasst werden, um beispielsweise neue Sensordaten verwerten zu können. Die ansteigenden Datenmengen, die aus intensiven Analysen und gegebenenfalls sogar Big-Data-Analysen resultieren, lassen die Anforderungen für den Rechenaufwand und den Speicherplatzbedarf enorm ansteigen. Auch die Datenschutzproblematik stellt eine Herausforderung für den landwirtschaftlichen Betrieb dar. Zwar existieren bereits Ansätze, wie z.B. die CARVER+ Shock Primer Methode (U.S. Food & Drug Administration, 2009), zur systematischen Identifikation von Systemschwachstellen, dennoch ist der Landwirt selbst verpflichtet diese anzuwenden, entsprechende Reaktionen bei entdeckten Schwachstellen einzuleiten und generell für den Schutz verwundbarer Systeme zu sorgen. Er sollte regelmäßig Sicherungen auf zusätzlichen Festplatten anlegen und diese sicher aufbewahren sowie sein System regelmäßig mit Updates pflegen. Cloud-Computing ist hier ein Ansatz: Die Verantwortung der Daten- und Ausfallsicherheit wird hiermit in andere, vermeintlich sichere Hände gelegt. Doch diese Methode ist auch mit erheblichen Risiken verbunden, denen meist nur am Rande Beachtung geschenkt wird.

Abbildung 1: Cloud Computing in der Landwirtschaft (Beispielkommunikation von 365Active (https://www.365farmnet.com/produkt/365active-system/), aufgerufen 28.01.18)

Bei den betrieblichen Daten handelt es sich in der Regel nicht um personenbezogene Daten. Personenbezogene Daten genießen einen besonderen gesetzlichen Schutz. Die hier zur Verfügung gestellten Daten fallen allerdings nur unter **freiwillig bereitgestellte Betriebsgeheimnisse**, die keinen besonderen gesetzlichen Regelungen unterliegen. Wenn ein Cloud-Anbieter diese Daten also für einen nicht legitimen Zweck verwendet, ist das Anwenden von Sanktionen schwierig. Zusätzlich ist es schwer nachzuvollziehen, wie die Daten von einem Cloud-Anbieter innerhalb seiner eigenen Rechnersysteme verwendet werden (Schneider, 2017). Besonders kritisch kann die unerwünschte Verwendung von Daten sein, wenn der Standort der Rechensysteme des Cloud-Anbieters im Ausland ist. Ein weiteres Problem stellt die Ausfallsicherheit der Vernetzung dar. Da der Service vieler Anbieter zumeist wie eine zentrale Drehscheibe funktioniert, über die alle Aktionen innerhalb des landwirtschaftlichen Betriebes koordiniert werden, muss bei deren Ausfall im schlimmsten Falle die gesamte Geschäftstätigkeit stillgelegt werden. Mit anderen Worten: Nutzen ausreichend viele große Betriebe den gleichen Anbieter, so kann es im Extremfall zu Produktionsausfällen bzw. Versorgungsengpässen kommen.

Auch absichtlich verursachte Ausfälle durch **Cyberangriffe** sind nicht auszuschließen. Ein Angreifer könnte zum Beispiel versuchen mithilfe eines so genannten Denial-of-Service-Angriffes den Zugriff auf eine Cloudlösung zu beeinträchtigen oder komplett zu blockieren. Bei einem solchen Angriff werden sehr viele Anfragen, meist von verschiedenen Geräten, an einen Webserver gesendet, mit dem Ziel diesen zu überfordern. Sendet ein Angreifer ausreichend viele Anfragen, ist der Server nicht dazu in der Lage, zwischen validen und böswilligen Anfragen zu unterscheiden und kann diese nicht mehr verarbeiten. Ein Angreifer kann zudem versuchen gezielten Zugriff auf das System zu erlangen. Er kann dazu eventuelle Sicherheitslücken auf den Servern der Cloud-Lösungen ausnutzen oder er kann versuchen über **Social Engineering** Zugriff auf einzelne Konten eines Landwirtes zu erlangen. Dazu dienen zum Beispiel Phishing-Mails, welche den Anschein einer offiziellen E-Mail des Cloud-Anbieters erwecken. Der Landwirt wird dazu aufgefordert, sich auf einer speziell präparierten Webseite mit seinem Kennwort anzumelden, welches der Angreifer anschließend auslesen kann.

Eine mögliche Gegenmaßnahme wäre hier, um den Gefahren des Cloud Computing zu adressieren, zumindest ein teilweise **eigenes dezentrales Netzwerk** zu errichten. Bei einem solchen „Offline-First"-System geht es darum, dass Programme so geschrieben werden, dass sie grundsätzlich ohne Internetanbindung nutzbar sind. Sie können zusätzlich auch noch alle gewohnten Online-Fähigkeiten bieten, um so beispielsweise eine optionale Steuerung über das Smartphone zu ermöglichen. Alle Internetaktivitäten sollten sich jedoch unter Rücksicht auf Datenschutzproblematiken jederzeit deaktivieren lassen (Schneider, 2017). Um eine möglichst resiliente Infrastruktur zu gewährleisten ist ein internes Rechner-zu-Rechner System einer zentralisierten Cloud-Lösung in jedem Fall vorzuziehen. Im Krisenfall stehen so auch ohne Internet in jedem landwirtschaftlichen Betrieb solche abgeschotteten Inselsysteme zur Verfügung, die die Arbeit und Kommunikation der Maschinenflotte aufrechterhalten können. Abbildung 2 veranschaulicht die Funktionsweise von Inselsystemen.

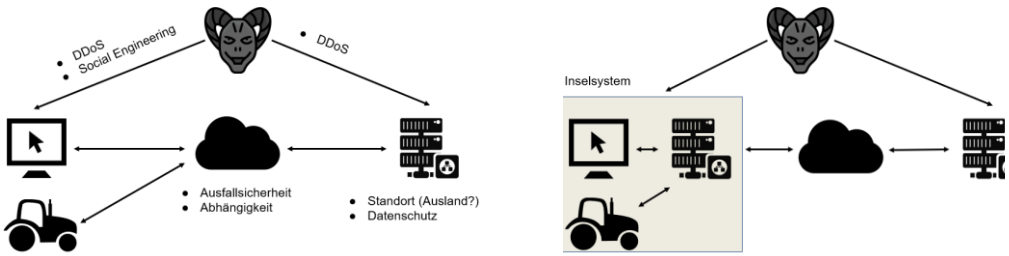

Abbildung 2: Angriffsszenarien (links) und Lösungen (rechts), eigene Darstellung

Bei diesen Maßnahmen gilt es allerdings zu bedenken, dass insbesondere die anfangs beschriebenen Probleme bei der Selbstverwaltung der Infrastruktur auftreten und hier der allgemeinen Computersicherheit starke Beachtung geschenkt werden sollte. Ein Landwirt muss sich also entweder regelmäßig fortbilden oder sollte für die Verwaltung der Infrastruktur entsprechende Serviceangebote von IT-Spezialisten nutzen.

2.2 Landtechnik – Precision Farming & Autonomie

Landtechnik bezeichnet die in der Landwirtschaft eingesetzten Landmaschinen und Geräte sowie deren zugrundeliegende Technik. Darüber hinaus ist der Begriff noch für den Wirtschaftszweig im Agrarsektor gebräuchlich. **Precision Farming** ist dabei ein eingesetzter Lösungsweg, um eine möglichst ortsdifferenzierte und zielgerechte Bewirtschaftung der Felder zu erreichen. Über satellitengesteuerte Navigations- und Kartierungssysteme und Vernetzung von Landmaschinen können Daten erhoben und ausgewertet werden (Pößneck, 2011). Eine im Zuge der Landwirtschaft 4.0 immer weitreichendere Methode in der Landtechnik ist **Precision Agriculture**. Dabei handelt sich um eine Methode, welche durch automatisierte Aufzeichnung und digitale Vernetzung die Bodenverhältnisse und Eigenschaften der Pflanzen auswertet, um so die Landmaschinen sowie den Einsatz von Betriebsmitteln in der Feldwirtschaft möglichst effizient zu nutzen. Zum Einsatz kommen dabei Satellitennavigationssysteme, Sensortechnik und Schnittstellen zu mobilen Endgeräten (Marc et al., 2005). ISOBUS ist der Markenname eines dort verwendeten Datenbusses für landwirtschaftliche Zwecke. Es ist konform zu ISO 11783 entwickelt und ermöglicht einen anbieterübergreifenden Datenaustausch verschiedenster Geräte in der Agrarwirtschaft. Ruggeri (2015) thematisiert das erhöhte **Sicherheitsrisiko** des ISOBUS-Systems und stellt dar, dass ein Traktor in einem ISOBUS-Netzwerk weder in Hinsicht auf **Lokal- oder Fernzugriffe** ein geschlossenes System sei, da das Konzept des Precision Farmings die Offenheit fordere. Es bietet die Möglichkeit mehrere Systeme miteinander zu vernetzen und ermöglicht das Wechseln von Systemkomponenten im laufenden Betrieb, dem sogenannten „Hot-Plugging“. So sei zum Beispiel der eingesetzte „Breakaway Connector“ nicht nur eine Schnittstelle für diverse Verbindungen, sondern auch für alle Arten von Angriffen. In dem Control-Area-Network (CAN-Bus), auf welchem ISOBUS basiert, könne es zu verschiedenen Ausfällen und Fehlern kommen. Mitunter seien Kommunikationsverluste, Nachrichtenwiederholungen, Verzögerungen und Zusammenbrüche des Netzes denkbar.

Darüber hinaus sei es möglich, in dem Netzwerk Nachrichten abzufangen, eigene Nachrichten auf den Bus zu schicken, **Denial-of-Service-Attacken** zu konstruieren und Pakete im laufenden Betrieb zu verändern. Die Folgen eines gezielten Angriffs sind sehr weitreichend und könnten z.B. vom Abgreifen von vertraulichen Daten bis hin zum ungewollten Zugriff auf die Steuerung der Landmaschinen reichen. Dies könnte demzufolge ökonomische Konsequenzen für die landwirtschaftlichen Betriebe, die Wertschöpfungskette der Ernährungswirtschaft oder sogar Auswirkungen auf die Sicherstellung der Ernährungsversorgung haben. Mit einem Anschluss ans Internet seien noch weitere Angriffsmöglichkeiten möglich, indem Personen beispielsweise per WLAN in das ISOBUS System eindringen (Ruggeri, 2015).

Das Betrachten weiterer ISO-Normen (z.B. der ISO 15998 zur Netzwerksicherheit) sei laut Ruggeri eine der Maßnahmen, die es zu treffen gilt. So würde man den Bus möglicherweise um Maßnahmen der Fehlererkennung erweitern. Ein solches Vorgehen solle zumindest die Ausfallsicherheit eingrenzen. Böswilligen Angriffen könne man mit proprietären Ansätzen entgegentreten. Diese folgen dem Prinzip der „**Security through Obscurity**“, womit gemeint ist, dass die eigentliche Funktionsweise geheim gehalten wird (Ruggeri, 2015). Dieser Ansatz werde zwar schon verfolgt, ist jedoch von Standardisierungskörperschaften sehr umstritten. Das US-amerikanische Institut „National Institute of Standards and Technology“ spricht sich

dafür aus, dass Systeme nicht auf dieser Basis konzipiert werden sollten (Scarfone & Tracy, 2008), da die Sicherheit nicht von der Geheimhaltung der Implementierung abhängen sollte.

Eine weitere Maßnahme bestünde darin, explizit die CAN-Bus Architektur gegen Angriffe zu schützen. Um das Abgreifen von Nachrichten zu unterbinden, wäre es möglich eine Verschlüsselung der zu übermittelnden Pakete zu realisieren. Mit einer Authentifizierung könne man zudem das absichtliche Verändern von Nachrichten im laufenden Betrieb, sowie das Senden komplett neuer Pakete einstellen. Replay-Attacken könne man mit einem zeitabhängigen Schutz, wie einer Sequenzierung von Paketen, sicherstellen. Damit wäre jedoch noch nicht die Möglichkeit unterbunden, einen Denial-of-Service-Angriff auszuführen (Ruggeri, 2015). Die Problematik des ISOBUS liegt in der Funktionalität an sich. Das System soll möglichst offen sein, um übergreifend verschiedene Module miteinander zu verbinden. Diese Offenheit bildet jedoch das Einfallstor für Ausfälle und insbesondere Angriffe. Es zeigt sich, dass diese Technik noch viel Verfeinerung braucht, um den Anforderungen kritischer Infrastrukturen gerecht zu werden.

2.3 Globale Navigationssatellitensysteme

In der digitalen Landwirtschaft werden globale Navigationssatellitensysteme (kurz GNSS) für mehrere Methoden verwendet. Dabei kommt bislang zumeist das US-amerikanische „Global Positioning System“ (GPS) zum Einsatz. Die Umlaufbahn der GPS-Satelliten befindet sich in ungefähr 21.000 Metern Höhe, weswegen die Signale eine sehr geringe Feldstärke besitzen. Schon kleinere Störsignale würden GPS-Empfänger vom Entgegennehmen der eigentlichen Signale abhalten (Coffed, 2014). Dies könne bereits durch unbeabsichtigte Einflüsse zu Interferenzen und Ausfällen führen. Demnach sei es möglich mit einem UKW-Radio und einer bestimmten Frequenz das GPS-Signal zu belasten.

Selbst Sonneneruptionen können das Signal stören (Cerruti et al., 2008). Angreifern ist es mit Störsendern, sogenannten **GPS-Jammern**, und einer Rauschmodulation möglich den Empfang des GPS komplett zu unterdrücken (Hui & Na, 2009). Landwirte, welche zukünftig auf den Einsatz autonomer Landmaschinen setzen, könnten so vor Probleme bezüglich der Feldbewirtschaftung gestellt werden. Der Hersteller Case IH präsentierte in diesem Zusammenhang einen autonomen Traktor, welcher sich nach Herstellerangaben ausschaltet, sofern das GPS-Signal gestört oder nicht vorhanden ist (Krauß, 2016). Eine zusätzliche Angriffsmethode ist das **GPS-Spoofing**, mit welchem man nicht nur GPS-Signale beim Empfänger unterdrückt, sondern zusätzlich imitierte Signale aussendet (Jafarnia-Jahromi et al., 2012). Studien zeigen, dass es damit möglich sein kann die Kontrolle des Kurses einer Jacht zu übernehmen (Psiaki & Humphreys, 2016). Angreifern ist es so zum Beispiel möglich GPS-Daten zu manipulieren und damit die Ernte auf den Feldern zu gefährden. Ein politisches Risiko besteht außerdem im Ursprung der GNSS-Lösungen. Die Betreiberländer könnten in Konfliktfällen die Signale verzerren oder regional abschalten.

3 Fazit und Ausblick auf die digitale Hofbox

Die Vernetzung und Digitalisierung in der Ernährungswirtschaft nehmen exponentiell zu. In der Literaturrecherche fällt auf, dass der kritischen Infrastruktur Landwirtschaft jedoch weniger Aufmerksamkeit eingeräumt wird. So ist vor allem erkennbar, dass sich zunächst auf den zukünftigen Nutzen bezogen wird, ohne dabei Risiken und drohende Konsequenzen genau zu untersuchen. Viele Neuerungen führen jedoch zur Erhöhung der Verletzlichkeit. Wie bereits beschrieben sehen 66% der befragten Landwirte eine Chance, jedoch nur 13% ein Risiko in der Digitalisierung (Bitkom, 2016). Diese Einstellung ist wahrscheinlich auch der Grund für das Fehlen wissenschaftlicher Artikel auf diesem Gebiet. Es existieren zwar IT Standards, wie beispielsweise die ISO/IEC-Normen, jedoch fehlt der konkrete Bezug zu den neuen Systemen und Integrationsmöglichkeiten der Landwirte. So ist von den Landwirten auch keine große Reflektiertheit im Sinne der IT-Sicherheit zu erwarten, da das Berufsbild keine tiefgehenden informationstechnologischen Voraussetzungen hat (BMEL, 2018).

Im Zuge des IT-Sicherheitsgesetzes in Deutschland ist zunächst fraglich, ob auch landwirtschaftliche Betriebe oder vielleicht die Vertreiber der Systeme für erfolgreich durchgeführte Cyberangriffe in Verantwortung gezogen werden sollten.. In der Ernährungswirtschaft spielt das Kollektiv der landwirtschaftlichen Betriebe mit unterschiedlicher Betriebsgröße jedoch eine große Rolle. Ein Angriff auf die in der Landwirtschaft weit verbreiteten IT-Systeme, könnte viele Betriebe treffen und würde somit zu einer deutlich höheren Zahl von betroffenen Personen führen, wie die vom BSI formulierten Schwellenwerte.

Die Digitalisierung wird in der Ernährungswirtschaft große Veränderungen bringen. Es fehlt jedoch an der notwendig kritischen Auseinandersetzung mit dem Sicherheitsaspekt der Technologie. Viele Ansätze der IT-Sicherheit oder des betrieblichen Kontinuitätsmanagements adressieren eher Konzerne als kleinere Unternehmen (Reuter, 2015). Es wäre daher von hoher Relevanz resiliente Systeme zu erstellen, und gleichzeitig deren einfache Nutzbarkeit in den Vordergrund zu rücken. Beispiele beinhalten Dashboard-basierte Systeme (Kaufhold, Reuter, & Radziewski, 2018), die die verbleibende Interaktion so einfach wie möglich unterstützen und nicht nur zur Erhöhung der theoretischen Möglichkeiten von Sicherheit, sondern der praktischen Sicherheit beiträgt.

Ein Ansatz, der dies adressiert ist die **digitale Hofbox** (Abbildung 3). Sie beinhaltet neben *karten- und tabellenbasierter Darstellung* der Betriebsdaten auch *GeoFormulare* zum Erteilen von Aufträgen sowie eine verschlüsselte *Kommunikation* mit anderen Nutzern. Den landwirtschaftlichen Betrieben werden die für sie relevanten Geodatendienste des Landes zur kostenfreien Nutzung bereitgestellt; dabei ist sowohl die innerbetriebliche Speicherung und Verteilung als auch die kombinierte On- und Offline-Nutzung mit mobilen Endgeräten möglich. Mit dem Ansatz können relevante Basisdaten für ein überbetriebliches Smart Farming auf Betriebsebene standardisiert vorgehalten werden. Dies sichert zudem die Datensouveränität und damit auch die Wertschöpfung in den Betrieben, was dem ländlichen Raum und der regionalen Wirtschaft insgesamt dient. Insgesamt wird deutlich, dass bei entsprechender Sensibilisierung mobile, dezentrale und ausfallsichere Lösungen bevorzugt werden, aber auch noch zahlreiche

offene Fragen bestehen: Wie können hybride Services, die aus konventioneller Maschinenleistung mit notwendig begleitenden Datendiensten bestehen, beispielsweise über Smart Contracts abgewickelt werden? Wie müssen Interfaces gestaltet werden, welche diese Aspekte für die Zielgruppe der Landwirte umsetzen? Dies sind beispielhafte Fragen, die im Kontext aktueller Arbeiten verfolgt werden.

Abbildung 3: Startbildschirm/Hauptmenü (Tablet- und Smartphone-Version) (links und Mitte), Karteneditor mit ein- und ausklappbarem Menü (rechts oben), Tabelleneditor und aktive Suchfunktion nach Stichworten (rechts unten)

Literaturverzeichnis

Bendel, O. (2018). Industrie 4.0. http://wirtschaftslexikon.gabler.de/Archiv/-2080945382/industrie-4-0-v2.html

Birnesser, C. (2017). Smart Farming: der digitale Bauernhof. https://www.techtag.de/digitalisierung/smart-farming-der-digitale-bauernhof/

Bitkom. (2016). Digitalisierung in der Landwirtschaft. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/November/Bitkom-Pressekonferenz-Digitalisierung-in-der-Landwirtschaft-02-11-2016-Praesentation.pdf

Bundesministerium des Innern (BMI). (2015). *Verordnung zur Bestimmung Kritischer Infrastruktur en nach dem BSI-Gesetz (BSI-Kritisverordnung–BSI-KritisV).*

Bundesministerium für Ernährung und Landwirtschaft. (2018). *Digitalpolitik Landwirtschaft*. http://www.bmel.de/SharedDocs/Downloads/Broschueren/DigitalpolitikLandwirtschaft.pdf

Cerruti, A. P., Kintner, P. M., Gary, D. E., Mannucci, A. J., Meyer, R. F., Doherty, P., & Coster, A. J. (2008). Effect of intense December 2006 solar radio bursts on GPS receivers. *Space Weather*, *6*(10). https://ieeexplore.ieee.org/document/7766339/

Coffed, J. (2014). The Threat of GPS Jamming: The Risk to an Information Utility. https://www.harris.com/sites/default/files/downloads/solutions/d0783-0063_threatofgpsjamming_v2_mv.pdf

Europäische Union. (2008). Richtlinie 2008/114/EG des Rates, 75–82.

Hui, H., & Na, W. (2009). A study of GPS jamming and anti-jamming. *PEITS 2009 - 2009 2nd Conference on Power Electronics and Intelligent Transportation System*, *1*(1), 388–391. https://doi.org/10.1109/PEITS.2009.5406988

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, *2012*. https://doi.org/10.1155/2012/127072

Kaufhold, M.-A., Reuter, C., & Radziewski, E. von. (2018). Design eines BCM-Dashboards für kleine und mittlere Unternehmen. In R. Behling, R. Dachselt, & G. Weber (Eds.), *Mensch & Computer 2018: Workshopband*. Dresden, Germany: Gesellschaft für Informatik e.V.

Krauß, H. (2016). Der autonome Traktor von Case IH. https://www.agrarheute.com/technik/traktoren/brandneu-autonome-traktor-case-ih-526391

Marc, R., Rolf, D., & Meyer, C. (2005). *Precision agriculture: Moderne Agrartechniken und Produktionsmethoden-ökonomische und Ökologische Potenziale*. Büro für Technikfolgen-Abschätzung beim Dt. Bundestag (TAB).

Martínez, J. (2016). Chancen und Risiken der Digitalisierung in der Landwirtschaft – die rechtliche Dimension, *378*(378). http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-4ae5f9fa-478e-4ea1-be57-e45200688bab

Pößneck, J. (2011). Analysen und Trends Thema : Precision Farming im Pflanzenbau. *Landesamt Für Umwelt, Landwirtschaft Und Geologie*, 1–6.

Psiaki, M. L., & Humphreys, T. E. (2016). Protecting GPS From Spoofers Is Critical to the Future of Navigation. *IEEE Spectrum*. https://www.golem.de/news/kursaenderung-forscher-lenkt-luxusjacht-mit-gefaelschtem-gps-signal-um-1307-100702.html

Reuter, C. (2015). Betriebliches Kontinuitätsmanagement in kleinen und mittleren Unternehmen – Smart Services für die Industrie 4.0. In A. Schmidt, A. Weisbecke, & M. Burmester (Eds.), *Mensch & Computer: Workshopband* (pp. 37–44). Oldenbourg-Verlag.

Reuter, C. (2018). *Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement*. Wiesbaden: Springer Vieweg.

Reuter, C., Kaufhold, M.-A., Leopold, I., & Knipp, H. (2017). KATWARN, NINA or FEMA? Multi-Method Study on Distribution, Use and Public Views on Crisis Apps. In *Twenty-Fifth European Conference on Information Systems (ECIS)* (pp. 2187–2201). Atlanta, GA: AISeL.

Ruggeri, M. (2015). Is ISOBUS safe? Regulatory and Technical aspects for the use of ISOBUS in the context of ISO25119, (November).

Scarfone, K., & Tracy, M. (2008). Guide to General Server Security. *National Institute of Standards and Technology*, 53. https://doi.org/10.6028/NIST.SP.800-123

Schneider, W. (2017). Neben Chancen auch Risiken der Landwirtschaft 4.0. *GetreideMagazin*, *6*, 1–15.

U.S. Food & Drug Administration. (2009). An Overview of the Carver Plus Shock Method for Food Sector Vulnerability Assessment. U.S. Food & Drug Administration.