Resilient Smart Farming (RSF) – Nutzung digitaler Technologien in krisensicherer Infrastruktur

Christian Reuter[1], Wolfgang Schneider[2] und Daniel Eberz[2]

Abstract: Resilienz ist in aller Munde. Die vorliegende Arbeit setzt sich mit der Ausfall- und Angriffssicherheit der Landwirtschaft als zentralem Bestandteil der Ernährungswirtschaft im digitalen Zeitalter kritisch auseinander. Dabei geht es nicht um die Frage, ob Smart Farming in der landwirtschaftlichen Praxis sinnvoll ist, sondern ob deren Infrastruktur den Anforderungen einer ausfallsicheren (resilienten) Infrastruktur gerecht wird. Da die Ernährungswirtschaft ein Teil der kritischen Infrastruktur ist, ist deren Analyse in Hinsicht auf mögliche Angriffspotenziale und auf Ausfallsicherheit von gesellschaftlicher Relevanz. Wir schlagen *Resilient Smart Farming (RSF)* zur Nutzung digitaler Technologien in krisensicherer Infrastruktur vor.

Keywords: Smart Farming, Resilienz, Ernährungsvorsorge, Dezentrales Internet, Inselnetze

1 Einleitung

Nach der Verordnung zur Bestimmung kritischer Infrastrukturen gilt ein Landwirt als Betreiber kritischer Infrastruktur im Sektor Ernährung, sofern der Schwellenwert der Produktion von 434.500 Tonnen Speisen oder 350 Millionen Liter Getränke pro Jahr überschritten wird [BI16]. 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 als die vom BSI formulierten Schwellenwerte. Gleichzeitig gilt: Im Ernährungssicherstellungs- und vorsorgegesetz (ESVG) ist die Deckung des lebensnotwendigen Nahrungsmittelbedarfs im Falle einer Versorgungskrise durch den Staat sicherzustellen.

Der Fokus der deutschen Landwirtschaft 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. Die derzeit auf dem Markt verfügbaren Dienstleistungen und Produkte sind dabei durch die Funktionsweise des Cloud-Computing geprägt. Das bedeutet, dass Daten nicht mehr vor Ort gespeichert werden, sondern auf Servern in Rechenzentren ausgelagert werden. Bei den betrieblichen Daten handelt es sich um freiwillig bereitgestellte Betriebsgeheimnisse. Das heißt, dass das Anwenden von Sanktionen schwierig ist, wenn ein Cloud-Anbieter diese Daten

[1] Technische Universität Darmstadt, Wissenschaft und Technik für Frieden und Sicherheit (PEASEC), reuter@peasec.tu-darmstadt.de; www.peasec.de
[2] Dienstleistungszentrum Ländlicher Raum (DLR) Rheinhessen-Nahe-Hunsrück, Bad Kreuznach; wolfgang.schneider@dlr.rlp.de, daniel.eberz@dlr.rlp.de

für einen nicht legitimen Zweck verwendet. Zusätzlich ist es schwer nachzuvollziehen, wie die Daten von einem Cloud-Anbieter innerhalb seiner eigenen Rechnersysteme verwendet werden.

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. Nutzen also 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 (z .B. Denial-of-Service-Angriffe). Eine mögliche Gegenmaßnahme wäre hier, um die Gefahren des Cloud-Computing zu adressieren, zumindest ein teilweise eigenes dezentrales Netzwerk zu errichten (z. B. „Digitale HofBox“). Bei einem solchen „Offline-First“-System geht es darum, dass Programme grundsätzlich ohne Internetanbindung nutzbar sind [Re18]. Sie können zusätzlich auch noch alle gewohnten Online-Fähigkeiten bieten, um so beispielsweise eine optionale Steuerung über das Smartphone zu ermöglichen. Um eine möglichst resiliente Infrastruktur zu gewährleisten, ist ein internes Rechner-zu-Rechner-System einer zentralisierten Cloud-Lösung in jedem Fall vorzuziehen.

In der Ernährungswirtschaft spielt das Kollektiv der landwirtschaftlichen Betriebe mit unterschiedlicher Betriebsgröße jedoch eine große Rolle. Die Vernetzung und Digitalisierung in der Ernährungswirtschaft nimmt exponentiell zu und wird große Veränderungen bringen. In der Literaturrecherche fällt auf [Re18], dass der kritischen Infrastruktur Landwirtschaft und der notwendigen kritischen Auseinandersetzung mit dem Sicherheitsaspekt der Technologie jedoch wenig Aufmerksamkeit eingeräumt wird. Viele Ansätze der IT-Sicherheit oder des betrieblichen Kontinuitätsmanagements adressieren eher Konzerne als kleinere Unternehmen. Es wäre daher von hoher Relevanz, die Infrastruktur für ein resilientes Smart Farming (RSF) zu erstellen. Existierende Herausforderungen und Ansätze sollen im Beitrag detailliert betrachtet werden. Ziel ist es, die Fortschritte der Digitalisierung in der Landwirtschaft zu nutzen, ohne die Ausfallsicherheit der landwirtschaftlichen Primärproduktion und damit die Lebensmittelversorgung der Verbraucher zu gefährden.

Im Folgenden möchten wir auf die Verwundbarkeit der Landwirtschaft (Kapitel 2) eingehen, um im Anschluss die Ernährungsvorsorge in Zeiten von Cyber-Angriffen (Kapitel 3) zu betrachten, auf herstellerübergreifende Standards (Kapitel 4) einzugehen und unsere Vision von Resilient Smart Farming, mit dezentralem Internet und Inselnetzen (Kapitel 5), vorzustellen.

2 Verwundbarkeit der Landwirtschaft und Notwendigkeit resilienter Systeme

Erste Forschungsinitiativen widmen sich der Digitalisierung in der Landwirtschaft. Die Innovationsinitiative *Landwirtschaft 4.0* setzt sich die Ziele, 1) durch spezifische und adaptive Produktionsprozesse die natürlichen Ressourcen und Ökosystemleistungen zu erhalten und zu verbessern, 2) das Ernährungsverhalten unterschiedlicher Bevölkerungsgruppen zu erfassen und zu prognostizieren, um die Bereitstellung von Lebensmitteln mit hoher Qualität zu gewährleisten, und 3) alle Aspekte vom Feld bis zur Gesellschaft zu vernetzen [Le16].

In der Landwirtschaft findet ein Strukturwandel statt [Za13]. Während sich die Zahl der Betriebe verringert, wachsen die durchschnittlichen Kapazitäten, Flächen und Tierbestandsgrößen. Die Digitalisierung bietet Chancen, diesem Strukturwandel entgegenzuwirken. Intelligente Systeme können die Landwirte entlasten, indem sie operative Arbeiten oder Entscheidungen unterstützen. *Smart Farming* betrachtet Automatisierungstechnologien sowie die Erfassung, Verarbeitung und Analyse von Daten in Echtzeit [Ka16].

Die Ausfallsicherheit der landwirtschaftlichen Produktion beziehungsweise deren Resilienz (Widerstandsfähigkeit bei Krisen) wird von Landwirten und deren Organisationen kaum thematisiert. Dabei müsste gerade die Landwirtschaft, die als kritische Infrastruktur von existenzieller Bedeutung eingestuft ist, bei politischen und gesellschaftlichen Weichenstellungen rechtzeitig auf die Resilienz verweisen. Eine ganz neue Dimension und Brisanz liefert die digitale Landwirtschaft 4.0 mit vernetzter Smart-Farming-Landtechnik und zentralen Big-Data-Rechenzentren [Sc17]. Führende Landwirte und Lohnunternehmer schwärmen zwar schon von den Chancen der Technologie. Aber keiner stellt die Frage, wer die Verantwortung trägt, wenn bei dieser geplanten Ausbaustufe der digitalen Landwirtschaft das Internet ausfällt oder Maschinenflotten durch Cyberangriffe paralysiert werden, so dass es zu Produktionsengpässen und -ausfällen kommen könnte. Die global aufgestellten Agrarbusiness- und IT-Konzerne sind nicht verantwortlich, denn diese haben einen zulässigen Stand der Technik umgesetzt. Entsprechend darf der heimischen Landwirtschaft kein Vorwurf gemacht werden, wenn zugelassene und marktgängige Technologien angeschafft wurden.

Dennoch ist von den betroffenen Verbrauchern, die vor leeren Regalen stehen, kein Verständnis für digitale Ausfallursachen zu erwarten. Die Bürger werden den Staat vehement auf dessen Verantwortung zur Sicherung der Ernährung hinweisen, wie es im Ernährungssicherstellungs- und -vorsorgegesetz (ESVG) festgeschrieben ist. Die Veränderung hin zu einem resilienten System ist demnach sozial komplex [Re16]. Es besteht heute ein eklatanter Mangel an Erkenntnissen, welche Auswirkungen auf die informatisierte, in Teilen cloudbasierte Landwirtschaft in zukünftigen Ausnahmesituationen zu erwarten sind. Bereits die zu erwartenden Auswirkungen von Ausnahmesituationen auf die landwirtschaftliche Primärproduktion des heutigen Technisierungsstandes sind unzureichend erforscht. Je nach Zeitpunkt können diese jedoch gravierend sein, z. B. wenn die Anwendung eines Pflanzenschutzmittels oder die Ernte nicht im möglichen Zeit- und

Witterungsfenster erfolgen können. Hier ist eine sehr differenzierte Zukunfts- und Auswirkungsanalyse erforderlich. Setzt sich, wovon auszugehen ist, Smart Farming weiter durch, kommt es zu neuen Gefährdungspotenzialen. Während heute noch Maschinen manuell gesteuert werden können, sind bereits aktuelle Prototypen von Feldrobotern nicht mit dieser Möglichkeit ausgestattet. Zukünftige Ausnahmesituationen werden in ihrer Auswirkung auf die landwirtschaftliche Primärproduktion also durch die technische Dimension nochmals verschärft werden.

3 Ernährungsvorsorge in Zeiten von Cyber-Angriffen gefährdet

Heute ist unbestritten, dass die Digitalisierung die Verwundbarkeit einer Landwirtschaft 4.0 erhöhen kann [Sc17]. Eine wesentliche Ursache ist die technologische Kapselung beziehungsweise die internetbasierte Auslagerung des „digitalen Zentralnervensystems" automatisierter Funktionen im landwirtschaftlichen Produktionsprozess. Entsprechende Sicherheitsprobleme belegt eine Warnung des FBI in den USA vom Frühjahr 2016 [FB16], die besagt, dass das digitale Smart Farming zunehmend im Visier von Cyberangriffen stehe [Re19]. In Krisenfällen können weder Politiker noch Vertreter der Landwirtschaft damit argumentieren, dass die neu geschaffenen Probleme einer digitalen Landwirtschaft nicht vorhersehbar waren. Zudem stellt sich aktuell die Frage, ob eine Allianz zwischen Forschung und Wirtschaft, die in keinem Land der Erde direkte Verantwortung für die Ernährung der Bevölkerung trägt, eine Landwirtschaft 4.0 ohne Auflagen bezüglich der Ausfallsicherheit gestalten darf. Der einzig seriöse Weg ist, die neuen digitalen Herausforderungen den Bürgern gegenüber offen und transparent zu kommunizieren und diese in den Dialog über die Zukunft der Landwirtschaft einzubinden. Hilfreich wäre es, wenn die EU-Agrarforschung baldmöglichst belastbare Ergebnisse aus den Bereichen Sicherheitsforschung und Technikfolgenabschätzung im Bereich der Landwirtschaft 4.0 vorlegen würde. Zudem benötigen Industrie und Landwirtschaft branchenweit abgestimmte Resilienz-Kriterien, um Fehlinvestitionen beim Aufbau einer möglichst ausfallsicheren digitalen Landwirtschaft zu vermeiden.

4 Herstellerübergreifende Standards können die Ausfall-Risiken senken

Mit Blick auf die erwünschte Einführung von Verfahren des Smart Farmings könnte die EU auf die landwirtschaftliche Praxis hören und die Einführung verbindlicher Standards für den Datenaustausch auf Betriebsebene umsetzen. Dies wäre der erste und entscheidende Schritt zu mehr Resilienz und Ausfallsicherheit in der künftigen Landwirtschaft: Statistiken über den Maschinenbesatz werden in Krisenzeiten weitgehend wertlos, wenn sich nicht abschätzen lässt, wie häufig komplette Maschineneinsätze paralysiert werden, weil beispielsweise von Herstellern zwingend geforderte Onlinezugriffe auf Cloud-Rechenzentren ausfallen oder digitale Schnittstellenprobleme vor Ort nicht mehr gelöst

werden können. Für eine kritische Infrastruktur und vor allem für die Bürger sind das kaum akzeptable Zustände, zumal der Gesetzgeber in diesem Bereich die Einhaltung von Schnittstellenstandards und Möglichkeiten des Notbetriebs fordern könnte. Ein positives Beispiel von EU-Aktivitäten sind die standardisierten Schnittstellen für Ladekabel bei Smartphones. Entsprechende Initiativen zur Verbesserung der Ausfallsicherheit einer digitalisierten Landwirtschaft fehlen bisher.

5 Resilient Smart Farming: dezentrales Internet und Inselnetze als Kernkomponente der Ausfallsicherheit

Eine digitale Landwirtschaft 4.0 ist nicht auf den Aufbau zentraler und monopolähnlicher Cloud-Rechenzentren angewiesen. Dieses Ansinnen widerspricht ohnehin dem freien Wettbewerb und den Interessen einer Vielzahl von Firmen, die befürchten, dass sie auf diese Weise von ihrem Kundenstamm in der Landwirtschaft abgekoppelt werden könnten. Diesen meist kleineren Unternehmen, kommt entgegen, dass der neue Trend bei Internetanwendungen in Richtung „Offline-First“ geht. Dabei werden Programme so entwickelt, dass sie auf einer eigenen Datenbank mit den wichtigsten Informationen aufsetzen und auch ohne Internetverbindung funktionsfähig sind. Bei Bedarf besteht jedoch volle Konnektivität, um Daten etwa mit Kollegen zu synchronisieren, die mit Tablets im Schlepper unterwegs sind, oder aber mit der Zentralanwendung auf dem Büro-PC. Bei diesem Ansatz können Landwirte selbst entscheiden, ob sie das Internet nutzen oder die Datentransfers auf das heimische WLAN-Netzwerk beschränken wollen. Damit sichern sie nicht nur ihre Datenhoheit, sondern pflegen auch eine betriebsinterne Digitalisierungsvariante, die sogar funktioniert, wenn Telefonnetze ausfallen sollten.

Dieser in vielen Betrieben mit den unterschiedlichsten Hofprogrammen bereits realisierte Ansatz zeigt, dass Resilienz und Ausfallsicherheit in der Landwirtschaft eher mit betriebsinternen Lösungen und kostengünstigen Apps erreicht werden können als mit Cloudstrukturen von Internet-Giganten. Genau aus diesen Gründen treiben inzwischen auch große Technologiekonzerne die Dezentralisierung des Internets voran. Besonders spannend ist dabei die Entwicklung der direkten Rechner-zu-Rechner-Kommunikation ohne flankierende Vermittlungsdienste. Dies ermöglicht mittelfristig den Aufbau eines möglichst resilienten ländlichen Raums, der im Krisenfall in beliebig zugeschnittene digitale Inselnetze, je nach verfügbarer Notkommunikation, zerfallen kann. Inselnetzfähigkeit und verbindliche Datenaustauschstandards auf Betriebsebene sind die Kernkomponenten einer ausfallsicheren Landwirtschaft 4.0 zur Notkommunikation mit seiner Maschinenflotte, seiner Werkstatt, seinem Landhändler, seinem Lohnunternehmer und zu Nachbarbetrieben, mit denen er möglicherweise noch nie zusammengearbeitet hat. Ausfälle können durch kurzfristige und dezentrale ad-hoc-Kooperation vieler Beteiligter aufgefangen werden, etwa via Smartphones und Tablets durch Rechner-zu-Rechner-Technologien und mobiler ad-hoc Netzwerke (MANET) [Re17a] unter Nutzung von Standards wie Bluetooth oder Wi-Fi Direct [Al14, Re17b].

Danksagung: Das Projekt *Standardisierung der Geobox-Infrastruktur* wird vom Bundesministerium für Ernährung und Landwirtschaft (BMEL) gefördert.

Literaturverzeichnis

[Al14] Al-Akkad, A. et al..: Help Beacons: Design and Evaluation of an Ad-Hoc Lightweight S.O.S. System for Smartphones. In (Jones, M.; Palanque, P.; Schmidt, A.; Grossman, T., Hrsg): Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14). ACM, New York, S. 1485-1494, 2014.

[BI16] Bundesministerium des Innern (BMI): Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung–BSI-KritisV), Bundesgesetzblatt Jahrgang 2016 Teil I Nr. 20, 2016.

[FB16] FBI: FBI Warns of Smart Farm Risk. https://securityledger.com/2016/04/fbi-warns-of-smart-farm-risk/, Stand 30.10.2018.

[Ka16] Kamilaris, A.; Gao, F.; Prenafeta, B.; Ali, M.I.: Agri-IoT: A Semantic Framework for Internet of Things-enabled Smart Farming Applications. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE, Piscataway, S. 442-447, 2016.

[Le16] Leibniz-Forschungsverbund: Positionspapier der Innovationsinitiative Landwirtschaft 4.0. Leibniz-Forschungsverbund, Berlin, 2016.

[Re16] Reuter, C.; Ludwig, T.; Pipek, V.: Kooperative Resilienz – ein soziotechnischer Ansatz durch Kooperationstechnologien im Krisenmanagement. In: Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie (GIO), 47/2, S. 159-169, 2016.

[Re17a] Reuter, C. et al.: Social Media Resilience during Infrastructure Breakdowns using Mobile Ad-Hoc Networks. In (Wohlgemuth, V.; Fuchs-Kittowski, F.; Wittmann, J., Hrsg): Advances and New Trends in Environmental Informatics - Proceedings of the 30th EnviroInfo Conference. Springer, Berlin, S. 75-88, 2017.

[Re17b] Reuter, C. et al.: Digitalisierung und Zivile Sicherheit: Zivilgesellschaftliche und betriebliche Kontinuität in Katastrophenlagen (KontiKat). In (Hoch, G.; Schröteler von Brandt, H.; Stein, V.; Schwarz, A., Hrsg): Sicherheit (DIAGONAL Jahrgang 38). Vandenhoeck & Ruprecht, Götingen, S. 207-224, 2017.

[Re18] Reuter, C. et al.: Resiliente Digitalisierung der kritischen Infrastruktur Landwirtschaft - mobil, dezentral, ausfallsicher. In: Dachselt, R.; Weber, G. (Hrsg.): Mensch und Computer 2018: Workshopband. Gesellschaft für Informatik e.V., Dresden, S. 623-632, 2018.

[Re19] Reuter, C.: Information Technology for Peace and Security. Springer, 2019.

[Sc17] Schneider, W.: Neben Chancen auch Risiken der Landwirtschaft 4.0. In: GetreideMagazin, 6, S. 1-15, 2017.

[Za13] Zander, K. et al.: Erwartungen der Gesellschaft an die Landwirtschaft. Stiftung Westfälische Landwirtschaft, Braunschweig, 2013.