BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Pauline Riousset

Cybersicherheit in der Nahrungsmittelversorgung

Endbericht zum TA-Projekt

Oktober 2024
Arbeitsbericht Nr. 213

Pauline Riousset

Cybersicherheit in der Nahrungsmittelversorgung

Endbericht zum TA-Projekt

TAB-Arbeitsbericht Nr. 213

Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag
Neue Schönhauser Straße 10
10178 Berlin

Telefon: +49 30 28491-0
E-Mail: buero@tab-beim-bundestag.de
Web: www.tab-beim-bundestag.de

2024

Umschlagbild: racool_studio, pikisuperstar/Freepik

ISSN-Internet: 2364-2602

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) berät das Parlament und seine Ausschüsse in Fragen des wissenschaftlich-technischen Wandels. Das TAB wird seit 1990 vom Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) des Karlsruher Instituts für Technologie (KIT) betrieben. Hierbei kooperiert es seit September 2013 mit dem IZT – Institut für Zukunftsstudien und Technologiebewertung gGmbH sowie der VDI/VDE Innovation + Technik GmbH.

Inhalt

Zusammenfassung

Mit der Digitalisierung und Vernetzung technischer Systeme steigt die Verwundbarkeit von Unternehmen in der Nahrungsmittelkette gegenüber Bedrohungen aus dem Cyberraum. Die Bedrohungslage bei der IT-Sicherheit war 2023 höher als je zuvor, wobei Cyberkriminalität eine besonders große Bedrohung darstellt. Der Sektor Ernährung (Lebensmittelproduktion, -verarbeitung und -handel) gehört zu den kritischen Infrastrukturen, die es besonders zu schützen gilt. Im Hinblick auf die Informationssicherheit erfolgt dies durch das BSI-Gesetz[1], nach welchem große Unternehmen im Ernährungssektor verpflichtet sind, ihre IT-Systeme nach aktuellem Stand der Technik abzusichern. Allerdings sind vor allem die Landwirtschaft und das Lebensmittelhandwerk stark von kleinen und mittleren Unternehmen geprägt, für die die Verpflichtungen des BSI-Gesetzes bisher nicht galten. Mit der Umsetzung der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)[2] wird zum einen der Ernährungssektor als wichtiger Sektor auch auf europäischer Ebene anerkannt. Zum anderen werden mit der Richtlinie nicht mehr nur große Betreiber, sondern auch mittlere Unternehmen in die Pflicht genommen, ihre Systeme gegen IT-Sicherheitsvorfälle abzusichern. Der vorliegende Bericht beleuchtet, wie hoch die Vulnerabilitäten der Nahrungsmittelversorgung in Deutschland vor dem Hintergrund möglicher Bedrohungen aus dem Cyberraum sind und skizziert Handlungsoptionen zur Stärkung der Cyberresilienz des Sektors.

IT-Systeme in Landwirtschaft und Ernährungsindustrie

Die Digitalisierung prägt aktuell alle Stufen der Ernährungsversorgung von der landwirtschaftlichen Erzeugung von Nahrungsmitteln bis hin zum Einzelhandel.

Landwirt/innen nutzen, wie andere Berufsgruppen auch, im beruflichen Alltag inzwischen verbreitet mobile Endgeräte, wie Smartphones und Tablets, um auf relevante Informationen, wie beispielsweise Wetterprognosen, zuzugreifen. Spezifischere Anwendungspotenziale eröffnet die Digitalisierung vor allem bei der datenbasierten Steuerung und fortschreitenden Automatisierung der landwirtschaftlichen Produktionsprozesse. Entsprechende Digitaltechnologien unterscheiden sich deutlich je nach Produktionsschwerpunkt und weisen folglich eine große Heterogenität auf. In der Tierhaltung werden hauptsächlich softwarebasierte Herdenmanagementsysteme, Sensortechnologien für die Einzeltierbeobachtung sowie Robotertechnologien zur Automatisierung des Melk-

1 BSI-Gesetz vom 14.8.2009, zuletzt am 23.6.2021 geändert

2 Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

vorgangs, der Fütterung und der Reinigung eingesetzt. In der Pflanzenproduktion sind Sensorsysteme bereits seit etlichen Jahren am Markt erhältlich. Eine vollständige Marktdurchdringung fand allerdings bisher nicht statt. Viele Farmmanagementsysteme sind auf dem Markt verfügbar, die meisten davon werden als cloudbasierte Plattformen angeboten. Drohnen und Feldroboter spielen derzeit noch keine große Rolle im Pflanzenbau, könnten zukünftig jedoch an Bedeutung gewinnen.

In der industriellen Nahrungsmittelverarbeitung gibt es einen starken Trend zum Einsatz digitaler Lösungen. Bei der Schlachtung und der Herstellung von Fleischprodukten, aber auch bei der Verarbeitung von Gemüse und Getreide sind die Prozesse vielfach hoch automatisiert und fließbandbasiert. Zahlreiche Prozesse werden durch Roboter gesteuert. Für das reibungslose Funktionieren der Verarbeitung von Nahrungsmitteln sind vor allem Warenwirtschafts- und industrielle Steuerungssysteme maßgeblich. Perspektivisch könnten informations- und softwaretechnische mit mechanischen Komponenten immer stärker verbunden werden, wobei Datentransfer und -austausch sowie Kontrolle bzw. Steuerung über eine Infrastruktur, wie das Internet, in Echtzeit erfolgen werden.

In der Logistik werden sensible Daten, wie Kundeninformationen, Bestellungen, Lieferungen und Zahlungen, verwaltet. Dafür sind Schnittstellen zu Kundensystemen, z. B. Auftrags-, Lieferavis-, Rechnungsschnittstellen, vorhanden, um eine nahtlose Kommunikation und Zusammenarbeit zwischen den Akteuren in der Lieferkette sicherzustellen. Digitale Lösungen bieten Unterstützung insbesondere bei der Verwaltung von Lagerbeständen und der Einhaltung von Hygiene- und Regulierungsstandards. Lösungen mithilfe von künstlicher Intelligenz (KI) werden zunehmend zur Optimierung von Lieferketten eingesetzt. Die Zunahme des Lebensmittelonlinehandels verstärkt den Trend zum Einsatz von Sensoren und Logistiksystemen. Auf Cloudlösungen wird in der Logistik zugegriffen, um den Datenaustausch zwischen Akteuren entlang der Lieferkette zu erleichtern. Virtual Reality (VR) und Augmented Reality (AR) sind in der Branche bereits weit verbreitet. Zu den weiteren Technologien, die perspektivisch eine Rolle in der Branche spielen könnten, gehören digitale Zwillinge zur virtuellen Nachbildung einer realen Lieferkette, Blockchaintechnologien, um Warenflüsse entlang der Lieferkette transparenter zu gestalten und eine verlässlichere Rückverfolgbarkeit der Lebensmittel zu gewährleisten, sowie Drohnen bei der Zustellung von Produkten zu den Endkunden und in der Lagerhaltung.

Auch im (Einzel-)Handel spielen zentrale Verwaltungssysteme, wie Warenwirtschaftssysteme, eine zentrale Rolle. Fallen solche zentralen Verwaltungssysteme aus, führt das zu größeren Störungen im Betrieb. Kernbestandteil des IT-Systems in Einzelhandelsfilialen sind digitale Kassensysteme – auch Point-of-Sale(POS)-Systeme genannt. Diese dienen der Abwicklung von Verkäufen und Transaktionen. Weitere Trends sind die Verknüpfung von Kassensystemen mit digitalen Preisschildern und die zunehmenden Bezahlmöglichkei-

ten via Smartphone bzw. Smartwatch. Von vielen deutschen Händlern ist die Einführung kassenloser Stores vorgesehen. Digitale Handelsplattformen können zwischen verschiedenen Stufen der Wertschöpfungskette eingesetzt werden. Die Grenze zwischen On- und Offlinehandel verschwimmt durch die Zunahme von kanalübergreifenden Geschäftsmodellen. Auch im Handel halten cloudbasierte Lösungen Einzug ebenso wie KI-Anwendungen.

Bedrohungslage

Auch wenn die offiziellen Meldungen den Anschein erwecken, dass der Ernährungssektor im Sektorenvergleich wenig von Cyberanfällen betroffen ist, zeigt die vorliegende Analyse ein alarmierendes Bild. Mehr als zwei Drittel der 2018/2019 befragten Unternehmen im Sektor Landwirtschaft und Ernährung und verbundenen Sektoren gaben an, bereits Opfer eines oder mehrerer Angriffe geworden zu sein. Die Analyse deutet darauf hin, dass die Nahrungsmittelindustrie, vor allem in den letzten Jahren, verstärkt in das Visier von Cyberkriminellen geraten ist.

Motive für Cyberangriffe sind vielfältig und lassen sich auf unterschiedliche Akteursgruppen zurückführen. Aktuell gilt die wirtschaftliche Bereicherung als das häufigste Motiv und die größte Gefahr für Unternehmen. Global agierende Unternehmen sehen sich außerdem zunehmend von Nationalstaaten mit geopolitischen Motiven bedroht. Zu den häufigsten und gefährlichsten Angriffsarten zählen insbesondere die Manipulation, Zerstörung oder Verschlüsselung von Daten mit der Aufforderung zur Zahlung eines Lösegelds (Ransomware) sowie die Vortäuschung der Identität einer Person mit dem Ziel, an vertrauliche Information zu gelangen oder eine Person zu einer Geldüberweisung zu bewegen (Phishing). Außerdem stellt das Absetzen massenhafter Anfragen auf ein System (Denial-of-Service[DoS]-Angriffe) besonders für Unternehmen, deren Kernleistung auf der Nutzung einer Internetplattform beruht, eine größere Herausforderung dar. Mit der Verbreitung von KI-gestützten Systemen entstehen auch neue Angriffsarten.

Die Anzahl der Angriffe auf den Sektor Landwirtschaft und Ernährung sowie die erpressten Geldsummen nahmen in den letzten Jahren zu. Es ist anzunehmen, dass die Dunkelziffer noch höher ist, als es die gemeldeten Fälle und Statistiken vermuten lassen. Von Cyberangriffen sind die Wertschöpfungsstufen unterschiedlich stark betroffen. Vor allem Angriffe auf Unternehmen der Nahrungsmittelverarbeitung sowie auf Logistik- und Handelsunternehmen führten in der Vergangenheit zu einer kurzzeitigen Nichtverfügbarkeit der entsprechenden Produkte. Es konnten allerdings kaum Cybersicherheitsvorfälle bei der Erzeugung von Lebensmitteln gefunden werden, die wirklich schwerwiegende Folgen für das operative Tagesgeschäft des Unternehmens oder sogar die Wertschöpfungskette, also die vor- und/oder nachgelagerten Unternehmen, nach sich zogen.

Durch die stetig zunehmende Digitalisierung, die Vernetzung von Systemen und ihre Verbindung mit dem Internet werden Unternehmen und Prozesse angreifbar, die früher beispielsweise durch die physische Trennung von IT- und Betriebstechnologien geschützt waren. So wird es leichter möglich, durch einen Angriff auf einen Hersteller von Betriebstechnik zahlreiche kleinere und mittlere Unternehmen anzugreifen. Im mehrheitlich dezentral organisierten Sektor Landwirtschaft und Ernährung sind gleichzeitige Angriffe auf eine Vielzahl von Unternehmen einer der möglichen Hauptwege, um die Versorgung mit Lebensmitteln bedeutsam zu stören. Dafür können Angreifer Hersteller von Betriebstechnik oder IT-Dienstleister ins Visier nehmen (Supply-Chain-Angriff), die mit zahlreichen der eigentlichen Zielunternehmen digital vernetzt sind. Außerdem wird es durch die Fortschritte im Bereich der KI leichter möglich, Angriffe zu planen und durchzuführen, die darauf abzielen, mehrere Akteure auf einmal in der Wertschöpfungskette auszuschalten. Längerfristig könnte nicht nur KI, sondern auch das Quantencomputing eine größere Herausforderung für die Cybersicherheit in Landwirtschaft und Ernährung darstellen.

Gefährdung der Versorgungssicherheit

Auf Basis einer umfangreichen Dokumentenanalyse, ergänzt um eine empirische Erhebung, untersuchten die im Projekt beauftragten Gutachter/innen Teuteberg und Anton (2023) sowie Hoffmann und Haas (2023), wie sich ein Ausfall von IT-Systemen auf die Produktion und die Verteilung von Lebensmitteln auswirken könnte und inwiefern ein solcher Ausfall eine Gefährdung für die Nahrungsmittelversorgung insgesamt darstellen könnte.

Landwirtschaft

Zu Angriffen auf landwirtschaftliche Betriebe ist vergleichsweise wenig bekannt. Dies liegt vermutlich daran, dass die Landwirtschaft bisher nicht das Hauptziel ausgeklügelter Angriffe auf die Betriebstechnologien war, wobei mehr als zwei Drittel der deutschen Landwirtschaftsbetriebe bis 2019 Opfer eines Cyberangriffs wurden. Die Gutachter gehen davon aus, dass tendenziell wenige Schutzvorkehrungen in IT-Netzwerken landwirtschaftlicher Betriebe vorhanden sind, weswegen Einfallstore existieren, die leicht ausgenutzt werden können. Allerdings führen Angriffe in der Regel nicht zu Lieferengpässen. Der Ausfall der Produktion bei einem Betrieb lässt sich meist leicht von Mitbewerbern abfedern. Eher ist davon auszugehen, dass landwirtschaftliche Betriebe von einem Angriff auf die Hersteller der von ihnen eingesetzten Betriebstechnik oder auf extern beauftragte Dienstleister mit starker Marktdurchdringung betroffen sein können.

In der Nutztierhaltung gilt das für IT-Dienstleister, wie Cloudhostingplattformen, die Speicherplatz, Rechenleistung und Datenbanken zur Verfügung stellen, sowie Anbieter cloudbasierter Systeme, wozu meist Farmmanagementsysteme gehören. Ähnlich problematisch kann sich der Ausfall von Internet- oder Labordienstleistungen auswirken. Neben indirekten Angriffen auf Dienstleister mit hohem Marktanteil können auch solche IT-Systeme direkt angegriffen werden, die standardgemäß in der Nutztierhaltung eingesetzt werden und eine hohe Kritikalität aufweisen. Dazu gehört insbesondere die Robotertechnologie. Besonders kritisch sind dabei Stallbelüftungs- und Bewässerungssysteme sowie automatische Melksysteme in Milchviehbetrieben.

Der Pflanzenbau ist aufgrund der geringeren Verderblichkeit der Produkte grundsätzlich von einer geringeren Kritikalität geprägt. Dennoch sind auch in der Pflanzenproduktion Supply-Chain-Angriffe mit einem relevanten Gefahrenpotenzial verbunden. Dazu gehören zum einen Angriffe auf Händler von Saatgut und Düngemittel während der Aussaat- und Pflanzsaison. Als wahrscheinlich werden zudem Angriffe auf die Flotten von Landtechnikherstellern bzw. auf Landmaschinen eingeschätzt. Die meisten modernen Maschinen verfügen über vernetzte Bordelektronik und sind in Telematiklösungen eingebunden. Vor allem skalierte Angriffe auf Landtechnikhersteller, wodurch Traktoren mit digitaler Steuerungstechnik fahrunfähig gemacht werden können, sind mit größeren Risiken verbunden. In zeitkritischen Prozessen wie der Ernte, wo ganze Landmaschinenflotten über wenige Wochen zeitgleich gebraucht werden, könnte sich ein solcher Angriff als hochproblematisch erweisen. Denn der optimale Erntezeitpunkt hängt von der Jahreszeit und der Witterung ab. Stehen die Erntemaschinen nicht rechtzeitig zur Verfügung, kann es zum Totalverlust für landwirtschaftliche Betriebe kommen.

Verarbeitung

Im Vergleich zu einem Ausfall der Technik in der Landwirtschaft kann ein Ausfall der Technik bei der Verarbeitung von Lebensmitteln schneller weitreichende Auswirkungen haben. Grund dafür ist, dass viele kritische Prozesse der Verarbeitung von einer hohen Abhängigkeit von IT-Systemen – zunehmend auch von einem Internetzugang – geprägt sind. Ohne Zugang zu den zentralen Systemen und dabei besonders zum Warenwirtschaftssystem können die erforderlichen Dienste schnell nicht mehr erbracht werden. Ob sich Produktionsausfälle auf die Ernährungssicherheit auswirken, hängt insbesondere auch von der Verderblichkeit der betroffenen Produkte und der Anzahl der versorgten Personen ab. Besonders bedrohlich für die Versorgungssicherheit sind Angriffe auf Unternehmen, die als zentrale Anlaufpunkte für Produkte (z. B. eine Molkerei, die die Milch zahlreicher Milcherzeuger sammelt) fungieren. Starke Marktkonzentrationen geben Hinweise auf mögliche Schwachstellen.

Logistik

Angriffe auf IT-Systeme zur Unterstützung von Logistikprozessen werden als besonders schwerwiegend eingestuft. Denn die Logistik stellt unter Umständen einen neuralgischen Punkt in der Versorgungskette dar. Beeinträchtigungen der Logistiksysteme können zu Störungen im Transport- und Abfertigungsprozess führen, die wiederum Lieferengpässe und eine Beeinträchtigung der Produktverfügbarkeit zur Folge haben können. Kritisch ist vor allem ein Ausfall zentraler Verwaltungssysteme, wie Warenwirtschafts- oder Lagerverwaltungssysteme, wodurch z. B. keine Aufträge im Logistiklager mehr abgearbeitet werden können. Besonders Internet-of-Things(IoT)-Anwendungen und Cloudcomputing erhöhen den Vernetzungsgrad von Anlagen. Künftig könnten auch digitale Zwillinge, VR- und AR-Anwendungen sowie Drohnen den Vernetzungsgrad erhöhen. Auch die Vernetzung von Systemen zwischen Handelspartnern entlang der Wertschöpfungskette birgt neue Risiken für Logistikunternehmen, denn Vorfälle durch schwache Cybersicherheitsmaßnahmen bei einem Lieferanten können sich schneller als in der Vergangenheit auf Partner in der Lieferkette ausbreiten. Der wachsende Zugriff auf Clouddienste für die Speicherung von Daten zwischen Handelspartnern wird in dieser Hinsicht als besonders problematisch angesehen. Auch blockchainbasierte Systeme werden zunehmend zu attraktiven Zielen für Cyberkriminelle. Dass Störungen weitreichende Konsequenzen haben können, liegt auch daran, dass viele Logistikprozesse so synchronisiert werden, dass Waren in der exakten Menge und zum richtigen Zeitpunkt an den richtigen Ort gelangen, um den Produktionsprozess ohne Verzögerungen oder Überbestände aufrechtzuerhalten. Störungen können entsprechend nur schwer abgefedert werden. Eine hohe Eintrittswahrscheinlichkeit und potenziell große Auswirkungen haben zudem Angriffe auf Kühlungssysteme (Kühltransporter und -häuser), da die Produkte schnell verderben würden. Einfallstore könnten z. B. die Telemetrie (Telematiksysteme) in Kühl-LKWs oder die Fernwartung von Kühlhäusern sein.

Handel

Neben der Logistik ist der Einzelhandel aufgrund der umfangreichen Verarbeitung sensibler Kunden- und Geschäftsdaten ein attraktives Ziel für Cyberkriminelle. Ransomware stellt auch im Handel die größte Bedrohung dar, insbesondere durch den Angriffsvektor des Phishings, wodurch Datenschutzverletzungen entstehen können. In der Regel bleibt die Verfügbarkeit der Kerndienstleistung von Datenschutzverletzungen unberührt. Unter den Angriffen, die auf IT-Systeme des Handels stattfinden können, stellen Attacken auf zentrale Verwaltungssysteme (z. B. Warenwirtschaftssysteme), aber auch auf digitale Kassensysteme aktuell die größte Gefahr für den Einzelhandel dar. Entsprechende Vorfälle können prinzipiell den Zugang zu Lebensmitteln erschweren. Bisher konn-

ten die Folgen einzelner Störungen durch die Dichte des Supermarktnetzes in Deutschland zwar abgefedert werden, allerdings besteht durch die starke Konzentration des Handels von Lebensmitteln in Deutschland die Gefahr einer Homogenisierung der eingesetzten Systeme, wodurch skalierte Angriffe über Softwareaktualisierungen gefährlich werden könnten. Noch problematischer kann sich ein indirekter Angriff auf einen externen IT-Dienstleister erweisen, wenn die Mehrheit der Einzelhandelsfilialen auf die gleiche Dienstleistung zugreift. Neben Dienstleistungen zur Überwachung und Steuerung von IT-Netzwerken oder Software für Kartenzahlungsterminals könnte auch die wachsende Nutzung von cloudbasierten Anwendungen, die durch die Verbindung mit dem Internet neue Angriffsfläche für Hackerangriffe bieten, zu einer erhöhten Verletzlichkeit führen.

Wo Webserver im Spiel sind, stellen Angriffe von Cyberkriminellen meist eine große Gefahr dar. Das betrifft vor allem Unternehmen, deren Kerngeschäft im Onlinehandel liegt und für die der Ausfall der Server eine Bedrohung für die Verfügbarkeit der Kernleistungen mit sich bringt. Trotz der verheerenden Auswirkungen auf die einzelnen Betriebe ist ein Ausfall des Onlinegeschäfts in der Regel kein gravierendes Problem für die Versorgungssicherheit insgesamt, denn der Onlinehandel hat bisher nur einen relativ kleinen Marktanteil und stellt für die meisten Lebensmitteleinzelhändler nicht den primären Vertriebskanal dar.

Handlungsoptionen

Kritische Dienstleistungen sind für das Funktionieren unserer Gesellschaft von essenzieller Bedeutung, weswegen sie einem hohen Schutz unterliegen sollen. Allerdings können Sicherheitsmaßnahmen hohe Kosten verursachen. Deswegen gilt es abzuwägen, wo die größten Bedrohungen bestehen, um Anhaltspunkte für angemessene Vorkehrungen zu identifizieren, die zugleich einen ausreichenden Schutz sicherstellen. Um die Lebensmittelversorgung zu sichern, muss u. a. die Versorgung mit Energie bzw. Strom, mit Wasser für den Anbau von Pflanzen und für die Tierhaltung sowie mit einer funktionierenden Infrastruktur der Informations- und Kommunikationstechnik (IKT) gewährleistet sein. Darüber hinaus kann ein Angriff auf IT-Systeme insbesondere dann weitreichende Auswirkungen haben, wenn:

- das IT-System standardgemäß in sehr vielen Betrieben oder zur Erbringung einer extern beauftragten Dienstleistung eingesetzt wird;
- das IT-System oder die Dienstleistung eine hohe Kritikalität aufweist, also eine zentrale und kaum ersetzbare Funktion im Betrieb übernimmt;
- das System nur von wenigen Herstellern angeboten wird;
- das System die Verderblichkeit der Waren beeinflusst.

Die hohe Vielfalt der Produkte und Unternehmen im Ernährungssektor sorgt dafür, dass der Ausfall eines Anbieters bzw. eines Betriebes in den meisten Fällen keine gravierenden Folgen für die Versorgung der Bevölkerung hat. Daher wurden bislang in diesem Sektor vor allem Betreiber größerer kritischer Anlagen ab einem gesetzlich definierten Schwellenwert dazu verpflichtet, ihre IT-Systeme und Netzwerke gegenüber Cyberangriffen zu schützen. Vor dem Hintergrund wachsender Gefahren durch die Vernetzung und Integration von Systemen und Daten sowohl innerhalb einzelner Betriebe als auch entlang der Wertschöpfungskette sowie der Möglichkeiten, Angriffe auf zahlreiche kleinere Betreiber bzw. durch Supply-Chain-Angriffe mittels KI leichter durchzuführen, sind eine Absenkung der Schwellenwerte und ein stärkerer Fokus auf Lieferketten sinnvoll. 2022 wurde die NIS-2-Richtlinie veröffentlicht. Durch das Umsetzungsgesetz in Deutschland (derzeit im Gesetzgebungsverfahren) wird die Cybersicherheit des Sektors erhöht. Insgesamt erfordert eine höhere Cybersicherheit der Lebensmittelversorgung, externe Dienstanbieter und Anbieter kritischer IT-Technik stärker in die Pflicht zu nehmen, kleine Betreiber zu mehr Cybersicherheit zu bewegen sowie das Wissen zum Grad der Verbreitung von IT-Systemen, zu Störfällen und Schutzniveaus in der Branche sowie zu Risiken durch neue Technologien zu verbessern. Außerdem erscheinen Maßnahmen zur Reduzierung des IT-Fachkräftemangels, zur Erhöhung von Effizienz und Effektivität in den Sicherheits- und Strafverfolgungsbehörden sowie zur Stärkung des Bewusstseins für Cyberrisiken als besonders wichtig.

1 Einleitung

Nicht zuletzt im Kontext des Krieges in der Ukraine befassen sich Entscheidungsträger/innen europaweit mit der Sicherheit der Nahrungsmittelversorgung. Im Vordergrund stehen die Importabhängigkeit bei bestimmten Produkten und Vorleistungen (z. B. Dünger) sowie die steigenden Betriebsmittelkosten und Lebensmittelpreise. Mit der Digitalisierung und Vernetzung technischer Systeme steigt zudem die Verwundbarkeit von Unternehmen in der Nahrungsmittelkette gegenüber Bedrohungen aus dem Cyberraum. Die Bedrohungslage bei der IT-Sicherheit war 2023 höher als je zuvor (BSI 2023), wobei Cyberkriminalität eine besonders große Gefahr darstellt.

Einige Vorfälle zeigen die Verwundbarkeit des Ernährungssektors: 2021 legte ein Angriff auf die Betriebstechnologie des brasilianischen Fleischverarbeiters JBS S.A. dessen gesamte nordamerikanische und australische Fleischproduktion lahm. Im Mai 2023 musste der US-amerikanische Landtechnikkonzern AGCO infolge eines Ransomwareangriffs die Arbeit in seinen Produktionsanlagen einstellen. Diese Beispiele sind nur zwei von inzwischen vielen, die verdeutlichen, dass digitale Technologien in der Lebensmittelversorgung von Cyberstraftaten nicht verschont bleiben.

Cyberangriffe auf Unternehmen in der Nahrungsmittelkette könnten gravierende Auswirkungen für die Bevölkerung haben. Folgerichtig gehört der Sektor Ernährung (Lebensmittelproduktion, -verarbeitung und -handel) zu den kritischen Infrastrukturen, die es besonders zu schützen gilt. Im Hinblick auf die Informationssicherheit erfolgt dies durch das BSI-Gesetz, nach welchem große Unternehmen im Ernährungssektor verpflichtet sind, ihre IT-Systeme nach aktuellem Stand der Technik abzusichern. Allerdings sind vor allem die Landwirtschaft und das Lebensmittelhandwerk stark von kleinen und mittleren Unternehmen geprägt, für die die Verpflichtungen des BSI-Gesetzes bisher nicht galten. Dies ist besorgniserregend, denn laut BSI (2023, S. 11) werden kleine und mittlere Unternehmen überproportional häufig angegriffen. Mit der 2022 veröffentlichten NIS-2-Richtlinie wird zum einen der Ernährungssektor als wichtiger Sektor auch auf europäischer Ebene anerkannt. Zum anderen werden mit der Richtlinie nicht mehr nur große Betreiber, sondern auch mittlere Unternehmen in die Pflicht genommen, ihre Systeme gegen IT-Sicherheitsvorfälle abzusichern.

Zwar wurde die Vulnerabilität des Ernährungssystems in den letzten Jahren intensiv erforscht, allerdings lag der Schwerpunkt der meisten Studien auf den Folgen der COVID-19-Pandemie und den Anpassungen an den Klimawandel. Die Vulnerabilität und die Resilienz gegenüber IT-Störungen bzw. Cyberangriffen wurden vergleichsweise weniger betrachtet.

Ziel und Struktur des Berichts

Ziel ist es, die Vulnerabilitäten der Nahrungsmittelversorgung in Deutschland vor dem Hintergrund möglicher Bedrohungen aus dem Cyberraum näher zu beleuchten. Dabei wird die Bedrohungslage für den Ernährungssektor vor dem Hintergrund des aktuellen und perspektivischen Digitalisierungsgrads analysiert und es wird erörtert, inwiefern die Digitalisierung von Produktion, Logistik und Handel von Nahrungsmitteln in Deutschland zu einer erhöhten Anfälligkeit für Störungen führen kann bzw. bereits führte. Es werden mögliche Schwachstellen entlang der Herstellungs- und Lieferketten identifiziert sowie die Frage erörtert, inwieweit gezielte Angriffe das Potenzial haben, die Nahrungsmittelversorgung zu gefährden. Anhand der Erkenntnisse aus dieser Vulnerabilitätsanalyse wurden abschließend Ansatzpunkte für eine Stärkung der Resilienz des Ernährungssektors abgeleitet. Cyberangriffe auf IT-Systeme von Betrieben, die leicht verderbliche Waren produzieren, bzw. Produktionsausfälle stellen eine besondere Herausforderung dar, weswegen der Fokus auf die Milchwirtschaft liegt.

Auch wenn Cyberangriffe für einzelne Betriebe verheerende Auswirkungen haben können (z. B. Reputationsschäden, wirtschaftliche Verluste) oder zu Verletzungen des Datenschutzes führen können, werden diese Auswirkungen im vorliegenden Bericht nicht näher untersucht, sondern darauf fokussiert, welche Angriffstypen und Szenarien zu Beeinträchtigungen bei der Produktion oder Verteilung von Lebensmitteln führen können und die Versorgung der Bevölkerung mit Nahrungsmitteln beeinträchtigen könnte. Zunächst wird der Stand der Digitalisierung in Landwirtschaft und Ernährungsindustrie skizziert (Kap. 2). Danach wird die aktuelle Bedrohungslage beschrieben (Kap. 3). Auf dieser Grundlage werden die Ergebnisse aus beiden Gutachten zusammengefasst und die Gefährdung von Cyberangriffen für die Versorgungssicherheit bewertet (Kap. 4). Aus der Analyse werden abschließend Handlungsoptionen für den Gesetzgeber abgeleitet (Kap. 5).

Zusammenarbeit mit Gutachter/innen und Danksagung

Zur fachlichen Fundierung dieses Berichts wurden zwei Gutachten vergeben:

- Cybersicherheit im Bereich Nahrungsmittelverarbeitung- und -handel sowie Kühllogistik von Milch und Milchprodukten: Vulnerabilitätsanalyse und Handlungsfelder zur Stärkung der Resilienz. Prof. Dr. Frank Teuteberg, Dr. Eduard Anton; synovacom GmbH, Osnabrück
- Cybersicherheit in der Nahrungsmittelversorgung (Schwerpunkt Landwirtschaft) – Identifizierung von Risikoelementen, hypothetische Angriffsszenarien und Auswirkungen auf die Ernährungsversorgung. Dr. Christa Hoffmann, Prof. Dr. Roland Haas; oeconos GmbH, Dettingen

Die Verantwortung für die Auswahl, Strukturierung und Interpretation der Gutachtenergebnisse liegt bei der Autorin, Dr. Pauline Riousset, des vorliegenden Berichts. An dieser Stelle sei den Gutachter/innen für die Bereitschaft zur Kooperation und Kommunikation herzlich gedankt. Dank gebührt ebenfalls Dr. Arnold Sauter und Dr. Christoph Kehl für Durchsicht und Kommentierung von Entwurfsversionen sowie Carmen Dienhardt und Brigitta-Ulrike Goelsdorf für die Bearbeitung der Abbildungen, die redaktionelle Bearbeitung des Manuskripts und die Erstellung des Layouts.

2 IT-Systeme in Landwirtschaft und Ernährungsindustrie

Die Digitalisierung prägt aktuell alle Stufen der Ernährungsversorgung – von der landwirtschaftlichen Erzeugung von Nahrungsmitteln bis hin zum Einzelhandel. In der Landwirtschaft werden sowohl digitale Einzeltechnologien als auch intelligent vernetzte und miteinander kommunizierende Technologiesysteme eingesetzt (TAB 2021). Auch in der Ernährungsindustrie, also Nahrungsmittelverarbeitung, Logistik und Handel, spielt die Digitalisierung eine zunehmend wichtige Rolle. Die überwiegende Mehrheit der Unternehmen assoziiert mit Digitalisierung und Automatisierung zahlreiche Chancen, so eine Umfrage von Bitkom und der BVE (Rohleder/Minhoff 2019). Erwartet werden eine erhöhte Prozesseffizienz, Echtzeitdaten für Entscheidungen, bessere Kundenkenntnisse, neue Kundenzugänge, eine Rückverfolgbarkeit der Produkte und eine bessere Kommunikation zwischen Akteuren der Wertschöpfungskette (Rohleder/Minhoff 2019, S. 3).

Im Folgenden wird ein Überblick über IT-Systeme und Digitalisierungstrends gegeben, die sich bei einem Ausfall auf die Kernprozesse in jeder Wertschöpfungsstufe auswirken und die Sicherheit der Lebensmittelversorgung gefährden könnten.

2.1 Landwirtschaft

Landwirt/innen nutzen, wie andere Berufsgruppen auch, im beruflichen Alltag inzwischen verbreitet mobile Endgeräte, wie Smartphones und Tablets, um auf relevante Informationen, wie beispielsweise Wetterprognosen, zuzugreifen; Computer und handelsübliche Bürosoftware sind in Betrieben ebenfalls Standard. Spezifischere Anwendungspotenziale eröffnet die Digitalisierung bei der datenbasierten Steuerung und fortschreitenden Automatisierung der landwirtschaftlichen Produktionsprozesse. Entsprechende Digitaltechnologien differieren je nach Produktionsschwerpunkt und weisen folglich eine große Heterogenität auf. Von übergreifender Bedeutung sind vor allem Entwicklungen in den Bereichen Sensoren, Landmaschinen, Drohnen und Roboter sowie bei plattformbasierten Managementsystemen, die zunehmend vernetzt sind und Daten aus unterschiedlichen Quellen integrieren. Eine ausführliche Befassung mit dem Stand und den Perspektiven der Digitalisierung in der Landwirtschaft findet sich im TAB-Arbeitsbericht Nr. 193 (TAB 2021). Im Folgenden wird ein kurzer Überblick über die wichtigsten Anwendungsfelder differenziert nach Nutztierhaltung und Pflanzenbau gegeben.

Digitalisierung und Automatisierung in der Nutztierhaltung

In der Tierhaltung haben Themen wie Mechanisierung, Automatisierung und Digitalisierung aufgrund der steigenden Zahl von Tieren pro Betrieb und des Rückgangs an verfügbarer Arbeitskraft stark an Bedeutung gewonnen (Pöllinger-Zierler et al. 2021, S. 10 f.). Zur Bestandsführung und Dokumentation sowie effizienten Verwaltung der landwirtschaftlichen Nutztiere kommen zunehmend softwarebasierte Herdenmanagementsysteme zum Einsatz (dazu und zum Folgenden Teuteberg/Anton 2023, S. 38 ff.). Typische Herdenmanagementaufgaben umfassen Überwachung und Management von Tierverhalten und -gesundheit, Fruchtbarkeitsmanagement, Fütterungssteuerung und -kontrolle sowie Leistungserfassung (TAB 2021, S. 40). Eine Vielzahl an Systemen steht bereits auf dem Markt zur Verfügung – von Insellösungen zur Unterstützung einzelner Herdenmanagementaufgaben bis hin zu integrierten Lösungen mit breitem Funktionsspektrum (Büscher et al. 2021).

Grundlage für das datenbasierte Herdenmanagement bilden *Sensortechnologien* für die Einzeltierbeobachtung. Mittels unterschiedlicher Sensoren, die am Tier befestigt oder in es eingebracht werden, können Daten zu physiologischen Parametern (z. B. Körpertemperatur, pH-Wert im Pansen) sowie zum Verhalten und der Position des Tieres erfasst werden. Die Art der dabei eingesetzten Sensoren unterscheidet sich zwischen Milchvieh-, Schweine- und Geflügelhaltung. Die Sensordaten werden meist per Radiofrequenztechnologie an eine Funkstation und anschließend an einen zentralen Rechner weitergeleitet, wo die Datenauswertung und -aufbereitung mit entsprechenden Algorithmen erfolgt (TAB 2021, S. 41). Auch für das Stallmanagement kommen Sensoren zur Steuerung der Belüftung, des Stallklimas oder der Trinkwassertemperatur zum Einsatz.

Sensoren und *innovative Datenanalyse* können schon heute Tierhaltungsbetriebe bei der Beurteilung des Wohlergehens von Tieren unterstützen. Die Anwendungsfälle konzentrieren sich dabei zumeist auf die Gesundheit, das Verhalten und die Fütterung der Tiere (Monteiro et al. 2021; Stygar et al. 2021). Perspektivisch könnten Sensordaten und algorithmenbasierte Analysesysteme noch viel stärker kombiniert werden, um bei der Bewirtschaftung von Viehbeständen unterschiedliche Parameter in Bezug auf Zucht, Gesundheit und Wohlergehen tierindividuell mit hoher Präzision zu messen. Dabei wird von Precision Livestock Farming gesprochen (Monteiro et al. 2021). Zu erwarten ist, dass sich KI-basierte Anwendungen, z. B. zur Verhaltenserkennung oder Tierzählung, die sich derzeit noch weitgehend im Versuchsstadium befinden, zunehmend verbreiten.

Robotertechnologien sind vor allem in größeren Tierhaltungsbetrieben schon recht weit verbreitet und werden zur Automatisierung von körperlich anstrengenden Arbeitsroutinen wie Melken, Fütterung oder Reinigung eingesetzt.

Gebräuchliche Anwendungen sind auf die Stallwirtschaft beschränkt und umfassen automatische Melksysteme, *automatische Fütterungssysteme* sowie *Reinigungsroboter* (TAB 2021, S. 91 ff.). Automatische Fütterungssysteme, die der Automatisierung des Fütterungsprozesses dienen, werden hauptsächlich in der intensiven Schweine- und Geflügelhaltung eingesetzt, zunehmend aber auch in der Milchviehhaltung (TAB 2021, S. 96). In der Geflügelproduktion ist außerdem das Ausbrüten bereits weitestgehend automatisiert (Hoffmann/Haas 2023, S. 25). In der Milcherzeugung spielen automatische Melksysteme (AMS), die ein vollautomatisiertes Melken des Tierbestands ermöglichen (von der Zitzenreinigung über das Vormelken und das Melken bis hin zur Kontrolle des Ausmelkgrads), inzwischen eine wichtige Rolle (zum Vergleich Kasten 2.1) – die Mehrheit aller neu installierten Melkanlagen ist den AMS zuzurechnen. Melk- und Fütterungssysteme enthalten verschiedene Sensoren, über die Daten etwa zur Kontrolle der Milchmenge und -qualität oder zur Futteraufnahme des Tieres erhoben und an das Herdenmanagementsystem übermittelt werden.

Kasten 2.1 Verbreitung von automatischen Melk- und Fütterungssystemen in Deutschland

2022 waren laut einer Umfrage des Branchenverbandes Bitkom (Rohleder/Meinel 2022) auf 19 % der landwirtschaftlichen Betriebe ein Melk- oder Stallroboter, auf 24 % der Betriebe ein Fütterungssystem im Einsatz. Weitere 26 bzw. 16 % der Betriebe gaben an, den zukünftigen Einsatz solcher Systeme zu planen. Aufgrund der Spezialisierung dieser Maschinen gibt es auch nur wenige zentrale Anbieter, die einen hohen Marktanteil besitzen (DLG e. V. 2023; LVN 2020).

Nicht nur die einzelnen Stufen der Wertschöpfungskette werden digitalisiert. Auch zwischen den einzelnen Wertschöpfungsstufen werden zunehmend Informationsschnittstellen geschaffen und mit IT-Lösungen geschlossen. So ermöglichen *integrierte Softwarelösungen* in der Fleischproduktion die Herkunftsrückverfolgbarkeit der Produkte von der Viehvermarktung bis zur Ladentheke.[3]

Digitalisierung und Automatisierung im Pflanzenbau

Auch in der Pflanzenproduktion ist ein klarer Trend zur Digitalisierung erkennbar (TAB 2021; dazu und zum Folgenden Hoffmann/Haas 2023, S. 23 ff.). *Sensorsysteme* werden eingesetzt, um die Wachstumsbedingungen für Pflanzen zu optimieren und Erträge zu sichern bzw. zu steigern. Anwendungsbereiche mit besonderer Relevanz sind Boden-, Stickstoff-, Unkraut- sowie Erntesensoren,

3 https://web.ftrace.com/ (28.5.2024)

die eine differenzierte, flächenbezogene Erhebung diverser Daten zu Bodeneigenschaften, zum Stickstoffbedarf des Pflanzenbestandes, zum Unkrautvorkommen oder zur Erntemenge bzw. -qualität ermöglichen. Entsprechende Daten bilden die Grundlage für eine teilflächenspezifische (und damit effizientere) Bewirtschaftung. Viele dieser Sensorsysteme sind bereits seit etlichen Jahren am Markt erhältlich, eine vollständige Marktdurchdringung hat allerdings bisher nicht stattgefunden (Spohrer 2023). Laut einer Umfrage setzten 2022 23 % der Landwirt/innen digitale Anwendungen für die teilflächenspezifische Ausbringung von Pflanzenschutzmitteln und 30 % für die teilflächenspezifische Anwendung von Düngemitteln ein (Rohleder/Meinel 2022).

Bei der Verarbeitung der erhobenen Sensordaten ist zwischen On- und Offlineverfahren zu unterscheiden. Bei Offlineverfahren finden Datenerhebung und Datenanalyse zeitlich getrennt statt, während bei Onlineverfahren die Daten in Echtzeit analysiert und direkt zur Steuerung von Bewirtschaftungsmaßnahmen eingesetzt werden (TAB 2021, S. 26 f.). Onlinesensorsysteme sind häufig integraler Bestandteil von *Landmaschinen*, um Prozesse wie Bodenbearbeitung, Aussaat, das Ausbringen von Pflanzenschutzmitteln oder von Dünger datenbasiert zu optimieren. Neue Landmaschinen, die über einen eigenen Antrieb verfügen, sind inzwischen standardmäßig mit automatischen Spurführungssystemen und satellitengestützter Navigation ausgestattet (TAB 2021, S. 58). Zudem kommen Telemetrie- oder Telematiksysteme zum Einsatz, die die Echtzeitüberwachung unterschiedlicher Betriebsparameter (z. B. Position, Prozessdaten) per Mobilfunk sowie zudem den Fernzugang zu den Maschinen ermöglichen. Es ist davon auszugehen, dass der Trend zur Automatisierung von Landmaschinen und ihrer Funktionen weiter anhält. Aktuelle Entwicklungen gehen in Richtung eines vollautonomen Betriebs (TAB 2021, S. 69).

Technologien, die derzeit noch keine große Rolle im Pflanzanbau spielen, zukünftig jedoch an Bedeutung gewinnen könnten, sind Drohnen und Feldroboter. *Drohnen* sind prinzipiell als Trägerplattform für den Einsatz von diversen Sensorsystemen gut geeignet und können etwa für das Bestandsmonitoring, die Rehkitzortung sowie die Schädlings- und Unkrautbekämpfung eingesetzt werden. Da die Analyse der generierten Bilddaten sehr komplex ist, werden landwirtschaftliche *Drohnendienstleistungen* derzeit allerdings hauptsächlich von darauf spezialisierten Firmen angeboten (TAB 2021, S. 88 f.). Kleine autonome *Feldroboter* könnten perspektivisch diverse Aufgaben wie Bodenbearbeitung, Aussaat oder Unkrautjäten übernehmen. Erste praxistaugliche Prototypen stehen zur Verfügung (z.B. Feldroboter »Dino«; Forum Moderne Landwirtschaft o. J.), geforscht wird u. a. an schwarmbasierten Einsatzkonzepten. Noch ist die Anwendung von Robotik im Pflanzenbau allerdings in einem frühen Entwicklungsstadium und in der Praxis auf Spezialbereiche wie den Gemüseanbau beschränkt.

Das Pendant zu den Herdenmanagementsystemen sind im Pflanzenbau die *Farmmanagementsysteme*. Dabei handelt es sich spezifisch auf Anwendungs-

zwecke im Pflanzenbau zugeschnittene Softwarelösungen, die Verwaltung und Analyse diverser Betriebsdaten ermöglichen und für die Prozessplanung und -steuerung verwendet werden können (TAB 2021, S. 77 ff.). Dazu werden in der Regel Daten aus weiteren externen Quellen (z. B. Wetter-, Markt- oder Satellitendaten) eingebunden. Inzwischen sind viele *Farmmanagementsysteme* auf dem Markt verfügbar. Die meisten davon werden als *cloudbasierte Plattformen* angeboten. Beispiele dafür sind XARVIO[4] oder Farm Facts[5].

2.2 Nahrungsmittelverarbeitung

In der industriellen Nahrungsmittelverarbeitung gibt es einen starken Trend zum Einsatz digitaler Lösungen. Bei der Schlachtung und der Herstellung von Fleischprodukten, aber auch bei der Verarbeitung von Gemüse und Getreide sind die Prozesse vielfach hoch automatisiert und fließbandbasiert. Zahlreiche Prozesse werden durch Roboter gesteuert, beispielsweise die Portionierung (Hoffmann/Haas 2023, S. 22). Für das reibungslose Funktionieren der Verarbeitung von Nahrungsmitteln sind vor allem Warenwirtschafts- und industrielle Steuerungssysteme maßgeblich.

Warenwirtschafts- bzw. Enterprise-Resource-Planning(ERP)-Systeme sind Softwaresysteme, die einem Unternehmen dabei helfen, zentrale betriebliche Prozesse zu steuern. Warenwirtschaftssysteme sind darauf ausgerichtet, alle Unternehmensprozesse in den Bereichen Finanzen, Personalwesen, Fertigung, Lieferkette, Dienstleistungen, Beschaffung zu integrieren (SAP SE o. J.). In der Verarbeitungsindustrie ermöglichen es Warenwirtschaftssysteme, Produktchargen zurückzuverfolgen und Qualitätsstandards und gesetzliche Vorschriften einzuhalten und zu dokumentieren. Sie unterstützen die Verwaltung von Lagerbeständen und die Kontrolle über den Verfall von Produkten, außerdem die Planung von Produktionsaufträgen und der effizienten Zuweisung von Ressourcen, wie Maschinen, Arbeitskräften und Rohstoffen. Warenwirtschaftssysteme sind inzwischen an spezieller Automatisierungs- und Prozessleittechnik (Prozess-IT) gekoppelt, die auf die Verarbeitung von Nahrungsmitteln zugeschnitten ist.

Industrielle Steuerungssysteme (Industrial Control Systems – ICS) sind das Herzstück der IT-gestützten Produktionsprozesse bzw. operativen Technologien (Prozess-IT[6]) und werden in der verarbeitenden Industrie zur Überwachung und Steuerung von Abläufen und Anlagen eingesetzt, so auch in der Milchverarbeitung (Kantale et al. 2022; Yaseen et al. 2022). Mit ICS können beispielsweise bei der Milchannahme Temperatur und pH-Wert mithilfe von Sensoren gemessen und so sichergestellt werden, dass nur qualitativ hochwertige Milch in die Produktion aufgenommen wird. Menge und Durchflussrate des

4 https://www.xarvio.com/de/de/de-lp.html (28.5.2024)
5 https://www.farmfacts.de/ (28.5.2024)
6 Gebräuchlich ist auch der Begriff Operational Technology (OT).

Rahms können außerdem über Ventile und Pumpen in Echtzeit gemessen und so Pasteurisierungs- und Rekonstitutionsprozesse gesteuert werden (Teuteberg/Anton 2023, S. 50). Fernwartungszugänge zu den Herstellern der eingebauten Maschinen oder Anlagen sind an vielen Stellen der Produktionsprozesse vorhanden (Hoffmann/Haas 2023, S. 23).

Perspektivisch könnten sich cyberphysische Systeme (CPS) verbreiten. Der Begriff CPS beschreibt »Systeme, bei denen informations- und softwaretechnische mit mechanischen Komponenten verbunden sind, wobei Datentransfer und -austausch sowie Kontrolle bzw. Steuerung über eine Infrastruktur wie das Internet in Echtzeit erfolgen« (Bendel 2024). CPS gehen in Integration und Automatisierung über herkömmliche ICS hinaus, denn sie beschreiben eine Vision der Vollintegration aller physischer Komponenten im System und die Verbindung mit fortschrittlichen Computertechnologien, um ein autonomes prädiktives Management, Selbstdiagnose- bzw. Wartungsmechanismen zur Risikovermeidung und eine kollaborative Produktionsplanung zur Leistungssteigerung bieten zu können (Gehlot et al. 2022, S. 11 ff.; Smetana et al. 2021, S. 92 ff.). In der Milchverarbeitung könnten CPS die Qualitätskontrolle unterstützen, indem Sensordaten von der Produktionslinie, Ergebnisse von Labortests und historische Daten zusammengeführt und analysiert werden, um Muster und Anomalien zu erkennen, die auf Qualitätsprobleme hinweisen könnten. Anhand dieser Daten können dann Entscheidungen über Prozessanpassungen getroffen werden, z. B. eine Änderung der Temperatur oder des pH-Werts der Milch während der Verarbeitung, um eine gleichbleibende Produktqualität zu gewährleisten. Auch eine Integration mit dem Kundenfeedbacksystem ist vorstellbar, um die Daten zur Kundenzufriedenheit möglichst schnell in die Analyse einfließen zu lassen (Smetana et al. 2021, S. 99).

2.3 Logistik

Die Logistik agiert als Bindeglied zwischen den Akteuren entlang der Wertschöpfungskette. Sie bedient nicht nur traditionelle Verkaufsstellen wie Supermärkte, sondern auch das Gastgewerbe und die Gemeinschaftsverpflegung. Logistikunternehmen verwalten sensible Daten wie Kundeninformationen, Bestellungen, Lieferungen und Zahlungen. Es werden Schnittstellen zu Kundensystemen (z. B. Auftrags-, Lieferavis-, Rechnungsschnittstellen) genutzt, um eine nahtlose Kommunikation und Zusammenarbeit zwischen den Akteuren in der Lieferkette sicherzustellen (Teuteberg/Anton 2023, S. VII). Die Verteilung (verderblicher) Waren erfordert spezialisierte Logistiknetze, die dafür sorgen, dass strenge Hygiene- und Regulierungsstandards eingehalten werden. Um diese Anforderungen zu erfüllen, bieten digitale Lösungen, wie Lagerverwaltungssysteme, Internet of Thinks etc., Unterstützung.

Lagerverwaltungssysteme (Warehouse-Management Systems – WMS) unterstützen Logistikunternehmen bei der Verwaltung von Lagerbeständen, der Planung der Lagerbewegungen und der Überwachung aller Lageraktivitäten vom Wareneingang über den Versand bis zur Rücksendung. Sie können mit einem Warenwirtschaftssystem verknüpft werden (Tropé 2022). WMS unterstützen auch die Verwaltung von Mindesthaltbarkeitsdaten, die Chargenrückverfolgbarkeit und die Kontrolle von allergenen Produkten. WMS werden von 59 % der Logistikfirmen in Deutschland eingesetzt – so eine repräsentative Umfrage mit 404 Logistikunternehmen in Deutschland mit 20 oder mehr Mitarbeitern (Bitkom 2022). Bereits ein Fünftel der Logistikunternehmen in Deutschland setzt KI ein (Bitkom 2022), u. a. in Verbindung mit WMS. Die Sammlung und Auswertung von großen Datenmengen mit Technologien wie KI können dazu beitragen, die Steuerung der Lieferkette zu optimieren, die Kosten zu senken und die Durchlaufzeiten zu verbessern (QTRADO Logistics GmbH & Co. KG 2023; Remondino/Zanin 2022, S. 11 f.). Müssen Waren neu bestellt werden, findet die Kommissionierung vermehrt automatisch oder durch sprachgesteuerte Systeme statt (Hoffmann/Haas 2023, S. 22; Teuteberg/Anton 2023, S. 62).
Internet of Things (IoT): Durch den Einsatz von IoT-Anwendungen, wie Sensoren in Lagereinrichtungen oder in Transportbehältern, können wichtige Parameter, wie Temperatur, Feuchtigkeit und Luftqualität, überwacht werden (dazu und zum Folgenden Teuteberg/Anton 2023, S. 60 f.). Dies ermöglicht eine frühzeitige Erkennung von Abweichungen in der Kühlkette und hilft dabei, potenzielle Qualitätsprobleme zu identifizieren, bevor sie sich auf die Lebensmittel auswirken. Dies ist vor allem entscheidend für leicht verderbliche Produkte (z. B. Milch und Milchprodukte), für die strenge Hygiene- und Regulierungsstandards eingehalten werden müssen. Die Kühllogistik von Milch und Milchprodukten erstreckt sich von der Milcherzeugung bis hin zur Verteilung der Produkte an den Lebensmitteleinzelhandel (Kasten 2.2).

Kasten 2.2 Anforderungen an die Logistik von Milch und Milchprodukten

In der gesamten Lieferkette von Milch und Milchprodukten müssen strenge Hygiene- und Temperaturanforderungen eingehalten werden, um die Gesundheit der Verbraucher/innen nicht zu gefährden (dazu und zum Folgenden Teuteberg/Anton 2023, S. 31). Die Anforderungen an die Rohmilcherzeugung besagen, dass die Tiere, von denen die Rohmilch stammt, frei von ansteckenden Krankheiten sein müssen, gesunde Lebensbedingungen haben, keine unerlaubten Substanzen oder Behandlungen erhalten und frei von Brucellose oder Tuberkulose sein müssen. Sind diese Anforderungen nicht erfüllt, kann die Rohmilch nur unter bestimmten Bedingungen verwendet werden, z. B. nach Wärmebehandlung. Die Kühlkette muss streng eingehal-

ten werden: Die Milch muss unmittelbar nach dem Melken auf 8 °C gekühlt werden, wenn sie täglich, oder auf 6 °C, wenn sie nicht täglich gesammelt wird. Bis zur Verarbeitung darf die Temperatur 10 °C nicht überschreiten. Im Verarbeitungsbetrieb ist die Milch auf 6 °C abzukühlen. Um die Einhaltung der Temperatur zu kontrollieren, sind Kühltanks mit einer Kontrolleinheit ausgestattet, die bei technischen Problemen, wie z. B. einer Störung des Rührwerks oder des Kühlsystems, einen Alarm auslöst. Die Technik im Sammelfahrzeug ermöglicht es, Milchproben für die spätere Analyse im Labor zu entnehmen. In der Molkerei wird die Rohmilch auf verschiedene Kriterien geprüft, bevor sie in großen Lagertanks der Molkerei gelagert wird. Die fertigen Molkereiprodukte werden an Großverbraucher oder die Ernährungsindustrie geliefert. Die Molkereierzeugnisse gelangen schließlich überwiegend über den Lebensmitteleinzelhandel zu den Verbraucher/innen (Milchindustrie-Verband e. V. 2020, S. 4).

IoT-Anwendungen werden von 61 % der deutschen Logistikfirmen eingesetzt (Bitkom 2022). Moderne Lagerhäuser (Abb. 2.1) setzen mit KI ausgestattete Roboterarme und fortschrittliche Sensorik ein, um Artikel aller Art mit der Präzision von Chirurgen zu entnehmen (Hao 2021). Die Zunahme des Lebensmittelonlinehandels verstärkt den Trend zum Einsatz von IoT, denn der Onlinehandel bringt neue Herausforderungen mit sich. Logistikdienstleister müssen eine große Auswahl an Produkten aus einem umfangreichen Sortiment kommissionieren und zustellen können, wobei diese Produkte verschiedenen Temperaturbereichen unterliegen und innerhalb eines 1- bis 2-stündigen Zeitfensters zum Kunden gebracht werden (BITO 2020). Durch den Einsatz digitaler Lösungen, wie spezialisierte Logistiksoftware und Sensorik, können Routen optimiert, Temperaturen überwacht und die Verwaltung von Beständen optimiert werden (Noss et al. 2022, S. 3 ff.). Modernste digitale Bestands- und Packsysteme versprechen eine 10-fache Effizienzsteigerung bei einzelnen Packaufgaben (Rodríguez García/Agmoni 2024, S. 6).

Abb. 2.1 Lagersystem der Ocado-Gruppe im Onlinehandel

Quelle: Rodríguez García/Agmoni 2024, S. 6

Cloudcomputing: 68 % der Logistikunternehmen mit 20 oder mehr Mitarbeiter/innen in Deutschland nutzen Cloudcomputing bzw. Clouddienstleistungen, um Logistikprozesse durch Senkung der Hard- und Softwarekosten zu optimieren (Remondino/Zanin 2022, S. 11 f.). Gemäß der Verordnung (EG) 178/2002[7] müssen entlang der gesamten Lebensmittellieferkette alle Schritte der Verarbeitung, Lagerung, Kommissionierung und des Transports nachweisbar sein. Das Teilen von Daten über ein zentrales Speichersystem erleichtert die nahtlose Zusammenarbeit und den Datenaustausch zwischen den verschiedenen Akteuren entlang der Lieferkette, um die Rückverfolgbarkeit von Lebensmitteln zu gewährleisten. Durch die Speicherung von Daten in der Cloud können Informationen über Produktionsbedingungen, Zertifizierungen, Transport- und Lagerbedingungen in Echtzeit zugänglich gemacht werden. Dadurch wird die Transparenz verbessert und eine effektive Überwachung der Einhaltung von Qualitäts- und Sicherheitsstandards in der Kühlkette ermöglicht (Teuteberg/Anton 2023, S. 61).

Virtual Reality (VR) und *Augmented Reality* (AR) sind in der Branche bereits weit verbreitet (IDG 2019, S. 7). Während VR eine virtuelle Umgebung schafft und für die Schulung von Mitarbeiter/innen am Arbeitsplatz genutzt wird, werden AR-Anwendungen zur Unterstützung von alltäglichen Logistikprozessen eingesetzt. Sie ermöglichen das Vision Picking, bei welchem Lager-

7 Verordnung (EG) Nr. 178/2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit, konsolidiert am 1.7.2022

arbeiter/innen visuelle Informationen über Auftrags- oder Bestandsdaten auf einem mobilen Gerät, wie etwa einem Tablet oder einer Datenbrille, erhalten und Sprachbefehle zur Kommissionierung gegeben werden können (Remondino/Zanin 2022, S. 11 f.; TeamViewer 2024). Diese Art von Lösungen könnten künftig um Exosuits ergänzt werden, also tragbare robotische Geräte, die den menschlichen Körper von Lagerarbeiter/innen unterstützen und körperliche Belastungen verringern (Rodríguez García/Agmoni 2024, S. 10).

Zu den weiteren Technologien, die perspektivisch eine Rolle in der Branche spielen könnten, gehören digitale Zwillinge, Blockchaintechnologien und Drohnen (dazu und zum Folgenden Teuteberg/Anton 2023, S. 63 ff.).

Digitale Zwillinge bezeichnen die virtuelle Nachbildung einer realen Lieferkette auf Grundlage realer Daten. Mithilfe von Prognosemodellen können die Auswirkungen angedachter Entscheidungen auf die Lieferkette simuliert werden, um eine vorausschauende Planung zu ermöglichen (Kroh 2022). Digitale Zwillinge können u. a. beim Management von Containerflotten, bei der Überwachung von Sendungen und bei der Gestaltung ganzer Logistiksysteme eingesetzt werden. Sie sind in 14 % der Logistikunternehmen im Einsatz (Bitkom 2022).

Blockchaintechnologien können dazu beitragen, Warenflüsse entlang der Lieferkette transparenter zu gestalten und eine verlässlichere Rückverfolgbarkeit der Lebensmittel zu gewährleisten, indem alle Transaktionen auf der Blockchain festgehalten werden, angefangen von der Erzeugung bis hin zum Verkauf an die Endverbraucher. Dies ermöglicht es, im Falle eines Rückrufs oder einer Kontamination schnell und präzise zu ermitteln, woher ein bestimmtes Produkt stammt und wohin es gegangen ist. Bislang sind Blockchainlösungen bei 5 % der Unternehmen aus der Logistikbranche im Einsatz (Schrauf et al. 2020, S. 22). Außerdem ermöglichen sie eine sichere Datenverschlüsselung und einen zuverlässigen, auf Berechtigungen basierenden Zugriff durch den Einsatz von Smart Contracts (Remondino/Zanin 2022, S. 11 f.).

Drohnen – ferngesteuerte oder autonom fliegende unbemannte Luftfahrzeuge – könnten die Zustellung zum Endkunden übernehmen, besonders in Gebieten, die für herkömmliche Transportmittel schwer erreichbar sind. Außerdem können sie zur Automatisierung der Lagerhaltung eingesetzt werden (z. B. Inventarüberwachung, Etikettierung und Platzierung von Produkten) (Remondino/Zanin 2022, S. 11 f.). Sie sind in 4 % der Logistikunternehmen verbreitet (Bitkom 2022).

2.4 Handel

Auch im (Einzel-)Handel ist eine voranschreitende Digitalisierung zu beobachten (HDE 2023a, S. 12), wobei ebenfalls zentrale Verwaltungssysteme, wie *Warenwirtschaftssysteme*, eine zentrale Rolle spielen. Sie ermöglichen die integrierte Überwachung und Steuerung wichtiger Prozesse im Unternehmen, wie

Bestellverwaltung und Lieferkettenmanagement, Buchhaltung und Finanzmanagement, Personalverwaltung und Gehaltsabrechnung sowie Berichterstattung und Analyse (Haufe o. J.). Fallen solche zentralen Verwaltungssysteme aus, führt das zu größeren Störungen im Betrieb. Trends im Handel sind insbesondere die Verbreitung digitaler Kassensysteme, digitaler Handelsplattformen und der zunehmende Zugriff auf Cloudcomputing und Einsatz von KI.

Digitale Kassensysteme (POS-Systeme) sind Kernbestandteil des IT-Systems in Einzelhandelsfilialen. Diese computerbasierten Systeme werden verwendet, um Verkäufe und Transaktionen abzuwickeln. Sie umfassen die gängigen Kassenfunktionen, gehen aber darüber hinaus (ionos 2021). Ein POS-System besteht normalerweise aus Hard- und Software sowie Peripheriegeräten wie Kassenschublade, Barcodescanner, Kreditkartenleser und Drucker. Die Hauptfunktionen umfassen das Scannen von Produkten, die Berechnung von Preisen, die Verarbeitung von Zahlungen, das Ausstellen von Quittungen und die Verwaltung von Beständen. Moderne POS-Systeme verfügen auch über Funktionen wie Kunden- und Mitarbeiterverwaltung, Bestandsverfolgung, Berichterstattung und Analyse. Sie helfen Unternehmen dabei, den Verkaufsprozess effizienter zu gestalten, Bestände zu verwalten, Umsätze zu verfolgen sowie Einblicke in das Kaufverhalten der Kunden zu gewinnen. Mit der Erweiterung von Funktionalitäten in Richtung Bestandsverwaltung in Echtzeit verschmelzen POS-Systeme mit Warenwirtschaftssystemen (ionos 2021). Warenbestände können in Echtzeit angezeigt werden, wodurch die Verwaltung von Beständen noch stärker optimiert wird bzw. »just in time« erfolgen kann. Dafür können sich POS-Systeme beispielsweise für die Bestellung von frischem Obst und Gemüse aus der EU auf speziell dafür entwickelte Algorithmen stützen. In der Regel wird eine Bestellung morgens erstellt, die dann an die Supermarktzentrale übermittelt und vor 12 Uhr mittags desselben Tages an einen ihrer Drittlieferanten in der EU weitergeleitet wird. Die Lieferung trifft am nächsten Tag in der Filiale ein. Dies wird als Tag-eins-für-Tag-zwei-System (Day one for Day two System; Garnett et al. 2020, S. 316) bezeichnet. Das Angebot an POS- und Warenwirtschaftssystemen weist grundsätzlich eine hohe Vielfalt auf (Martens 2023; trusted o. J.). Wie homogen die speziell im Lebensmitteleinzelhandel eingesetzten Systeme sind, ist nicht genau auszumachen. Weitere Trends sind die Verknüpfung von Kassensystemen mit digitalen Preisschildern (LZ direkt 2022) und die zunehmenden Bezahlmöglichkeiten via Smartphone bzw. Smartwatch (Statista 2023). Außerdem hatte 2023 etwas mehr als die Hälfte deutscher Händler kassenlose Stores entweder im Betrieb oder in Planung (EHI 2023).

Digitale Handelsplattformen können zwischen verschiedenen Stufen der Wertschöpfungskette eingesetzt werden (dazu und zum Folgenden Hoffmann/Haas 2023, S. 23; Teuteberg/Anton 2023, S. 55 f.).

- *Zwischen Anbietern von Betriebsmitteln und Landwirtschaftsbetrieben*: Neben Produkten werden auch Zusatzleistungen für Landwirte digital angebo-

ten. An- und Verkauf von Getreide erfolgen mittlerweile über digitale Plattformen. Darüber hinaus läuft ein erheblicher Teil des Betriebsmittel-, aber auch des Landmaschinenhandels über das Internet. Informationen zur Rückverfolgbarkeit oder zum CO_2-Fußabdruck werden zunehmend digital zwischen Produzenten und Händlern übermittelt.[8]

- *Zwischen Landwirten und Verarbeitern*: Digitale Handelsplattformen werden auch für den Handel zwischen Produzenten und Verarbeitern genutzt, wie beispielsweise zwischen Milchproduzenten und Molkereien. So stellt MilkScout[9] eine Vermittlungsplattform dar, über die Milchproduzenten Milch und Milchprodukte an Molkereien und Lebensmittelunternehmen verkaufen können.
- *Zwischen Landwirten und Verbraucher/innen*: Digitale Handelsplattformen werden von Landwirten eingesetzt, um alternative Absatzwege für ihre Produkte zu erschließen (Kreutz 2021). Aufgrund der hohen Transportkosten sind solche Geschäftsmodelle nicht immer wettbewerbsfähig, weswegen ihr Marktanteil gegenüber dem Marktanteil des Lebensmitteleinzelhandels relativ klein ist (Holzner/Hümmer 2023).
- *Zwischen Verarbeitung und Verbraucher/innen*: Auch für die Lieferung von fertigen Mahlzeiten werden Bestellmöglichkeiten über Lieferserviceportale immer stärker in Anspruch genommen (VuMA 2021).
- *Zwischen Supermärkten und Verbraucher/innen*: Schnelllieferdienste, die Lebensmittel und Produkte des täglichen Bedarfs oft innerhalb von 10 bis 20 Minuten an den Kunden bringen, werden immer beliebter. Zwischen 2021 und 2024 ist der Anteil der Internetnutzer/innen in Deutschland, die bereits einen Schnelllieferdienst genutzt haben, von 10 auf 16 % gewachsen (Bitkom 2024). Allerdings kaufen rund 54,8 % der Deutschen keine Lebensmittel online ein und lediglich 2,7 % aller Befragten kaufen mehr als die Hälfte der Nahrungsmittel online (Nusser 2024).

Die Grenze zwischen On- und Offlinehandel verschwimmt durch die Zunahme von Omnichanneldienstleistungen. Dabei handelt es sich um kanalübergreifende Geschäftsmodelle, bei denen beispielsweise die Verfügbarkeit von Artikeln online abgerufen werden kann oder Artikel online bestellt und in der Filiale abgeholt werden können (Click and Collect) (Statista 2023). Inzwischen verkaufen 85 % der Händler sowohl online als auch stationär (Bitkom 2023).

Softwaresysteme sind auch im Handel zunehmend *cloudbasiert*. 48 % der Handelsunternehmen maßen 2021 cloudbasierten Anwendungen eine große Bedeutung bei (Acar 2021). Diese dürften sich in naher Zukunft flächendeckend

8 hierzu beispielsweise https://www.cropspot.com; https://www.agriconomie.de/de_DE/; https://www.baywa.de/; https://web.ftrace.com/ (28.5.2024)
9 https://milkscout.eu/ (28.5.2024)

durchsetzen.[10] Ebenso hält *künstliche Intelligenz* im Einzelhandel Einzug (Teuteberg/Anton 2023, S. 56 ff.), obwohl die Einschätzungen zum Umfang des Einsatzes stark variieren: Zwischen 23,5 (HDE 2023b, S. 6) und 69 % (EHI 2023) der Handelsunternehmen setzen KI entweder in einzelnen Bereichen oder unternehmensübergreifend ein. Die Bereiche, in denen KI eingesetzt wird, reichen von Bedarfsprognose und Optimierung der internen Logistik über Preismanagement und Sortimentsgestaltung bis hin zum Kundenbeziehungsmanagement. Perspektivisch könnten KI-basierte Dienste eingesetzt werden, um die Nachfrage nach Lebensmitteln genauer zu ermitteln bzw. zu prognostizieren und Produktionsprozesse entsprechend anzupassen (BMWK o. J.).

10 Zumindest stimmen 60 % der Einzelhändler in Deutschland laut einer Umfrage dieser These zu (Acar/Hahn 2024).

3 Bedrohungslage

Cybersicherheit umfasst den Schutz vor einer Vielzahl an Bedrohungen, die die Sicherheit und Integrität von Computersystemen und Daten gefährden könnten. Das bedeutet nicht nur den Schutz vor Cyberangriffen, sondern auch die Vorbeugung und Bewältigung von Technikversagen sowie anderen potenziellen Risiken im Zusammenhang mit Informationstechnologie und Computersystemen. Entsprechend dem Auftrag werden im vorliegenden Bericht vor allem die möglichen Auswirkungen von Cyberangriffen durch vorsätzliche Handlungen auf betriebliche Prozesse entlang der Lebensmittelwertschöpfungskette in den Fokus genommen. Es werden die häufigsten Angriffsarten und -motive skizziert, die Prävalenz von Angriffen nach Wertschöpfungsstufen sowie ihre Schwere ausgewertet und schließlich neue Bedrohungen näher erörtert. Die Analyse stützt sich auf die Ergebnisse der Gutachten von Teuteberg und Anton (2023) und Hoffmann und Haas (2023). Insbesondere wird auf die quantitative Analyse von Teuteberg und Anton (2023) näher eingegangen (Kasten 3.1).

Kasten 3.1 Methodik des Gutachtens von Teuteberg und Anton

Die in den Kapiteln 3 und 4 durchgeführten Analysen zu Cyberangriffen (Angriffsarten, Prävalenz) stützen sich vornehmlich auf die von Teuteberg und Anton (2023) analysierten quantitativen Daten zu Cyberangriffen. Diese stammen zum einen aus der Datenbank des Centers for International & Security Studies at Maryland (CISSM-Datenbank) der University of Maryland. Die Datenbank nutzt eine Kombination aus automatisierten Verfahren und manueller Überprüfung, um Informationen zu Motiv, Art und Auswirkungen von Cyberangriffen aus verschiedenen Quellen zu sammeln (CISSM o. J.). Zum Zeitpunkt der Untersuchung konnten 182 Cybereregnisse identifiziert werden, die zwischen März 2014 und Februar 2023 stattfanden und mit der Landwirtschaft, Ernährungsindustrie und dem Gastgewerbe in Zusammenhang stehen. Lediglich 4 dieser Fälle fanden in Deutschland statt. Es wurden zum einen alle 182 Angriffe sowohl für Deutschland als auch international analysiert, die dem Sektor Landwirtschaft und Ernährung zugeordnet werden konnten. Zum anderen werteten Teuteberg und Anton (2023) alle 188 in der Datenbank erfassten Angriffe aus, die in Deutschland stattfanden, unabhängig von der betroffenen Branche.

Um die Prävalenz von Cybersicherheitsvorfällen in der Ernährungsindustrie innerhalb der deutschen Wirtschaft genauer zu erfassen und weil aktuellere Daten nicht vorliegen, zogen Teuteberg und Anton (2023) zusätzlich Sekundärdaten

aus einer älteren Befragung heran. Diese mithilfe computergestützter Telefoninterwies (Computer Assisted Telephone Interviewing – CATI) durchgeführten Befragung (im Folgenden CATI-Befragung) fand zwischen August 2018 und Januar 2019 mit 5.000 deutschen Unternehmen diverser Wirtschaftszweige statt – darunter 945, die sich dem Sektor Landwirtschaft und Ernährung zuordnen lassen (dazu u. a. von Skarczinski et al. 2023). Dabei wurden Informationen über Cyberangriffe, ihre Schäden und Schutzmaßnahmen der Unternehmen gesammelt. Die Daten geben Aufschluss über die Herausforderungen, denen sich insbesondere auch kleine und mittlere Unternehmen, die über begrenzte Ressourcen und ein sich noch entwickelndes Bewusstsein für Cybersicherheit verfügen, beim Schutz vor Cyberangriffen gegenübersehen (Dreißigacker et al. 2020 S. 47 ff.). Es ist zu beachten, dass die Zuordnung der wirtschaftlichen Aktivitäten der Unternehmen zu dem Sektor auf der Klassifikation der Wirtschaftszweige des Statistischen Bundesamtes (Destatis 2008) beruht. Dabei wurden alle Handelsunternehmen sowie Unternehmen im Bereich Verkehr und Lagerei in die Stichprobe genommen, unabhängig von der Art der Waren, die diese Unternehmen verkaufen, transportieren oder lagern (Teuteberg/Anton 2023, S. 84 f.). In der Summe handelt es sich um eine Auswertung von Cybersicherheitsvorfällen nicht nur in den Branchen Landwirtschaft und Ernährungsindustrie, sondern auch in verbundenen Branchen Handel und Logistik (im Folgenden als Sektor Landwirtschaft und Ernährung bezeichnet).

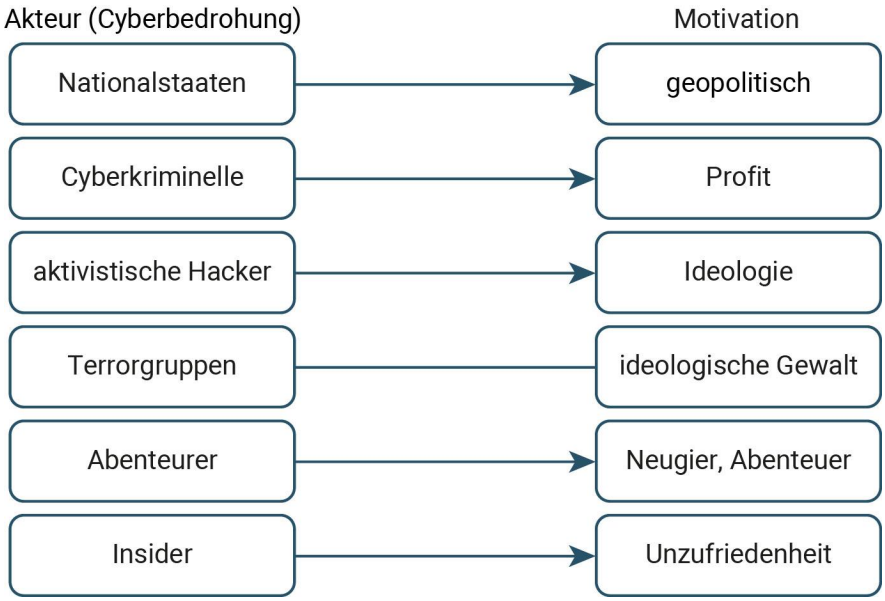
3.1 Angriffsarten und -motive

Motive für Cyberangriffe sind vielfältig und lassen sich auf unterschiedliche Akteursgruppen zurückführen (Abb. 3.1). Aktuell gilt die wirtschaftliche Bereicherung als das häufigste Motiv und die größte Gefahr für Unternehmen. Verantwortlich dafür sind Cyberkriminelle. Global agierende Unternehmen sehen sich auch von Nationalstaaten mit geopolitischen Motiven zunehmend bedroht. So zeigt die Analyse von Teuteberg/Anton (2023, S. 81), dass die wirtschaftliche Bereicherung als Motiv bei 59 % der untersuchten Cyberangriffe in Deutschland branchenübergreifend galt,[11] gefolgt von politischer Spionage in 8,5 % der Fälle (Abb. 3.2). Industriespionage macht 6,4 % der Cyberangriffe aus, Protest 2,66 %, Sabotage 1,1 % und allgemeine Spionage 0,5 %. In 21,8 % der Fälle sind die Motive nicht bekannt (Teuteberg/Anton 2023, S. 81). Für landwirtschaftliche Betriebe mit Tierhaltung und in der Fleischverarbeitung im Speziellen geht beispielsweise ein Gefahrenpotenzial durch Protest von aktivistischen Hackern mit ideologischen Motivationen aus, die die Tierhaltungsbedingungen anprangern oder grundsätzlich ablehnen. Durch die technischen Möglichkeiten, die generative KI bietet, wird auch Hobbyhackern zunehmend

11 Analyse der in der CISSM-Datenbank erfassten Cyberangriffe auf deutsche Unternehmen

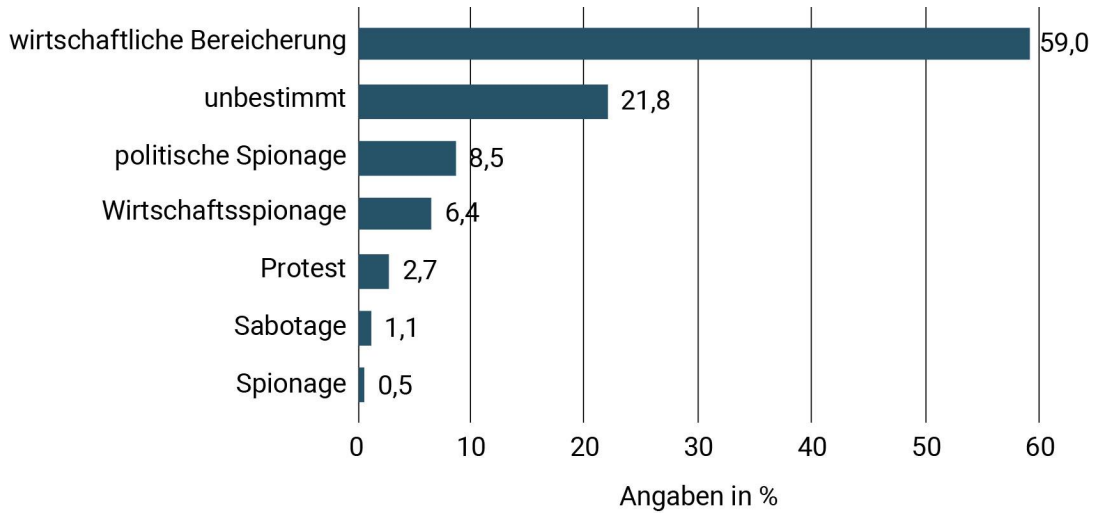
zugetraut, Schäden durch einen gezielten Cyberangriff auf landwirtschaftliche Betriebe anzurichten. Vereinzelt wurden in den Unternehmen auch ehemalige Mitarbeiter/innen als konkrete Angreifer ausgemacht (Hoffmann/Haas 2023, S. 33).

Abb. 3.1 Cyberakteure und deren Motivation



Quelle: nach Cyber Centre 2022, S. 2, nach Hoffmann/Haas 2023, S. 33

Abb. 3.2 Häufigkeit der Motive für Cyberangriffe in Deutschland



n = 188; Zeitraum 2014–2023, branchenübergreifend

Quelle: nach Teuteberg/Anton 2023, S. 81, auf Grundlage der CISSM-Datenbank

Zu den häufigsten und gefährlichsten Angriffsarten zählen vor allem Ransomware und Phishing. Diese gelten als typische Einfallstore für großangelegte Cyberattacken. Auf diese Angriffsarten sowie auf (D)DoS-Angriffe, die besonders für Unternehmen, deren Kernleistung auf einer Internetplattform beruht, ein Risiko darstellen, wird nachfolgend näher eingegangen (dazu und zum Folgenden Teuteberg/Anton 2023, S. 67 ff.):

- *Ransomware*: Unter Ransomware wird eine Manipulation, Zerstörung oder Verschlüsselung von Daten verbunden mit der Aufforderung zur Zahlung eines Lösegelds verstanden. Dafür wird eine Schadsoftware (Malware) in ein IT-System eingeschleust. Die Infektion kann über eine E-Mail, eine Internetseite, ein Speichermedium oder ein in das Unternehmensnetzwerk eingebundenes mobiles Endgerät erfolgen. Sobald der Zugriff auf Daten und Systeme gesperrt ist, beispielsweise über eine kryptografische Verschlüsselung, wird der Benutzer zur Zahlung des Lösegeldes in der Regel mittels schwer nachverfolgbarer Zahlungsmethoden in Kryptowährungen aufgefordert (Dreißigacker et al. 2020, S. 99). In den letzten Jahren nahmen die Häufigkeit und das Ausmaß der durch Ransomwareangriffe verursachten Schäden deutlich zu (BKA 2022, S. 1 f.). Außerdem hat sich das Ransomwaregeschäftsmodell in den letzten Jahren zu einem Ransomware-as-a-Service-Modell entwickelt, bei dem Schadsoftware und Dienste, wie z. B. die Datenexfiltration, anderen Gruppen und Einzelpersonen gegen Provision angeboten werden (Microsoft 2022, S. 9).
- *Phishing*: Beim Phishing wird die Identität einer Person vorgetäuscht, mit dem Ziel, an vertrauliche Informationen (z. B. Passwörter, Kreditkartennummern) zu gelangen oder eine Person zu einer Geldüberweisung zu bewegen. Dies geschieht beispielsweise, indem das Opfer dazu verleitet wird, auf einen gefälschten Link zu klicken. Werden dafür Absender-IP, -Name oder -Adresse so gefälscht, dass ein Empfänger sie für vertrauenswürdig hält, spricht man von Spoofing. Auch Unternehmensdienste können vorgetäuscht werden (z. B. Amazon, DHL) oder die eigenen Vorgesetzten (CEO-Fraud).
- *Denial-of-Service(DoS)-Angriffe*: Als DoS-Angriff wird das Absetzen massenhafter Anfragen auf ein System bezeichnet, welches dann durch Überlastung zum Erliegen kommt. Der Zugang zu internen oder externen Systemen (z. B. Kundenplattform) des Betriebs wird dadurch gesperrt. Werden Massenanfragen aus verschiedenen verteilten kompromittierten Computern verschickt, spricht man von Distributed-DoS(DDoS)-Angriffen. Die Eindämmung und die Abwehr von (D)DoS-Angriffen stellen für Unternehmen eine große Herausforderung dar (Teuteberg/Anton 2023, S. 135 f.).

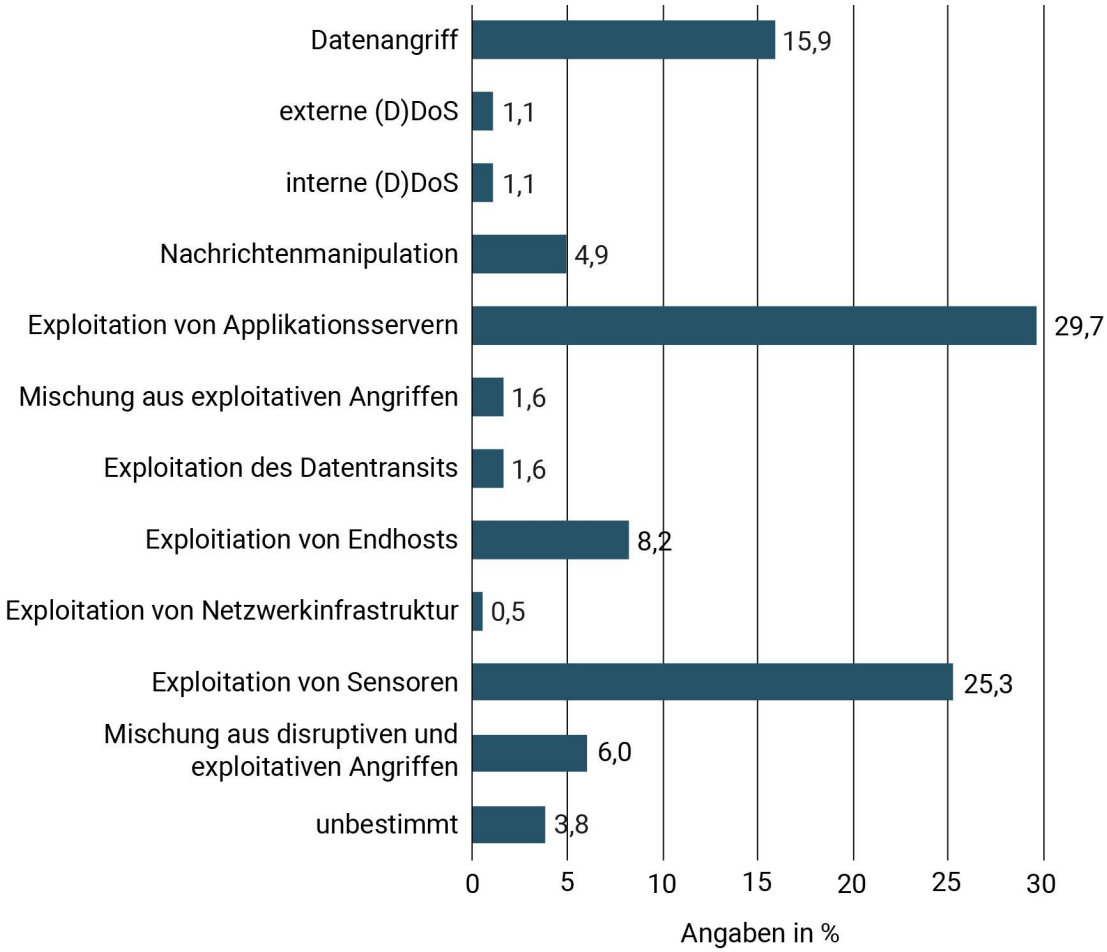
Angriffsarten sind vielfältig und der Kreativität von Angreifern kaum Grenzen gesetzt. Neben der Verschlüsselung von Daten zur Lösegeldforderung kann

bösartige Schadsoftware auch weiteren Zielen dienen. *Spyware* ermöglicht beispielsweise die Beobachtung des Onlineverhaltens von Nutzer/innen und das Ausspähen von Daten. Zu den üblichen Angriffsarten gehören außerdem das manuelle Hacking von Systemen, bei welchem Computerhard- und -softwareeinstellungen ohne den Einsatz von Schadsoftware manipuliert werden, oder auch die Verunstaltung von Webseiten (Defacing), beispielsweise um die Reputation des Webseitenbetreibers zu schädigen (BSI 2021a, S. 4). Neue Arten von Angriffen entstehen im Zusammenhang mit zunehmend verbreiteten Technologien, derzeit vor allem der KI. Dazu gehören die Manipulation von Eingabedaten (Evasion/Adversarial Attacks) oder von Trainingsdaten der KI (Data Poisoning Attacks) oder auch die Extraktion von Informationen über Funktionalität und Struktur der KI-Modelle (Model Stealing Attacks) (BSI 2021b, S. 5).

Cyberangriffe unterscheiden sich markant durch ihre Auswirkungen auf die Wertschöpfungskette (Harry/Gallagher 2018, S. 6 ff.). Ereignisse können disruptiver oder exploitativer Natur sein. Cybereereignisse disruptiver Natur wirken sich auf die IT-Infrastruktur eines Unternehmens aus und verursachen eine Betriebsstörung. Dazu zählen (D)DoS-Angriffe, Ransomware und manuelle Angriffe auf Steuerungssysteme oder Sensoren. Cybereereignisse exploitativer Natur dienen hingegen der illegalen Informationsgewinnung (Teuteberg 2023, S. 76 f.). Im Sektor Landwirtschaft und Ernährung überwiegen mit einem Anteil von etwa 69 % die exploitativen Angriffe[12] (Teuteberg/Anton 2023, S. 81). Dabei ist mit 29,7 % besonders die Exploitation von Applikationsservern die häufigste Angriffsart, gefolgt von der Exploitation von Sensoren (25,3 %) und Datenangriffen (15,9 %) (Abb. 3.3). Exploitative Angriffe können sich ebenfalls auf den Betrieb auswirken, allerdings zunächst nur indirekt (z. B. Stehlen von Daten und Drohung einer Veröffentlichung).

12 Nach der Analyse internationaler Vorfälle im Sektor Landwirtschaft und Ernährung auf Grundlage der CISSM-Datenbank (Zeitraum 2014–2023) (Teuteberg/Anton 2023, S. 83).

Abb. 3.3 Länderübergreifende Angriffsarten auf die Ernährungsindustrie



n = 182; Zeitraum 2014–2023

Quelle: nach Teuteberg/Anton 2023, S. 83, auf Grundlage der CISSM-Datenbank

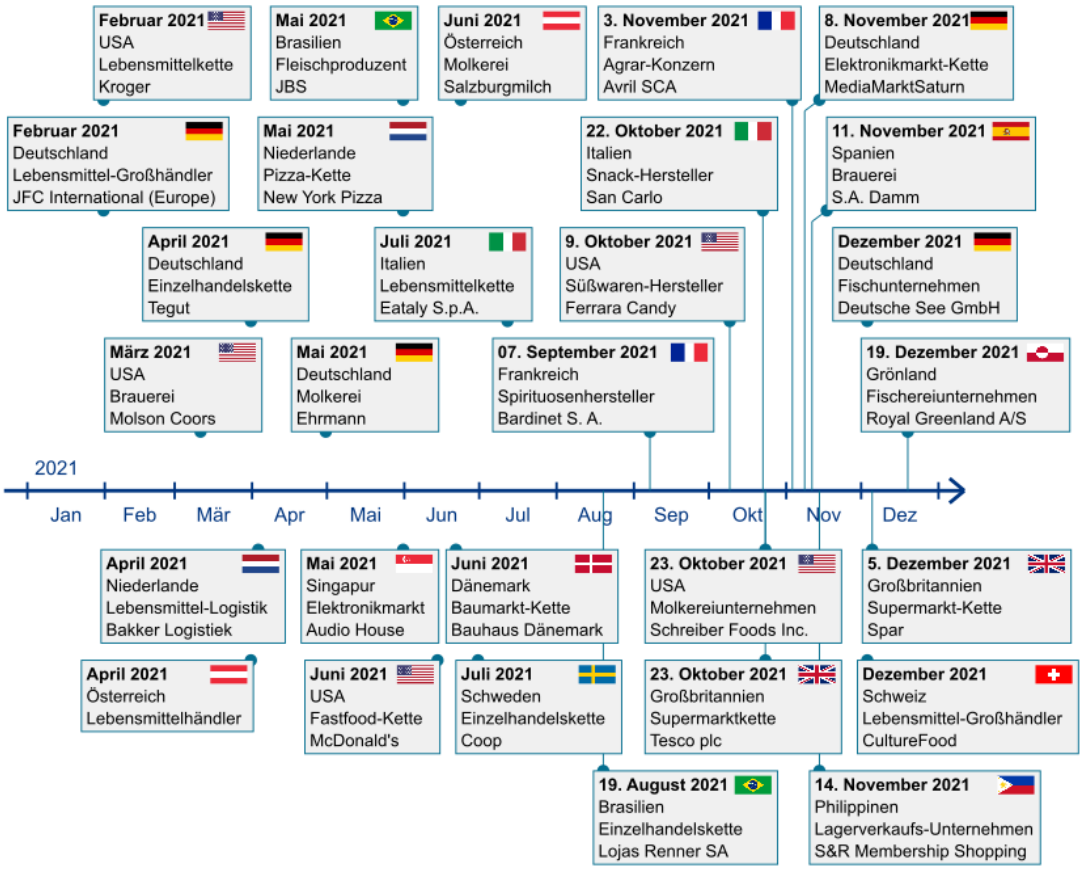
3.2 Prävalenz von Angriffen nach Wertschöpfungsstufen in Deutschland

Die Anzahl der Angriffe auf den Sektor Landwirtschaft und Ernährung und die erpressten Geldsummen nahmen in den letzten Jahren zu. Zwar werden die Lösegelder häufig nicht bekannt gemacht, allerdings zeigen einzelne Beispiele, dass diese bis in den zweistelligen Millionenbereich[13] reichen (Hoffmann/Haas 2023, S. 29). Knapp 69 % der deutschen Unternehmen im Bereich Landwirtschaft und Ernährung[14] waren bis 2019 bereits Opfer eines oder mehrerer Cyberangriffe geworden (Teuteberg/Anton 2023, S. 88). Es ist anzunehmen, dass die Dunkelziffer

13 Die erpresste Geldsumme für den Angriff auf Kaseya betraf 70 Mio. US-Dollar (Kap 4.4).
14 Diese Daten beziehen sich auf die von Teuteberg/Anton (2023) analysierten Daten aus der CATI-Befragung von 2018/2019.

noch höher ist, als es die gemeldeten Fälle und Statistiken vermuten lassen (Teuteberg/Anton 2023, S. 140). Außerdem hat sich die Lage der IT-Sicherheit in Deutschland in den letzten Jahren deutlich zugespitzt. 2023 war die Lage »angespannt bis kritisch« (BSI 2023, S. 11). Die Abbildungen 3.4 und 3.5 illustrieren den Umfang bekannter bedeutsamer Angriffe im Sektor Landwirtschaft und Ernährung in den Jahren 2021 und 2023. Um die Lage der Cybersicherheit im Sektor Landwirtschaft und Ernährung näher zu beschreiben, stützt sich die Analyse hauptsächlich auf die CATI-Befragung von 2018/2019 (Kasten 3.1). Genauere bzw. aktuellere Daten liegen dem TAB in diesem Detaillierungsgrad nicht vor.

Abb. 3.4 Cyberangriffe auf Unternehmen im Bereich der schnelllebigen Konsumgüter 2021



Quelle: KonBriefing 2022

Abb. 3.5 Bedeutende Cyberangriffe auf die Lebensmittelbranche 2023

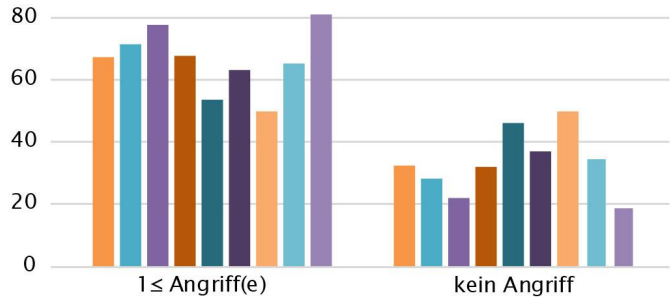
Quelle: KonBriefing 2024

Von Cyberangriffen sind die Wertschöpfungsstufen unterschiedlich stark betroffen (Abb. 3.6). Aus der CATI-Befragung lässt sich ablesen, dass bis 2019 zwei Drittel der Einzelhändler bereits von mindestens einem Angriff betroffen waren – Logistikunternehmen tendenziell weniger. Eine Ausnahme gilt für Expressdienste[15], von denen 80 % mindestens einen Angriff zu verzeichnen hatten (dazu und zum Folgenden Teuteberg/Anton 2023, S. 88 ff.).

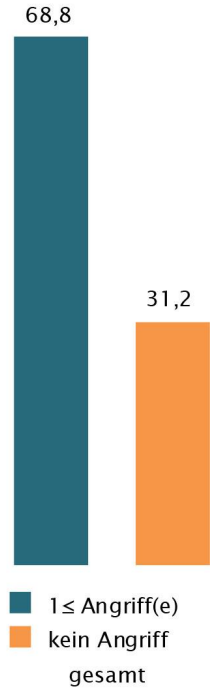
Zu den schwerwiegendsten Vorfällen im Sektor Landwirtschaft und Ernährung in Deutschland gehören mit 27 % das Phishing und mit 20,6 % die Ransomwareangriffe, die in der CATI-Befragung erfasst wurden (Abb. 3.7). In weiteren 20,1 % der Fälle ging der Cyberangriff auf sonstige Schadsoftware zurück. Diese drei Angriffsarten sind in fast allen Wertschöpfungsstufen zu finden. Außerdem sind weitere Angriffsarten in einzelnen Wertschöpfungsstufen vergleichsweise stärker vertreten, wie z. B. (D)DoS-Angriffe auf die Netzwerke von landwirtschaftlichen oder lebensmittelverarbeitenden Unternehmen oder Datenspionage durch Spyware im Transportwesen und in der Lagerei. Handel und Logistik haben zudem regelmäßig mit manuellem Hacking und Identitätsfälschung durch Phishing (insbesondere CEO-Fraud) zu kämpfen (Abb. 3.8) (Teuteberg/Anton 2023, S. 48).

15 Zu dieser Kategorie werden neben Expressdiensten auch Post- und Kurierdienste gezählt.

Abb. 3.6 Prävalenz von Cyberangriffen im Sektor Landwirtschaft und Ernährung in Deutschland bis 2019



	1≤ Angriff(e)	kein Angriff
WZ08-01 (n = 37)	67,6	32,4
WZ08-10 (n = 92)	71,7	28,3
WZ08-46 (n = 324)	77,8	22,2
WZ08-47 (n = 147)	68,0	32,0
WZ08-49 (n = 182)	53,8	46,2
WZ08-50 (n = 19)	63,2	36,8
WZ08-51 (n = 4)	50,0	50,0
WZ08-52 (n = 101)	65,3	34,7
WZ08-53 (n = 16)	81,3	18,8

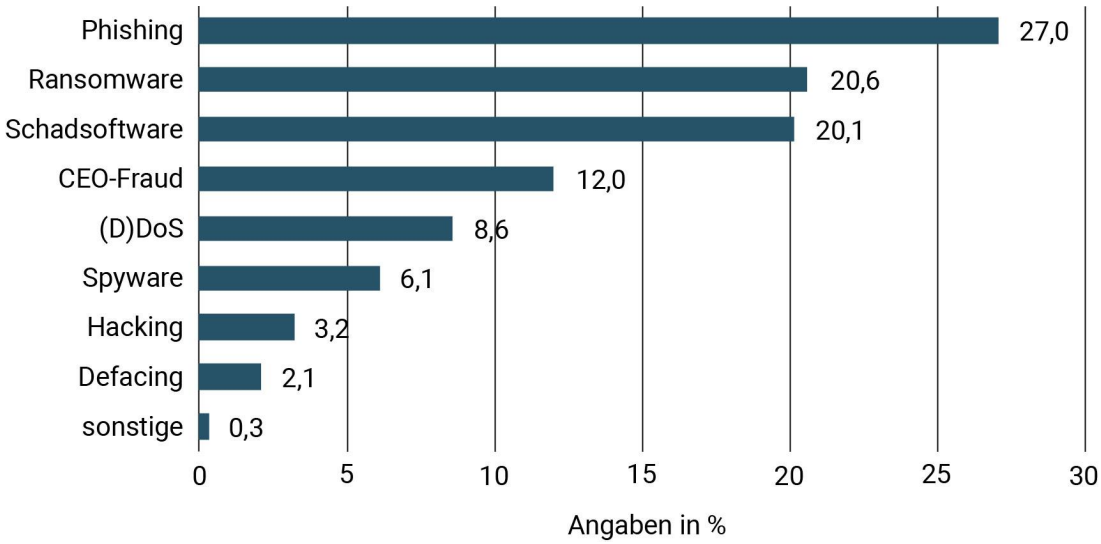


Angaben in %

n = 922; Befragungszeitraum 2018/2019

Quelle: Teuteberg/Anton 2023, S. 88, auf Grundlage der CATI-Befragung

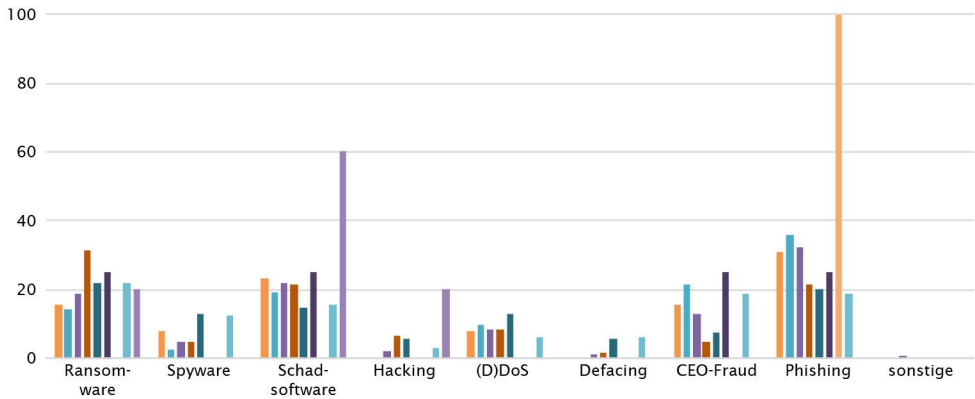
Abb. 3.7 Häufigkeit von Angriffen nach Angriffstyp im Sektor Landwirtschaft und Ernährung in Deutschland



n = 374; Befragungszeitraum 2018/2019, branchenübergreifend

Quelle: nach Teuteberg/Anton 2023, S. 89; auf Grundlage der CATI-Befragung

Abb. 3.8 Häufigkeit von Angriffen nach Angriffstyp und Wertschöpfungsstufe in Deutschland



	Ransom-ware	Spyware	Schad-software	Hacking	(D)DoS	Defacing	CEO-Fraud	Phishing	sonstige
WZ08-01 (n = 13)	15,4	7,7	23,1	0,0	7,7	0,0	15,4	30,8	0,0
WZ08-10 (n = 43)	14,3	2,4	19,0	0,0	9,5	0,0	21,4	35,7	0,0
WZ08-46 (n = 159)	18,7	4,5	21,9	1,9	8,4	1,3	12,9	32,3	0,6
WZ08-47 (n = 61)	31,1	4,9	21,3	6,6	8,2	1,6	4,9	21,3	0,0
WZ08-49 (n = 55)	21,8	12,7	14,5	5,5	12,7	5,5	7,3	20,0	0,0
WZ08-50 (n = 4)	25,0	0,0	25,0	0,0	0,0	0,0	25,0	25,0	0,0
WZ08-51 (n = 1)	0,0	0,0	0,0	0,0	0,0	0,0	0,0	100,0	0,0
WZ08-52 (n = 33)	21,9	12,5	15,6	3,1	6,3	6,3	18,8	18,8	0,0
WZ08-53 (n = 5)	20,0	0,0	60,0	20,0	0,0	0,0	0,0	0,0	0,0

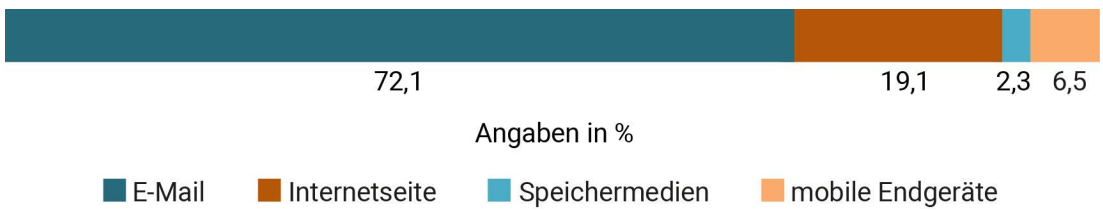
Angaben in %

n = 374; Befragungszeitraum 2018/2019

Quelle: Teuteberg/Anton 2023, S. 89, auf Grundlage der CATI-Befragung

Laut CATI-Befragung wurde Schadsoftware im Sektor Landwirtschaft und Ernährung mit 72,1 % der Fälle in Deutschland am häufigsten per E-Mail in das Unternehmen eingeschleust bzw. vermutlich eingeschleust. Bei 19 % der Fälle erfolgte der Schadsoftwarebefall über eine Internetseite. Andere Infektionswege, wie Speichermedien oder mobile Endgeräte, waren nur selten zu verzeichnen (Teuteberg/Anton 2023, S. 90).

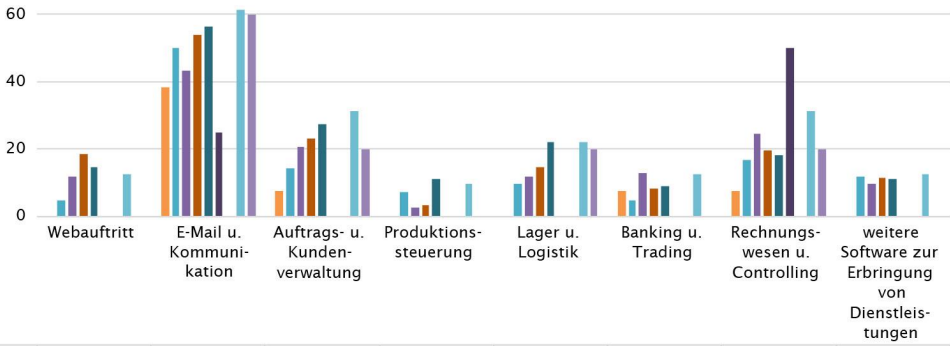
Abb. 3.9 Infektionswege von Schadsoftware im Sektor Landwirtschaft und Ernährung in Deutschland



Befragungszeitraum 2018/2019, branchenübergreifend

Quelle: Teuteberg/Anton 2023, S. 90, auf Grundlage der CATI-Befragung

Abb. 3.10 Betroffene Systeme nach Wertschöpfungsstufen



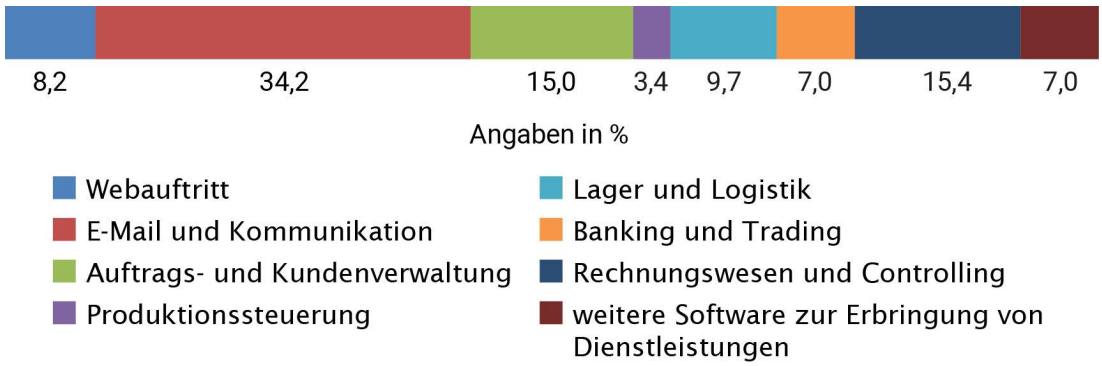
WZ08-01 (n = 13)	0,0	38,5	7,7	0,0	0,0	7,7	7,7	0,0
WZ08-10 (n = 42)	4,8	50,0	14,3	7,1	9,5	4,8	16,7	11,9
WZ08-46 (n = 155)	11,6	43,2	20,6	2,6	11,7	12,9	24,7	9,7
WZ08-47 (n = 61)	18,3	54,1	23,0	3,3	14,8	8,2	19,7	11,5
WZ08-49 (n = 55)	14,5	56,4	27,3	11,1	22,2	9,1	18,2	10,9
WZ08-50 (n = 4)	0,0	25,0	0,0	0,0	0,0	0,0	50,0	0,0
WZ08-51 (n = 1)	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
WZ08-52 (n = 32)	12,5	61,3	31,3	9,7	21,9	12,5	31,3	12,5
WZ08-53 (n = 5)	0,0	60,0	20,0	0,0	20,0	0,0	20,0	0,0

Angaben in %

n = 368; Befragungszeitraum 2018/2019

Quelle: Teuteberg/Anton 2023, S. 90, auf Grundlage der CATI-Befragung

Abb. 3.11 Von den schwerwiegendsten Angriffen betroffene Systeme im Sektor Landwirtschaft und Ernährung in Deutschland



n = 368; Befragungszeitraum 2018/2019, branchenübergreifend

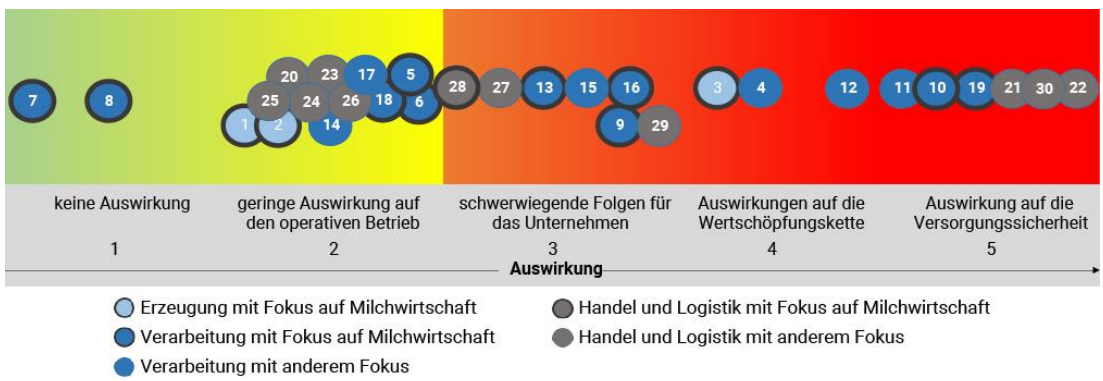
Quelle: Teuteberg/Anton 2023, S. 90, auf Grundlage der CATI-Befragung

Am häufigsten betroffen waren bei den schwerwiegendsten Angriffen E-Mail- und sonstige Kommunikationskanäle (34,2 % der Fälle), gefolgt von Systemen für das Auftrags- und Kundenverwaltungsmanagement sowie das Rechnungswesen und Controlling mit jeweils etwa 15 % der Cybersicherheitsvorfälle. Dies lässt sich damit erklären, dass solche Systeme sektorunabhängig in nahezu allen Unternehmen eingesetzt werden. Spezifischere Systeme (z. B. IT-Systeme zur Produktionssteuerung oder zur Lager- und Logistikverwaltung) waren entspre-

chend weniger oft betroffen – in jeweils 9,4 % und 9,7 % der Fälle (Abb. 3.10 u. 3.11). Neben Systemausfällen waren die betroffenen Unternehmen auch mit unbefugter Löschung, Manipulation, Diebstahl oder Verschlüsselung von Daten konfrontiert (Teuteberg/Anton 2023, S. 91 f.).

Kosten durch Betriebsunterbrechungen, Schäden durch Geldabflüsse, Schadensersatz und Strafen, Wiederherstellung und -beschaffung sowie Reaktionskosten verursacht durch Sofortmaßnahmen zur Abwehr und Aufklärung ebenso wie Kosten für externe Beratung variieren je nach Angriff und Wertschöpfungsstufe stark. Die durchschnittlichen Gesamtkosten für die schwersten Angriffe variieren von 161,42 Euro im landwirtschaftlichen Sektor bis 26.599,53 Euro im Bereich Transportwesen. Die Maximalkosten reichten bis 800.000 Euro und waren für Einzelhandel, Großhandel und Landverkehr/Logistik besonders hoch (Teuteberg/Anton 2023, S. 93). Um Schwere und mögliche Auswirkungen von Cyberangriffen zu evaluieren, werteten Teuteberg und Anton (2023) zusätzlich 30 Cyberangriffe aus, zu denen öffentlich-zugängliche Informationen vorhanden sind. Dabei lag der Fokus insbesondere auf Milch und Milchprodukten (Teuteberg/Anton 2023, S. 96 ff.). Abbildung 3.12 zeigt, wie umfangreich die Auswirkungen der ausgewählten Cyberangriffe auf die Versorgungssicherheit waren. Links sind solche Angriffe dargestellt, die abgewehrt werden konnten oder keine Folgen für das Unternehmen hatten. Rechts sind diejenigen zu sehen, die Auswirkungen auf die Versorgungssicherheit hatten, also eine kurzfristige Unzugänglichkeit von Lebensmitteln nach sich zogen. Dabei ist zu sehen, dass vor allem Cyberangriffe auf Unternehmen der Nahrungsmittelverarbeitung sowie auf Logistik- und Handelsunternehmen zu einer kurzzeitigen Nichtverfügbarkeit der entsprechenden Produkte geführt haben. Es konnten allerdings kaum Cybersicherheitsvorfälle bei der Erzeugung von Lebensmitteln gefunden werden, die wirklich schwerwiegende Folgen für das operative Tagesgeschäft des Unternehmens oder sogar die Wertschöpfungskette, also die vor- und/oder nachgelagerten Unternehmen, nach sich zogen.

Abb. 3.12 Schweregrad von Cyberangriffen nach Wertschöpfungsstufen



Quelle: Teuteberg/Anton 2023, S. 142

3.3 Herausgehobene Trends

Um in Computersysteme einzudringen, benötigen Angreifer Schwachstellen in der IT-Infrastruktur, die für Angriffe ausgenutzt werden können. Diese Schwachstellen können beispielsweise durch Programmierfehler, unzureichende Konfiguration von IT-Produkten im Betrieb oder fehlkonfigurierte Sicherheitseinstellungen entstehen. Aufgrund der zunehmenden Komplexität von IT-Systemen und der modulareren Produktionsbedingungen sind Schwachstellen weit verbreitet. Mit der zunehmenden Vernetzung von Systemen wächst die Angriffsfläche für Cyberkriminelle. Außerdem treten auch immer häufiger Schwachstellen in vernetzten Geräten auf (BSI 2023, S. 33). Auch veraltete Technik, für die keine Updates mehr vorhanden sind (Hoffmann/Haas 2023, S. 22) und Sicherheitslücken offenlassen, stellen Einfallstore dar. Generell ist »IT-Sicherheit so gut, wie der Mensch, der die Systeme bedient« (BSI o. J.). Schwache Passwörter sowie fehlende Softwareupdates können ebenfalls Cyberangriffe erleichtern. Eine Aufschlüsselung typischer Gefährdungen der Informationssicherheit in der Prozess-IT am Beispiel der Wasserwirtschaft ist im TAB-Arbeitsbericht Nr. 205 zu finden (TAB 2023, S. 222 ff.).

Cyberangriffe wurden in den vergangenen Jahren zunehmend komplex. Angriffe können verschiedenen Pfaden folgen, um die Erfolgschancen des Angriffs auf einen bestimmten neuralgischen Punkt in der Wertschöpfungskette zu erhöhen. So gelang es beispielsweise mit Stuxnet – ein 2010 entdecktes Schadprogramm zur Manipulation von Systemen zur Überwachung, Steuerung und Datenerfassung –, das Siemens Simatic S7 System zu infiltrieren, das zur Überwachung der Zentrifugen in der unterirdischen Atomanlage in Natanz im Iran eingesetzt wird (Stock 2024). Prozesse der Zentrifugensteuerung wurden durch Stuxnet manipuliert und die Manipulationen zeitgleich durch eine zusätzliche Manipulation von Sensoren verschleiert, weswegen der Angriff erst mit Verzögerung entdeckt wurde (Hoffmann/Haas 2023, S. 36).

Gleichzeitig wächst die Angriffsfläche durch die stetig zunehmende Digitalisierung, die Vernetzung von Systemen und ihre Verbindung mit dem Internet, wodurch Unternehmen und Prozesse angreifbar werden, die früher beispielsweise durch die physische Trennung von IT- und Betriebstechnologien geschützt waren. So wird es leichter möglich, durch einen Angriff auf einen Hersteller von Betriebstechnik zahlreiche kleinere und mittlere Unternehmen anzugreifen. Im mehrheitlich dezentral organisierten Sektor Landwirtschaft und Ernährung sind gleichzeitige Angriffe auf zahlreiche Unternehmen einer der möglichen Hauptwege, um die Versorgung mit Lebensmitteln bedeutsam zu stören. Blickt man auf das zukünftige Schadpotenzial sind drei Entwicklungen hervorzuheben: Supply-Chain-Angriffe, die Vereinfachung von Planung und Durchführung von Angriffen mittels KI und die neuen Herausforderungen, die

das Quantencomputing mit Blick auf die Cybersicherheit von Systemen mit sich bringen könnte.

Supply-Chain-Angriffe

Von einem Supply-Chain-Angriff spricht man, wenn Angreifer eine größere Anzahl von Betrieben stören, indem sie auf die Hersteller von Betriebstechnik abzielen. Bei einem solchen Angriff infiltrieren Angreifer nicht direkt das Hauptzielunternehmen, sondern greifen stattdessen Schwachstellen in den Systemen oder Prozessen von Drittanbietern an, die mit dem Hauptzielunternehmen digital vernetzt sind. Ein Beispiel für einen Supply-Chain-Angriff ist das Eindringen in die Systeme eines Lieferanten oder Subunternehmers, der Software oder Dienstleistungen für das Hauptzielunternehmen bereitstellt. Durch die Kompromittierung dieser Lieferanten können Angreifer Schadsoftware in die Software oder Dienste einschleusen, die dann unbemerkt in das System des Hauptzielunternehmens gelangen können, wenn es diese Software oder Dienste verwendet. Bei einem solchen Angriff kann beispielsweise ein Updatemechanismus eines legitimen Softwareanbieters genutzt werden, um bösartige Schadsoftware an Kunden zu verteilen (Teuteberg/Anton 2023, S. 108). Supply-Chain-Angriffe können aber auch auf die Hardware abzielen, indem einzelne zentrale Komponenten manipuliert werden. So können beispielsweise Chips gefälscht und verändert werden, um Hintertüren (Backdoors) einzubauen, über die dann später auf das System zugegriffen werden kann. Diese Backdoors sind zum Teil von außen völlig unauffällig und nur sehr schwer zu identifizieren. Das Problem gefälschter Chips hat in der COVID-19-Pandemie erheblich zugenommen (McCrea 2022). Wie verheerend die Auswirkungen von Supply-Chain-Angriffen auf ein weit verbreitetes Element bzw. die Software sein können, zeigt das Beispiel des Angriffs auf die Netzwerkmanagementsoftware Orion von SolarWinds (Kasten 3.1).

Kasten 3.2 Angriff auf SolarWinds

Ende 2020 wurde SolarWinds, ein großes US-amerikanisches Softwareunternehmen, von einer Hackergruppe namens Nobelium angegriffen. SolarWinds bietet Systemmanagementtools für die Netzwerk- und Infrastrukturüberwachung sowie andere technische Dienstleistungen für hunderttausende von Unternehmen weltweit an. Zu den Produkten des Unternehmens gehört das IT-Leistungsüberwachungssystem Orion. Durch Orion kann ein privilegierter Zugriff auf IT-Systeme erlangt werden, um Protokoll- und Systemleistungsdaten zu erhalten. Diese privilegierte Stellung und die weite Verbreitung machten SolarWinds zu einem attraktiven Ziel. Mehr als 30.000 öffentliche und private Organisationen einschließlich lokaler, staatlicher und

bundesstaatlicher Behörden nutzen Orion zur Verwaltung ihrer IT-Ressourcen. Als SolarWinds die Backdoorschadsoftware SUNBURST versehentlich zum Update für die Orion-Software auslieferte, wurden die Daten, Netzwerke und Systeme von tausenden Unternehmen kompromittiert (Oladimeji/Kerner 2023). Der Angriff diente Spionagezwecken (Kühl 2021). Wie viele Daten aus welchen Organisationen gestohlen wurden, ist nicht öffentlich bekannt.

Vereinfachte Angriffe durch KI

Je attraktiver ein Unternehmen für Hacker ist, desto mehr Angriffe werden verzeichnet. Ransomwareangriffe werden beispielsweise zurzeit von den Branchenexperten als größte Bedrohung empfunden, ihre Auswirkungen sind aber meist auf einzelne Unternehmen begrenzt. Durch die Fortschritte im Bereich der KI wird es leichter möglich, Angriffe zu planen und durchzuführen, die darauf abzielen, mehrere Akteure in der Wertschöpfungskette auszuschalten. Große Sprachmodelle, die u. a. auch zur Analyse und Generierung von Codes fähig sind, können dabei helfen, Schwachstellen in der Software deutlich einfacher und schneller zu identifizieren und auszunutzen (Eikenberg 2023). Die Erzeugung von Schadsoftware kann so mit nur geringem Aufwand automatisiert werden (Eikenberg 2023; Eikenberg/Königstein 2021, S. 14), beispielsweise indem aus einer groben Spezifikation von Schadcodes jeweils neue Varianten von Schadsoftware erzeugt werden (Schwartz 2023). Während die Komplexität und der Aufwand von Cyberangriffen seit 1980 kontinuierlich steigen, nimmt der dafür erforderliche Kenntnisstand hingegen schnell ab (dazu und zum Folgenden Hoffmann/Haas 2023, S. 52 ff. u. 59).

Große Sprachmodelle (Large Language Model – LLM) machen nicht nur die Erzeugung von Schadsoftware einfacher, auch das Phishing durch Identitätsfälschung kann mit ihrer Hilfe deutlich effizienter durchgeführt werden (Schirrmacher 2023). Textangriffe durch E-Mail können schneller erzeugt und ohne menschliche Interaktion gestreut werden (BSI 2023). Cyberkriminelle setzen zunehmend LLM-Technologie ein, um den individuellen Schreibstil zu imitieren und geschäftliche E-Mail-Kompromittierungen effektiver durchzuführen. Der Zugang zu den E-Mail-Nachrichten, z. B. eines Geschäftsführers, ist dafür ausreichend (Chaykin 2023; O'Flaherty 2024). Mit Deep-Voice-Technologie kann die Sprache von Entscheidungsträger/innen im Unternehmen nachgeahmt werden. Dies ist inzwischen schon mit wenigen Sekunden Tonmitschnitt möglich (Hoffmann/Haas 2023, S. 31). Diese Angriffsart wurde bereits in der Vergangenheit für den massiven Datenraub von Unternehmen im Energiesektor eingesetzt (Brewster 2021; Stupp 2019). Menschen können bereits mit den aktuell vorhandenen Technologien Sprachfälschungen nicht zuverlässig erkennen (Mai et al. 2023).

KI kann aber auch dabei helfen, Cybersicherheitspraktiken erheblich zu verbessern, indem sie zur Abwehr von Cyberangriffen eingesetzt wird. Große Sprachmodelle können dafür genutzt werden, Bedrohungen und Anomalien zu erkennen, und können so die Fähigkeit erhöhen, Angriffen zu widerstehen (Taddeo et al. 2019). Dafür wird eine Software darauf trainiert, normale (zulässige) von unnormaler (bösartigen) Netzwerkkommunikation zu unterscheiden, um möglichst viele Angriffe zu erkennen und ggf. auch abzuwehren bei gleichzeitig minimaler Anzahl von Fehlalarmen (Hoffmann/Haas 2023, S. 61). Auch Schutzmethoden und Best Practices zu recherchieren oder Phishingmails automatisch auszusortieren, wurde durch große Sprachmodelle einfacher (Eikenberg 2023). Perspektivisch könnte eine KI-Lösung darauf trainiert werden, Anomalien in Sprachmustern zu erkennen, um Manipulationsversuche von Stimmauthentifizierungs- und Gesichtserkennungsverfahren aufzudecken (Fitzmaurice 2024).

Quantencomputing

Perspektivisch könnte nicht nur KI, sondern auch das Quantencomputing eine größere Herausforderung für die Cybersicherheit in Landwirtschaft und Ernährung darstellen. Quantencomputing bezieht sich auf die Verwendung von Quantenmechanikprinzipien, um Computer zu entwickeln, die auf Quantenbits anstelle von klassischen Bits basieren. Im Gegensatz zu klassischen Computern, die Bits als 0 oder 1 darstellen, können Qubits aufgrund von Quantenüberlagerung und Verschränkung gleichzeitig Zustände von 0 und 1 einnehmen. Das ermöglicht Quantencomputern, bestimmte Berechnungen viel schneller durchzuführen als herkömmliche Computer. Mit der Entwicklung leistungsstarker Quantencomputer könnten mathematische Probleme, die klassischen Verschlüsselungsalgorithmen zugrunde liegen und derzeit zur Sicherung von IT-Systemen weit verbreitet sind, leicht lösbar werden. Dies würde die Vertraulichkeit und Integrität von Daten gefährden, die in cyberphysischen Systemen verarbeitet werden (Paul et al. 2022). Zwar wurde die Quantentechnologie bis heute noch von niemandem komplett durchdrungen (Pohlink 2022) und es könnte noch Jahrzehnte dauern, bis Quantencomputing einen bedeutsamen kommerziellen Nutzen erreicht (Bongs et al. 2023, S. 673). Befürchtet wird aber, dass Cyberkriminelle jetzt schon Daten sammeln, die auf klassischer Kryptografie beruhen, um sie später entschlüsseln zu können. Deshalb arbeiten viele IT-Unternehmen (z. B. Apple) an Verschlüsselungsmethoden (bzw. führten sie schon ein), um die Daten sicherer zu machen.

4 Gefährdung der Versorgungssicherheit

Auf Basis einer umfangreichen Dokumentenanalyse, ergänzt um eine empirische Erhebung, untersuchten Teuteberg und Anton (2023) und Hoffmann und Haas (2023), wie sich ein Ausfall von IT-Systemen auf die Produktion und Verteilung von Lebensmitteln auswirken könnte und inwiefern ein solcher Ausfall eine Gefährdung für die Nahrungsmittelversorgung insgesamt darstellen könnte (zur Methodik der beiden Gutachten siehe Kasten 4.1). Wie in Kapitel 3 dargelegt, zeigt die Analyse von internationalen Vorfällen, zu denen Informationen öffentlich-zugänglich sind, dass die Angriffe zu etwa 70 % rein exploitativer Natur waren. Lediglich ca. 30 % der Angriffe hatten disruptive Folgen für den operativen Betrieb (Teuteberg/Anton 2023, S. 81). Im Folgenden werden die Ergebnisse aus beiden Gutachten zusammengefasst, mit besonderem Fokus auf Angriffe mit disruptiven Folgen. Dabei wird nach Landwirtschaft, Verarbeitung, Logistik und Handel differenziert.

Kasten 4.1 Methodische Vorgehensweise der Gutachterteams

Neben der quantitativen Analyse von Cybersicherheitsvorfällen (Kasten 3) analysierten sowohl Teuteberg und Anton (2023) als auch Hoffmann und Haas (2023) Cybervorfälle qualitativ, um genauer zu erarbeiten, welche direkten Auswirkungen ein Ausfall von zentralen IT-Systemen auf die zentralen Aufgaben einzelner Wertschöpfungsstufen haben kann. Die 30 von Teuteberg und Anton (2023) untersuchten Fälle erstrecken sich von der Produktion über Verarbeitung und Logistik bis hin zum Handel. Die Gutachter wählten insbesondere Beispiele, die im Zusammenhang mit der Erzeugung, dem Transport und dem Handel von Milch und Milchprodukten in Zusammenhang stehen. Dabei ist anzumerken, dass sich die Auswirkungen schlecht erfassen lassen. In fast allen Fällen sind keine Details dazu bekannt, ob das jeweilige Unternehmen Lösegeld zahlte. Hoffmann und Haas (2023) führten eine Literaturanalyse sowie 19 Leitfadeninterviews mit Unternehmensexperten (vor allem IT-Verantwortliche) und Branchenvertretern durch. Auf dieser Basis wurden Risikoelemente der IT in den digitalen Produkten und Services identifiziert. Daraus wurden Szenarien für hypothetische, aber realistische (auch komplexe) Angriffe und deren Auswirkung auf die Lebensmittelversorgung entwickelt sowie deren Eintrittswahrscheinlichkeit und Schadenspotenzial bewertet.

4.1 Landwirtschaftliche Produktionssysteme

Informationen zu Angriffen auf landwirtschaftliche Betriebe wurden bisher nicht in großer Anzahl publiziert. Das liegt vermutlich daran, dass die Landwirtschaft bisher nicht das Hauptziel ausgeklügelter Angriffe auf die Betriebstechnologien war. Da weltweit keine einheitlichen Meldepflichten für Cyberangriffe existieren, ist allerdings von einer global hohen Dunkelziffer an getätigten und nicht publizierten Angriffen auf landwirtschaftliche Infrastruktur auszugehen (Hoffmann/Haas 2023, S. 28 u. 32). Die Analyse von Teuteberg und Anton (2023) ergab, dass bis Januar 2019 – dem Zeitpunkt der von ihnen herangezogenen Befragungsdaten – mehr als zwei Drittel der deutschen Landwirtschaftsbetriebe Opfer eines Cyberangriffs wurden (Teuteberg/Anton 2023, S. 88).

Potenzielle Angriffsziele auf landwirtschaftliche Betriebe betreffen alle IT-Systeme, die dort eingesetzt werden. Es können Sensornetzwerke, landwirtschaftliche Maschinen und Fahrzeuge oder einzelne digitalgesteuerte Systeme betroffen sein (Haas/Hoffmann 2020). Mit Blick auf IT-Netzwerke landwirtschaftlicher Betriebe wird davon ausgegangen, dass tendenziell wenige Schutzvorkehrungen vorhanden sind, weswegen Einfallstore existieren, die leicht ausgenutzt werden können (Teuteberg/Anton 2023, S. 46).

Angriffe auf einzelne landwirtschaftliche Betriebe bzw. ihre IT-Netzwerke und Technologien, beispielsweise bei einem Ransomwareangriff, führen in der Regel nicht zu Lieferengpässen (Teuteberg/Anton 2023, S. 53). Denn die Erzeugung landwirtschaftlicher Produkte ist stark dezentral organisiert, was einen grundsätzlichen Schutz gegen Cyberangriffe darstellt (Teuteberg/Anton 2023, S. 143). 2023 zählte das Statistische Bundesamt (Destatis 2024) etwa 255.000 landwirtschaftliche Betriebe. Der Ausfall der Produktion bei einem Betrieb lässt sich in der Regel entsprechend leicht von Mitbewerbern abfedern. In den meisten Fällen ist nicht mit bedeutsamen Auswirkungen auf die Lebensmittelversorgung zu rechnen. Gezielte Angriffe auf einzelne landwirtschaftliche Betriebe sind für Angreifer aus diesem Grund wenig attraktiv, wenn eine größere Schadwirkung hervorgerufen oder angedroht werden soll.

Eher ist davon auszugehen, dass landwirtschaftliche Betriebe von einem Angriff auf die Hersteller der von ihnen eingesetzten Betriebstechnik (Hoffmann/Haas 2023, S. 52) oder auf extern beauftragte Dienstleister mit hoher Marktstellung betroffen sein können. Angriffe auf Dienstleister, von denen viele kleine landwirtschaftliche Betriebe abhängen, könnten zu weitreichenden Auswirkungen führen und sich letztendlich sogar auf die Versorgungssicherheit auswirken, da zahlreiche Betriebe von einem solchen Ausfall zeitgleich betroffen wären (Teuteberg/Anton 2023, S. 143). Laut Teuteberg und Anton (2023, S. 128) kann ein Angriff auf IT-Systeme insbesondere dann weitreichende Auswirkungen haben, wenn:

- das IT-System standardgemäß in sehr vielen Betrieben oder zur Erbringung einer extern beauftragten Dienstleistung eingesetzt wird;
- das IT-System oder die Dienstleistung eine hohe Kritikalität aufweist, das heißt eine zentrale und kaum ersetzbare Funktion im Betrieb übernimmt;
- das System nur von wenigen Herstellern angeboten wird;
- das System die Verderblichkeit der Ware beeinflusst.

Bei welchen IT-Systemen sich ein Ausfall auf die Versorgungssicherheit auswirken könnte bzw. welche IT-Systeme dabei besonders schützenswert sind, wird anhand dieser Kriterien im Folgenden am Beispiel der Nutztierhaltung und des Pflanzenbaus diskutiert.

Nutztierhaltung

Die Nutztierhaltung und damit auch die Milcherzeugung und Fleischproduktion sind grundsätzlich hochempfindlich für Ausfälle. Werden die in Kapitel 2 dargestellten Anforderungen an die Herstellung von Produkten (z. B. Milch oder Fleisch) nicht eingehalten, können die Produkte schnell verderben bzw. nicht oder nur zu einem geringeren Preis auf dem Markt verkauft werden. Zur Erfüllung der unternehmenskritischen Aufgaben, wie beispielsweise Belüftung von Ställen, Tierfütterung oder Melken, werden IT-Systeme vielfach eingesetzt, wofür eine ununterbrochene Versorgung mit Strom und zunehmend auch Netzwerk- und Internetverbindungen unabdingbar sind (Nikander et al. 2020, S. 1 f.). Mit der Verbreitung digitaler Systeme und ihrer wachsenden Vernetzung wächst das Risiko von technischen Fehlfunktionen oder der Ausnutzung von Sicherheitslücken durch Angreifer (Teuteberg/Anton 2023, S. 44 f.).

Cyberangriffe auf einzelne Unternehmensnetzwerke von Milchviehbetrieben stellten bisher aufgrund der dezentralen Organisation der Tierhaltung bzw. Milcherzeugung kein unmittelbares Risiko für die Lebensmittelversorgung dar (Teuteberg/Anton 2023, S. 37). Anders sieht es bei Angriffen auf Dienstleister mit hoher Marktdurchdringung aus, deren Ausfall sich auf zahlreiche Betriebe der Nutztierhaltung auswirken kann. Dazu gehören IT-Dienstleister wie Cloudhostingplattformen, die Speicherplatz, Rechenleistung und Datenbanken zur Verfügung stellen (Teuteberg/Anton 2023, S. VI), sowie Anbieter cloudbasierter Systeme, wozu meist Farmmanagementsysteme gehören. Über die Cloud sind die Daten dauerhaft über das Internet verfügbar und grundsätzlich auch für Dritte zugänglich. Durch den Angriff auf die Cloudserver können zahlreiche Betriebe gestört und hohe Lösegeldforderungen für verschlüsselte Systeme gestellt werden (Hoffmann/Haas 2023, S. 52). Ähnlich problematisch wirkt der Ausfall von Internetdienstleistungen. Das zeigte der Angriff im Februar 2022 auf Viasat, ein US-amerikanischer Anbieter von Satelliteninternetdiensten. Viasat wurde Opfer eines Cyberangriffs auf sein Satellitennetzwerk KA-SAT. In der Folge wurden Satellitenbreitbanddienste wochenlang unterbrochen.

Milchviehbetriebe im Schwarzwald, die aufgrund ihrer abgelegenen Lage und der lokal nicht ausreichenden Internetverbindung auf Satelliteninternet angewiesen sind, konnten auf Daten zur Gesundheit und zum Wohlbefinden der Milchkühe wochenlang nicht mehr zugreifen. Der Internetausfall beeinträchtigte auch die tägliche Kommunikation mit der Molkerei, den Zugang zu Behördendiensten und die Erledigung alltäglicher Aufgaben, wie z. B. Abrechnungen und Antragstellung beim Landwirtschaftsamt (Baumann 2022).

Angriffe auf Anbieter von Labordienstleistungen können ähnliche Auswirkungen haben. So war National Milk Records, ein führender britischer Dienstleister in den Bereichen Milchqualität, Herdengesundheit und Genomtests, am 13. September 2019 von einem Ransomwareangriff betroffen. Der Angriff führte zu einem 1-wöchigen Ausfall vieler vom Unternehmen angebotener Dienstleistungen (James 2019a u. 2019b). Übergangsmaßnahmen mussten eingeführt werden, um Landwirt/innen die Ergebnisse der Labortestverfahren mitzuteilen, die von dem Virusangriff nicht betroffen waren.

Neben indirekten Angriffen auf Dienstleister mit hohem Marktanteil können auch solche IT-Systeme direkt angegriffen werden, die standardgemäß in der Nutztierhaltung eingesetzt werden und eine hohe Kritikalität aufweisen. Dazu gehört insbesondere die Robotertechnologie (dazu und zum Folgenden Teuteberg/Anton 2023, S. 42 u. 128). Wie jede Software kann auch die für die Steuerung der grundlegenden Funktionen des Roboters notwendige Software anfällig für Schadsoftware sein. Besonders kritisch sind dabei Stallbelüftungs- und Bewässerungssysteme sowie AMS in Milchviehbetrieben. Diese müssen kontinuierlich funktionieren – Ausfälle können innerhalb weniger Stunden fatale Folgen haben (Nikander et al. 2020, S. 3). Fällt das AMS aus, ist mit verzögerten Arbeitsabläufen im Milchviehbetrieb zu rechnen (Hanuschik/Moritz 2023, S. 6). Außerdem können potenzielle Gesundheitsprobleme der Tiere nicht mehr automatisch erkannt und die Milch der gesundheitlich beeinträchtigten und mit Medikamenten behandelten Tiere aussortiert werden, wodurch Medikamente in die Nahrungskette gelangen können (Teuteberg/Anton 2023, S. 88 u. 99).

Ein Einfallstor für Angreifer eröffnet sich beispielsweise über Schwachstellen bei der Fernwartung. Denn Robotersoftware wird häufig für die technische Wartung und den Support zugänglich gelassen, wodurch für Wartungszwecke eingesetzte Laptops, ggf. schwach geschützte Ports oder drahtlose Verbindungen von Angreifern ausgenutzt werden können (TÜV Rheinland 2019, S. 4 ff.). Werden die Systeme bzw. die Software nicht aktuell gehalten, kann das durch Angreifer ausgenutzt werden. Auch wenn bisher keine Vorfälle bei AMS registriert wurden, die Auswirkungen auf die Lebensmittelversorgung mit sich gebracht hätten, stellt ein flächendeckender Ausfall der Steuerung von AMS aufgrund ihrer Kritikalität, schwerer Ersetzbarkeit und hohen Verbreitungsgrads

wohl eine der gravierendsten Gefahren durch Cyberangriffe für die Versorgung mit Milchprodukten dar.

Ein Angriff auf weitere verbreitete Systeme in der Nutztierproduktion, wie Reinigungs- oder Herdenmanagementsysteme, wird hingegen aufgrund der geringeren Kritikalität bzw. Substituierbarkeit des Systems als weniger problematisch angesehen. Cyberangriffe auf Reinigungsroboter oder Fütterungssysteme wirken sich vergleichsweise weniger auf die Produktion aus, da ihr Ausfall durch den Rückgriff auf manuelle Methoden temporär bewältigt werden könnte (Baker/Green o. J., S. 30 f.; Grothmann et al. 2010; Sinnott et al. 2021). Auch ein Ausfall des Herdenmanagementsystems als zentrales Assistenzsystem würde zwar den Zugang zu Informationen über die Gesundheit der Milchkühe, Daten zum Haltungs-, Leistungs- und Fütterungsmanagement erschweren und einen größeren Aufwand bei der Nachverfolgung und Verwaltung der einzelnen Aufgaben mit sich bringen. Allerdings wird die Produktion bzw. Milcherzeugung dadurch in der Regel nicht direkt beeinträchtigt (Teuteberg/Anton 2023, S. 37 u. 41 f.).

Pflanzenbau

Im Vergleich zur Nutztierhaltung ist der Pflanzenbau von einer geringeren Kritikalität geprägt. Eine Unterbrechung der Getreideproduktion hätte beispielsweise kaum spürbare Auswirkungen auf die Versorgungssicherheit. Denn Getreide kann vergleichsweise gut und lange gelagert werden und hat einen im Vergleich zu Milchprodukten geringen Marktwert (Baker/Green o. J.). Zwar kommen auch in der Pflanzenproduktion verstärkt IT-Systeme zum Einsatz (Kap. 2), deren Ausfall Störungen im Betrieb verursacht. Allerdings verursachen solche Störungen nicht unmittelbar Ernteeinbußen. Werden beispielsweise Farmmanagementsysteme angegriffen und Daten manipuliert, könnte dies zwar zu fehlerhaften Produktionsprozessen führen (Hoffmann/Haas 2023, S. 52); z. B. können Ernteausfälle die Folge sein, wenn ein Pflanzenschutzmittel zu hoch dosiert wird (Hanuschik/Moritz 2023). Dennoch ist zu erwarten, dass die Fehlerhaftigkeit der Daten schnell auffällt, sodass die Dosierung manuell nachjustiert werden kann (Hoffmann/Haas 2023, S. 52). Ähnliches gilt für die Manipulation von Bewässerungssystemen, was vor allem Gefährdungspotenzial für Kulturen birgt, die stark von Bewässerung abhängig sind (z. B. Gemüseanbau). So wurde beispielsweise im Juli 2020 das Bewässerungssystem eines israelischen Unternehmens angegriffen, wodurch landwirtschaftliche Pumpen außer Betrieb gesetzt wurden. Regionale Schäden an den Kulturpflanzen und Teilausfälle in der Ernte waren die Folge (Hoffmann/Haas 2023, S. 32). Die Eintrittswahrscheinlichkeit eines solchen Falls wird für Deutschland unter den aktuellen klimatischen Bedingungen als niedrig eingestuft (Hoffmann/Haas 2023, S. 49). Insgesamt halten die im Rahmen des Gutachtens von Hoffmann und Hass

(2023, S. 7 u. 46) befragten Expert/innen orchestrierte Angriffe auf zeitkritische Prozesse (z.B. Ernte, Aussaat), die über Angriffe auf Farmmanagementsoftware oder Bewässerungssysteme durchgeführt werden, entsprechend für wenig wahrscheinlich und verbinden damit keine weitreichenden Auswirkungen auf die Nahrungsmittelversorgung (Hoffmann/Haas 2023, S. 7 u. 46).

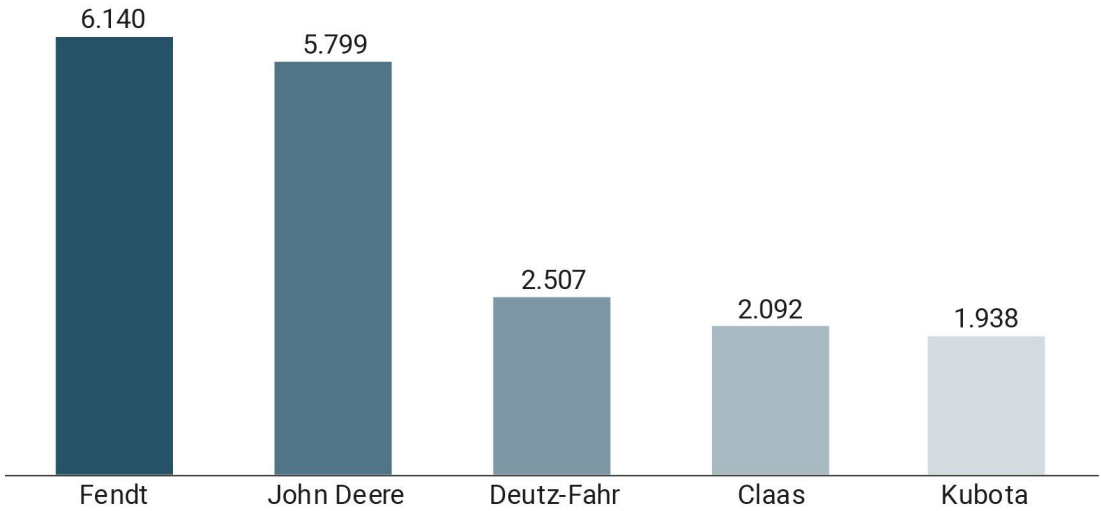
Hingegen sind auch in der Pflanzenproduktion, wie bei der Nutztierhaltung, Supply-Chain-Angriffe mit einem höheren Gefahrenpotenzial verbunden. Dazu gehören zum einen Angriffe auf Händler von Saatgut und Düngemitteln während der Aussaat- und Pflanzsaison, die in den USA vom Federal Bureau of Investigations (FBI 2022) vermehrt beobachtet wurden. Solche Angriffe in größerem Ausmaß hätten das Potenzial, die Versorgung mit Saatgut und Dünger bzw. die Getreideproduktion erheblich zu stören, was sich auf die gesamte Nahrungskette auswirken könnte. Sowohl die Düngemittel- und Stickstoff- als auch die Saatgutbranche weisen eine hohe Marktkonzentration auf und manche Produkte werden nur von wenigen Unternehmen angeboten (IBISWorld o. J.). Daher wäre zu erwarten, dass Angriffe auf wichtige Produktionsanlagen im Ausland die Versorgung in Deutschland auch stören könnten.

Als wahrscheinlich werden zum anderen Angriffe auf die Flotten von Landtechnikherstellern bzw. auf Landmaschinen eingeschätzt (Hoffmann/Haas 2023, S. 48). Die meisten modernen Maschinen verfügen über vernetzte Bordelektronik und sind in Telematiklösungen eingebunden. Angriffe auf einzelne landwirtschaftliche Maschinen sind also möglich. Fernwartungszugänge, die zunehmend für Landmaschinen angeboten werden (z. B. CLAAS o. J.), perspektivisch ggf. auch die Fernsteuerung per Handy (Göggerle 2024a), können Schwachstellen darstellen. Vor allem skalierte Angriffe auf Landtechnikhersteller, wodurch Traktoren mit digitaler Steuerungstechnik fahrunfähig gemacht werden können (Hanuschik/Moritz 2023, S. 6), sind mit größeren Risiken verbunden. In zeitkritischen Prozessen, wie der Ernte, wo ganze Landmaschinenflotten über wenige Wochen zeitgleich gebraucht werden, könnte sich ein solcher Angriff als hochproblematisch erweisen. Denn der optimale Erntezeitpunkt hängt von der Jahreszeit und der Witterung ab. Stehen die Erntemaschinen nicht rechtzeitig zur Verfügung, kann es zum Totalverlust für landwirtschaftliche Betriebe kommen (Pollmer 2017).

Auch bei der Landtechnik dominieren wenige Hersteller den Markt. Etwa 64 % der Neuzulassungen für Traktoren sind beispielsweise auf zwei Marken zurückzuführen (Abb. 4.1). Ein größerer Angriff, der auf eine ganze Landmaschinenflotte abzielen würde, könnte Softwareupdates als Einfallstor nehmen, um die Bordelektronik zu manipulieren. Dass Ortung und Lahmlegung zahlreicher Traktoren prinzipiell möglich sind, zeigte der Hersteller John Deere, der Maschinen aus seinem Sortiment ferngesteuert deaktivierte, nachdem sie in der Ukraine von russischen Soldaten gestohlen worden waren (Tangalakis-Lippert 2022). Auch wenn laut Hoffmann und Haas (2023) aktuell keine umfangreichen

Auswirkungen auf die Nahrungsmittelversorgung zu erwarten sind, da auf vielen Betrieben noch ältere, nicht vernetzte Maschinen im Einsatz sind, steigt das Risiko mit der zunehmenden Verbreitung moderner Landmaschinen.[16] Der technische Aufwand, der für einen solchen Angriff betrieben werden müsste, wird allerdings als vergleichsweise hoch eingeschätzt. Der Grund dafür ist, dass Landtechnikhersteller für ihre Landmaschinen die hohen Cybersicherheitsstandards aus der Automobilindustrie übernehmen können. Ein entsprechender Standard wird derzeit erarbeitet.

Abb. 4.1 Anzahl der neu zugelassenen Traktoren der führenden Marken in Deutschland 2023



Eigene Darstellung nach Göggerle 2024b

Auch wenn die Angriffsfläche im Pflanzenbau durch die Digitalisierung der Landwirtschaft zunehmend größer wird, verringern die dezentrale Organisation der Branche und die Vielzahl der eingesetzten Systeme im Vergleich zur zentralen Organisation und größeren Homogenität der Systeme in der Logistik und im Handel die mögliche Reichweite von Cyberangriffen. Gravierende Einschränkungen der Nahrungsmittelversorgung durch Störungen landwirtschaftlicher Systeme wären eher von einer Störung der zentralen Wasser- oder Energieversorgung zu erwarten (Hoffmann/Haas 2023, S. 53). Grundsätzliches zu den Auswirkungen eines Stromausfalls auf die Nahrungsmittelversorgung findet sich im TAB-Arbeitsbericht Nr. 141 (TAB 2010, S. 138 ff.).

16 Dasselbe gilt für die Feldrobotik, die jedoch kaum in der Praxis angekommen ist (Hoffmann/Haas 2023, S. 13, 22 u. 48).

4.2 Verarbeitung

In der Landwirtschafts- und Nahrungsmittelverarbeitung waren mit 71,7% mehr als zwei Drittel der Unternehmen 2019 Opfer von Cyberangriffen gewesen – so eine Befragung, die zwischen August 2018 und Januar 2019 mit 5.000 deutschen Unternehmen branchenübergreifend durchgeführt wurde (Teuteberg/Anton 2023, S. 88) (dazu auch Kasten 3.1). Im Vergleich zu einem Ausfall der Technik in der Landwirtschaft kann ein Ausfall der Technik bei der Verarbeitung von Lebensmitteln schneller weitreichende Auswirkungen haben. Grund dafür ist, dass viele kritische Prozesse der Verarbeitung von einer hohen Abhängigkeit von IT-Systemen geprägt sind. Zu den Prozessen, die eine besonders hohe Kritikalität aufweisen, gehören die Bedarfs- und Produktionsplanung, die Eingangslogistik, die Produktion und die Ausgangslogistik (BVE 2020, S. 8 ff.). Die Verwaltung der Bestände und Produkte folgt dem First-in-first-out(FiFo)-Prinzip. Das bedeutet, dass die Produkte, die zuerst eingelagert wurden, zuerst verarbeitet bzw. verkauft werden (BWL-Lexikon o. J.). Dafür ist eine Unterstützung durch digitale Systeme von zentraler Bedeutung. Ohne Zugang zu den zentralen Systemen und dabei insbesondere zum Warenwirtschaftssystem können die erforderlichen Dienste schnell nicht mehr erbracht werden. Ein Ausfall des Warenwirtschaftssystems würde beispielsweise zu einem Stillstand der Produktion innerhalb kürzester Zeit führen (Teuteberg/Anton 2023, S. 129 f.). Hält der Ausfall länger an, können Kontaminationen oder Fehlverarbeitungen resultieren bzw. die Waren können verderben (Teuteberg/Anton 2023, S. 52). Aus diesen Gründen werden Ausfälle eines Warenwirtschaftssystems im Schlacht- und Zerlegebetrieb mit einer mittleren Eintrittswahrscheinlichkeit und mittleren Auswirkungen eingeschätzt (Hoffmann/Haas 2023, S. 47). Wie ein einfacher Angriff auf die Computersysteme weitreichende Auswirkungen auf die Produktion haben kann, zeigte 2021 ein Angriff auf die drittgrößte Molkerei Österreichs SalzburgMilch (Kasten 4.2).

Ob sich Produktionsausfälle auf die Ernährungssicherheit auswirken, hängt vor allem auch von der Verderblichkeit der betroffenen Produkte ab. Besonders bei frischen Lebensmitteln (z. B. Rohmilch) können Produktionsausfälle aufgrund begrenzter Lagermöglichkeiten ein größeres Problem darstellen. Ausfälle, die Produkte mit längerer Haltbarkeit betreffen oder solche, die sich besser lagern lassen oder keine Grundnahrungsmittel sind, verursachen geringere Auswirkungen auf die Nahrungsmittelversorgung der Gesamtbevölkerung bzw. es können zunächst die größeren Lagerbestände genutzt werden, bevor es zu Lieferengpässen kommt. Dazu gehören beispielsweise Zucker oder Bier.

Kasten 4.2 Ransomwareangriff auf SalzburgMilch

Am 22. Juni 2021 wurde SalzburgMilch, Österreichs drittgrößte Molkerei, Opfer einer Ransomwareattacke. Der Angriff führte zu einem Ausfall aller Computer in der Produktionshalle. Passwörter funktionierten nicht, eine Wiederherstellung der Systeme war unmöglich und der Zugang zu IT-Systemen, File- und Mailservern, Buchhaltung, Logistik und Lager war gesperrt. Es erschien lediglich die Nachricht »SalzburgMilch, you are fucked.« mit einem Link zum Darknet, einem Ultimatum und dem Angebot, das System wiederherzustellen und die Daten gegen ein Lösegeld in Kryptowährung zu entschlüsseln (Hofer 2022). Durch den Ausfall der Computer in der Produktionshalle fielen alle unterstützenden Prozesse zur Sammlung und Verarbeitung von Milch – bis auf die Abfüllung – aus. Bis zur Rückkehr zum Normalbetrieb dauerte es 1 Woche. Insgesamt 400 Mitarbeiter/innen waren damit beschäftigt, Server, Arbeitsgeräte und Laptops neu einzurichten (Hofer 2022).

Quelle: Teuteberg/Anton 2023, S. 109

Anbieter von Verpflegungskonzepten, deren Kunden (z. B. Krankenhäuser, Pflegeheime, Schulen) auf die tägliche Bereitstellung von Mahlzeiten angewiesen sind, unterliegen einem höheren Druck bei Produktionsausfällen (Teuteberg/Anton 2023, S. 131). Das zeigt der Cyberangriff auf das US-amerikanische Unternehmen HP Hood Dairy, einer der größten Hersteller von Molkereiprodukten in New England. Das Unternehmen beliefert Schulen mit Milch in Großpackungen. Im März 2022 erlitt es einen Cybersecurityvorfall und seine landesweit 13 Fabriken mussten in der Folge für 1 Woche geschlossen werden. Die Verpackung von Milch sowie die Herstellung von Milchprodukten wurden dadurch komplett und plötzlich unterbrochen (Gardizy 2022). Die Lieferunterbrechungen betrafen mehrere Schulbezirke in New England (JGPR 2022).

Zwar kann ein Angriff auf die Büro-IT, beispielsweise über einen Angriff auf Warenwirtschaftssysteme, nur indirekt zu Einbußen in der Produktion führen, dennoch werden Kaskadeneffekte auf die Produktion durch die zunehmend enge Kopplung der Planungs- und Produktionsprozesse immer wahrscheinlicher. Mit fortschreitender Digitalisierung der Produktionsprozesse werden IT-gestützte Planungsprozesse (Büro-IT) und die IT-gestützten Produktionsprozesse bzw. operativen Technologien (Prozess-IT) immer stärker miteinander vernetzt (Teuteberg/Anton 2023, S. 6). Beispielsweise sind Warenwirtschaftssysteme teilweise im selben Netzwerk wie industrielle Steuerungssysteme integriert (Teuteberg/Anton 2023, S. 129 f.). Die Tendenz zur Vernetzung von Systemen gilt auch für die Vernetzung von Prozess-IT mit dem Internet, z. B. über den Zugriff auf Clouddienste zur Speicherung von Daten in Produktionssyste-

men. Auch die Fernwartung mit Smartphone und Tablets spielt in den Produktionssystemen inzwischen eine wesentliche Rolle (Teuteberg/Anton 2023, S. 129). So wird die Prozess-IT zunehmend auch durch die Schwachstellen und Angriffsszenarien der klassischen IT angreifbar. Angreifer können die Verbindung zwischen diesen Systemen ausnutzen, um unbefugten Zugriff auf sensible Daten zu erlangen oder kritische Betriebsabläufe zu stören. Die Angriffsfläche für Cyberkriminelle steigt und damit die Risiken für die Produktion sowie die Lieferketten (Hoffmann/Haas 2023, S. 37; Teuteberg/Anton 2023, S. 6).

Eine Sperrung des Zugriffs auf die IT-Systeme stellt das größte Risiko dar. Datenmanipulationen über die Prozess-IT, beispielsweise bei der Beimischung von Gewürzen, der Erhitzung zur Haltbarkeitsmachung oder bei komplexen Verpackungsprozessen sind hingegen weniger besorgniserregend. Denn der Aufwand für Angreifer wäre so hoch, dass die Wahrscheinlichkeit eines solchen gezielten Angriffs gering ist – so die Einschätzung der von Hoffmann und Haas (2023, S. 37) befragten Expert/innen aus der Lebensmittelindustrie. Außerdem wird die Lebensmittelproduktion streng kontrolliert und solche Manipulationen würden im Rahmen von International-featured-Standard-Food(IFS)-Audits auffallen (Hoffmann/Haas 2023, S. 36 ff.).

Angesichts der steigenden Zahl von Angriffen auf die Prozess-IT ist es von entscheidender Bedeutung, umfassende Sicherheitsmaßnahmen zu implementieren (Claroty 2023, S. 4; Dragos 2023, S. 6). Allerdings wurde ursprünglich bei der Entwicklung von operativen Technologien Cybersicherheit häufig nicht als vorrangiges Anliegen berücksichtigt. In der Regel wurden operative Technologien durch eine Luftlücke geschützt, was bedeutet, dass sie physisch isoliert und nicht mit dem Internet verbunden waren. Sobald sie jedoch mit der Außenwelt verbunden werden, sind sie neuen Risiken ausgesetzt (Fortinet Inc. 2021). In den vergangenen Jahren konzentrierten sich Angriffe mit Schadsoftware gegen produzierende Unternehmen zunehmend auf industrielle Steuerungssysteme bzw. Prozess-IT (Claroty 2023, S. 4; Dragos 2023, S. 6). Ein Beispiel dafür ist der gezielte Angriff auf die Betriebstechnologie des brasilianischen Fleischverarbeiters JBS S.A. im Jahr 2021, der dessen gesamte nordamerikanische und australische Fleischproduktion lahmlegte (Kasten 4.3).

Besonders bedrohlich für die Versorgungssicherheit sind Angriffe auf Unternehmen, die als zentrale Anlaufpunkte für Produkte fungieren, z. B. eine Molkerei, die die Milch zahlreicher Milcherzeuger sammelt. Solche Unternehmen haben eine erhöhte Bedeutung für die Versorgungssicherheit. Die zentrale Rolle solcher Unternehmen innerhalb der Wertschöpfungskette führt im Fall eines Ausfalls zu erheblichen Konsequenzen für vor- und nachgelagerte Abschnitte, was sogar in der Vergangenheit zu kurzfristiger Unzugänglichkeit von Lebensmitteln führte. Starke Marktkonzentrationen geben Hinweise auf mögliche Schwachstellen (Kasten 4.4).

Kasten 4.3 Ransomwareangriff auf JBS S.A.

Die brasilianische JBS S.A. ist das weltweit größte fleischverarbeitende Unternehmen, das etwa ein Fünftel des weltweiten Fleischbedarfs abdeckt (Rinder, Hühner, Schweine). JBS wurde am 31. Mai 2021 von einem Ransomwareangriff getroffen, der zu einer 5-tägigen Einstellung des Gesamtbetriebs in Nordamerika und Australien führte (Hardy/Larson 2021). Das U.S. Department of Agriculture rief offiziell andere Produzenten dazu auf, ihre Fleischproduktion zu erhöhen. Der genaue Angriffsvektor konnte nicht festgemacht werden. Vermutet wird ein fehlgeschlagener Fernzugriff auf die Rechner und durchgesickerte Anmeldedaten von Mitarbeiter/innen. Bei dem Angriff wurden Daten exfiltriert und die IT-Systeme des Unternehmens verschlüsselt. Die Beweggründe für den Angriff blieben unklar, wobei die US-Regierung bestätigte, dass REvil, eine auf Ransomware spezialisierte Hackergruppe, für den Angriff verantwortlich war (Sherstobitoff 2021). JBS zahlte ein Lösegeld in Höhe von 11 Mio. US-Dollar in Bitcoin, um Kunden- und Lieferanten- sowie andere Daten zu schützen (Hardy/Larson 2021).

Quelle: Teuteberg/Anton 2023, S. 103

Kasten 4.4 Marktkonzentration in der Nahrungsmittelverarbeitung

Fleisch: Eine sehr starke Konzentration ist bei Schlacht- und Zerlegebetrieben zu beobachten. Bei Schweinen schlachten die 3 größten Unternehmen in Deutschland 59 % der Tiere (darunter Tönnies, Westfleisch und die VION Food Group). Die 10 größten haben zusammen einen Marktanteil von 81 % (DBV 2023). Bei Geflügel und Rind sind ähnliche Verhältnisse zu beobachten. Die 10 größten Betriebe schlachten 77 % der Rinder (DBV 2023). Die Geflügelwirtschaft in Deutschland ist ebenfalls stark konzentriert. Die 4 umsatzstärksten Unternehmen der Branche verfügen über ca. 50 % Marktanteil (LZ 2023) (Hoffmann/Haas 2023, S. 16 f.).

Getreide: Geerntetes Getreide fließt zwar in sehr unterschiedliche Produktionsprozesse ein, weswegen eine Vielfalt an Akteuren zu verzeichnen ist. Allerdings sind im mengenmäßig größten Bereich der Mühlen große Konzentrationsprozesse zu verzeichnen, mit im Jahr 2020 nur noch 550 produzierenden Mühlenbetrieben, die insgesamt ca. 8 Mio. t Getreide pro Jahr vermahlen (VDM o. J.). Die 13 größten Mühlenbetriebe in Deutschland decken mehr als 40 % des Marktes ab (Hoffmann/Haas 2023, S. 15).

Milchverarbeitung: Deutschland ist mit einem Anteil von über 20 % der größte Produzent und Verarbeiter von Milch in der Europäischen Union (Statista 2024). Für die Erzeugung und Vermarktung von Rohmilch, behandelter

Milch und Erzeugnissen auf Milchbasis ist in Deutschland eine große Zahl von Betrieben zugelassen (insgesamt 1.416; Stand März 2023). Es gibt sowohl eine Reihe großer, industrieller Molkereien als auch kleine, lokale Betriebe. Bei etwa einem Sechstel der Zulassungen handelt es sich um Betriebe mit über 50 Mitarbeiter/innen. In den letzten Jahren hat sich ein Trend zur Fusionierung von Molkereien abgezeichnet, was letztendlich zu einem Rückgang der genossenschaftlichen Molkereien führte (Milchindustrie-Verband e. V. o. J.). Diese Entwicklung wird durch die zunehmende Technologisierung in den Unternehmen verstärkt, die hohe Investitionen erfordert und von kleineren Unternehmen oft nicht getragen werden kann (Schrode et al. 2019, S. 23).

Quelle: Teuteberg/Anton 2023, S. 27 f.

Dies macht nicht nur der Angriff auf JBS deutlich, sondern auch der Angriff auf das US-amerikanische milchverarbeitende Unternehmen Schreiber Foods, den Teuteberg und Anton (2023, S. 98 ff.) näher untersuchten: Schreiber Foods wurde im Oktober 2021 von einer Cyberattacke getroffen, die zum Ausfall aller Systeme und zur temporären Schließung aller Unternehmensstandorte führte. Durch den Angriff kam es zu einem Rückstau von Milch in den Produktionsanlagen sowie zum Verkauf mit Preisnachlässen auf dem Markt und Mindereinnahmen (Shepel 2021). Die Frischkäseproduktion ging im Oktober 2021 im Vergleich zum Vorjahr um 6,9 % zurück, was zum Teil auf den Angriff zurückzuführen war, und führte zu leeren Regalen in Supermarktketten (McKay 2021).

Perspektivisch dürfte sich durch die Vernetzung und (oft drahtlose) Kommunikation zwischen einzelnen Komponenten die Zahl der möglichen Angriffsvektoren für Cyberattacken erhöhen (Ashibani/Mahmoud 2017; Sen 2018). Denn jeder Knoten im Netz stellt einen potenziellen Angriffspunkt dar, der das gesamte System beeinflussen kann (Nourian/Madnick 2018). Bei dem Beispiel des Computerwurms Stuxnet wurden beispielsweise zentrale Softwarekomponenten des industriellen Steuerungssystems, also der Prozess-IT, angegriffen – mit weitreichenden Auswirkungen (Nourian/Madnick 2018, S. 7 f.).

4.3 Logistik

Angriffe auf IT-Systeme zur Unterstützung von Logistikprozessen wurden von den von Hoffmann und Haas (2023, S. 54) befragten Expert/innen als besonders schwerwiegend eingestuft. Denn die Logistik stellt unter Umständen einen neuralgischen Punkt in der Versorgungskette dar. Beeinträchtigungen der Logistiksysteme können zu Störungen im Transport- und Abfertigungsprozess führen (Hoffmann/Haas 2023, S. 54), was wiederum Lieferengpässe und eine Beeinträchtigung der Produktverfügbarkeit zur Folge haben kann (Teuteberg/Anton

2023, S. 136). Kritisch ist vor allem ein Ausfall zentraler Verwaltungssysteme, wie Warenwirtschafts- oder Lagerverwaltungssysteme, wodurch z. B. keine Aufträge im Logistiklager mehr abgearbeitet werden können.

Dass Störungen schnell weitreichende Auswirkungen haben können, liegt auch an der wachsenden Vernetzung von Systemen. Jede neue Technologie, die den Vernetzungsgrad von Anlagen und Systemen erhöht, erhöht zugleich auch die Cyberrisiken für die Logistik (Cheung et al. 2021, S. 1). Dies gilt heute besonders für IoT-Anwendungen und Cloudcomputing, künftig auch für die Verbreitung von digitalen Zwillingen, VR- und AR-Anwendungen sowie den Einsatz von Drohnen. Außerdem erfolgt die Vernetzung von Systemen nicht nur innerhalb eines Unternehmens, sondern auch zwischen Handelspartnern entlang der Wertschöpfungskette. Auch dies birgt neue Risiken für Logistikunternehmen, denn Vorfälle durch schwache Cybersicherheitsmaßnahmen bei einem Lieferanten können sich schneller als in der Vergangenheit auf seine Partner in der Lieferkette ausbreiten (Melnyk et al. 2022, S. 165 f.). Der wachsende Zugriff auf Clouddienste für die Speicherung von Daten auch zwischen Handelspartnern wird in dieser Hinsicht als besonders problematisch angesehen (Hoffmann/Haas 2023, S. 55). Blockchaintechnologien, die zunehmend in Wertschöpfungsketten eingesetzt werden, werden häufig als inhärent sicher gepriesen und bisher tendenziell als robuster gegen Missbrauch eingeschätzt. Allerdings werden blockchainbasierte Systeme auch zunehmend zu attraktiven Zielen für Cyberkriminalität (Schlatt et al. 2023).

Dass Störungen weitreichende Konsequenzen haben können, liegt auch daran, dass sie sich im Transport- und Abfertigungsprozess kurzfristig nicht immer einfach beheben lassen. Viele Logistikprozesse werden für eine Just-in-Time-Lieferung der Lebensmittel gestaltet (Hoffmann/Haas 2023, S. 51). Das heißt, Lieferungen werden so synchronisiert, dass Waren in der exakten Menge und zum richtigen Zeitpunkt an den richtigen Ort gelangen, um den Produktionsprozess ohne Verzögerungen oder Überbestände aufrechtzuerhalten. Dies erfordert eine enge und digital gestützte Zusammenarbeit zwischen Lieferanten, Herstellern und ggf. auch Vertriebspartnern. Den Ausgangspunkt dafür stellen Bestellungen über digitale Kassensysteme dar (Kap. 2.4). Durch die Implementierung von Just-in-Time-Prozessen können Unternehmen ihre Kapitalbindung in Lagerbeständen reduzieren, die Produktionskosten senken und gleichzeitig die Liefergeschwindigkeit und -qualität verbessern. In Situationen, in denen die Versorgungsketten normal funktionieren, kann der Ressourcenfluss dadurch stark optimiert und Lebensmittelverluste minimiert werden. Diese Optimierung kann allerdings dazu führen, dass an keinem Knotenpunkt des Netzes Redundanz vorhanden ist. Zwar wird dies unter dem Gesichtspunkt der Effizienz häufig als vorteilhaft angesehen, jedoch würde sich ein Ausfall in einem Teil des Netzes auf das gesamte (komplexe) Netz ausbreiten und zu Kaskadeneffekten an anderen Stellen der Lieferkette führen (Garnett et al. 2020, S. 316). Fehlende

Redundanzen erhöhen die Vulnerabilität des Systems (IPES-Food & ETC Group 2021; Wolfangel 2021) und bergen ein erhöhtes Sicherheitsrisiko für die Versorgungssicherheit. Bisher haben keine der von Teuteberg und Anton (2023) analysierten Angriffe auf Logistikdienstleister oder Lieferdienste die Versorgungssicherheit mit Lebensmitteln maßgeblich gestört. Einzig bei der Ransomwareattacke auf den niederländischen Logistikdienstleister für Supermärkte Bakker Logistiek wurde von konkreten Lieferengpässen berichtet. Der Angriff fand im April 2021 statt und störte den Transport und die Abfertigung von Lebensmitteln. Kundenbestellungen konnten nicht mehr entgegengenommen und Transportrouten nicht wie gewohnt geplant werden. Von Lieferengpässen waren vor allem Käseprodukte in den Handelsfilialen der größten niederländischen Supermarktkette Albert Heijn betroffen.

Eine hohe Eintrittswahrscheinlichkeit und potenziell große Auswirkungen haben laut Einschätzung der von Hoffmann und Haas (2023, S. 45) befragten Expert/innen Angriffe auf *Kühlungssysteme* (Kühltransporter und -häuser). Denn an diversen Stellen der drei Wertschöpfungsketten Getreide, Fleisch und Gemüse kommen Kühltransporter oder Kühlhäuser zum Einsatz. Ein skalierter Angriff auf diese Kühlsysteme hätte massive Ausfälle zur Folge, da die Produkte schnell verderben würden und vernichtet werden müssten. Einfallstore könnten z. B. die Telemetrie (Telematiksysteme) in Kühl-LKWs oder die Fernwartung bei Kühlhäusern sein (Hoffmann/Haas 2023, S. 55). Ein Ausfall von temperaturgeführten Lagern und Transportdienstleistungen kann sofortige Auswirkungen auf die Genießbarkeit der Produkte haben, wie der Angriff auf Americold im November 2020 illustriert. Americold ist ein US-amerikanischer Betreiber von temperaturkontrollierten Lagerhäusern und Transportdienstleistungen u. a. für Lebensmittel. Im November 2020 wurde das Unternehmen Opfer eines Ransomwareangriffs auf sein Netzwerk. Das gesamte IT-Netzwerk nebst Telefonsystem, E-Mail, Bestandsverwaltung und Auftragsabwicklung war von dem Vorfall betroffen (Muncaster 2020; Seals 2020). Kunden, die versuchten, Bestände zur Auslieferung abzuholen, erhielten keinen Zugang zu den Lagern (Abrams 2021). Die Verbindung zu den Geschäftspartnern in der Lieferkette ist oft das schwächste Glied in der Cybersicherheitsstruktur eines Unternehmens, wenn die Geschäftspartner Zugang zu den Systemen und Daten des Unternehmens haben, selbst aber nur über schwache Cybersicherheitsmaßnahmen verfügen. Dies kann zu Schwachstellen führen, die von Angreifern ausgenutzt werden können. Es ist daher wichtig, die Integrität der Cybersicherheitsmaßnahmen und die Bereitschaft für den Fall eines Angriffs bei Geschäftspartnern zu bewerten (Melnyk et al. 2022, S. 165 f.).

4.4 Handel

Neben der Logistik ist auch der Einzelhandel aufgrund der umfangreichen Verarbeitung sensibler Kunden- und Geschäftsdaten ein attraktives Ziel für Cyberkriminelle. Ransomware stellt auch im Handel die größte Bedrohung dar, insbesondere durch den Angriffsvektor Phishing, wodurch Datenschutzverletzungen entstehen können. In der Regel bleibt die Verfügbarkeit der Kerndienstleistung von Datenschutzverletzungen unberührt (Teuteberg/Anton 2023, S. 134).

Unter den Angriffen, die auf IT-Systeme des Handels stattfinden können, stellen Angriffe auf zentrale Verwaltungssysteme, z. B. Warenwirtschaftssysteme, aber auch auf digitale Kassen- bzw. POS-Systeme aktuell die größte Gefahr für den Einzelhandel dar – zu diesem Schluss kommen Hoffmann und Haas (2023) sowie Teuteberg und Anton (2023). Bei einem Angriff auf das Warenwirtschaftssystem im Lebensmitteleinzelhandel könnten z. B. keine Aufträge im Logistiklager mehr abgearbeitet werden. Ein Ausfall dieser oder der POS-Systeme kann zur vorübergehenden Schließung von Handelsfilialen führen (Hoffmann/Haas 2023, S. 7; Teuteberg/Anton 2023, S. IX). So mussten im Juni 2022 mehrere dm-Filialen in Deutschland aufgrund des Ausfalls der Kassensysteme geschlossen bleiben (Schimak 2022). Bei solchen Angriffen verschaffen sich Cyberkriminelle Zugang zum Netzwerk des Handelsmarktes über externe Systeme oder Phishing. Nachdem sie eine Übersicht über das Netzwerk erstellen, installieren die Angreifer Schadsoftware zum Datendiebstahl von Kreditkartendaten im POS-System. Die Angreifer nutzen Techniken zur Tarnung und Verschleierung der Schadsoftware, um unentdeckt zu bleiben. Die gestohlenen Kreditkartendaten werden dann meist im Darknet weiterverkauft oder selbst für finanzielle Absichten missbraucht (Symantec 2014, S. 8 f.).

Angriffe auf POS-Systeme im Einzelhandel führen in der Regel in erster Linie zu Datenschutzverletzungen und ggf. finanziellen Verlusten bei den betroffenen Kund/innen (wenn Bankinformationen der Kund/innen gestohlen werden) sowie bei Händlern. Entsprechende Vorfälle können prinzipiell den Zugang zu Lebensmitteln erschweren. Bisher konnten die Folgen einzelner Störungen durch die Dichte des Supermarktnetzes in Deutschland abgefedert werden (Teuteberg/Anton 2023, S. 58). Allerdings besteht durch die starke Konzentration des Handels von Lebensmitteln in Deutschland auf vier große Lebensmittelhändler, die zusammen über einen Anteil von 76 % des Gesamtumsatzes verfügen (BVE 2023, S. 42; Hoffmann/Haas 2023, S. 14), die Gefahr einer Homogenisierung der eingesetzten Systeme, wodurch skalierte Angriffe über Softwareaktualisierungen gefährlich werden können. Denn für POS-Systeme im Markteinsatz werden Softwarekomponenten verwendet, die regelmäßig ggf. per Funk aktualisiert werden müssen, wodurch Einfallstore für Cyberangriffe entstehen (Hoffmann/Haas 2023, S. 23). Das liegt z. B. daran, dass Aktualisierungen meist über mehrere Wochen durchgeführt werden. So werden

Kassensysteme zeitweise mit einer veralteten Software betrieben. Die bereits vorgenommenen Aktualisierungen lassen daher auf bestehende Sicherheitslücken in den alten Systemen schließen, die für Cyberangriffe genutzt werden können (Hoffmann/Haas 2023, S. 55). Zwar kann der Grad der Vielfalt von POS- und Warenwirtschaftssystemen nicht genau ermittelt werden, allerdings weisen einzelne Meldungen auf lokale Konzentrationseffekte hin (EDEKA-Verbund 2022). Sollte die Vielfalt der eingesetzten Systeme und Hersteller von POS-Systemen sinken, könnte sich das Risiko für die Versorgungssicherheit verschärfen.

Noch problematischer kann sich ein indirekter Angriff auf einen externen IT-Dienstleister erweisen, wenn die Mehrheit der Einzelhandelsfilialen auf die jeweilige Dienstleistung (z. B. Überwachung und Verwaltung von IT-Netzwerken, Datenspeicherung oder -verarbeitung) zugreift. Werden zentrale IT-Dienstleistungen extern durchgeführt, so besteht bei einem komplexen Angriff auf diesen Dienstleister immer das Risiko, dass er auch Auswirkungen auf die nachgelagerten Kunden hat (z. B. eingeschränkte Nutzung der Software durch z. B. fehlenden Cloudzugang). Äußerst kritisch ist dies an denjenigen Stellen, wo IT-Dienstleister annähernd marktbeherrschende Stellungen einnehmen. Wie verheerend die Folgen eines solchen Vorfalls sein können, zeigte der Supply-Chain-Angriff auf das Kassensystem des US-amerikanischen Unternehmens Kaseya, ein Anbieter von digitalen Lösungen zur Überwachung und Verwaltung von Rechnersystemen und Netzwerken. Der Angriff fand im Juli 2021 statt und richtete sich gegen Kunden von Kaseya, die die Dienste des Unternehmens zur Überwachung und Verwaltung ihrer IT-Infrastruktur nutzen. Die Schadsoftware wurde über die Plattform von Kaseya auf die verwalteten IT-Systeme verteilt, wodurch die Reichweite des Angriffs vergrößert wurde und fast 800 Filialen von Coop, eine der größten Supermarktketten Schwedens, betraf. Kassen und Selbstbedienungsstationen fielen aus, die Coop-Mitarbeiter/innen konnten keine Zahlungen in den Filialen abwickeln. Die Filialen mussten schließlich temporär geschlossen werden (Cimpanu 2021).

Der Angriff auf Kaseya erstreckte sich auf 800 bis 1.500 nachgelagerte Unternehmen (taz 2021). Eine Schwachstelle zur Umgehung der Authentifizierung ermöglichte es den Angreifern, die IT-Systemverwaltungssoftware VSA von Kasaya zu kompromittieren. Der Vorfall weckte Bedenken hinsichtlich der Sicherheit von Fernverwaltung digitaler Anwendungen und machte die Notwendigkeit besserer Cybersicherheitsmaßnahmen zur Verhinderung und Reaktion auf solche Angriffe deutlich (Hoffmann/Haas 2023, S. 55). Auch in Deutschland wurden bei einem Hersteller von Kartenzahlungsterminals Softwarefehler festgestellt, die zu Störungen bei Kartenzahlungen in Discountern wie Aldi und EDEKA führten (Mayerhofer 2022). Neben Dienstleistungen zur Überwachung und Steuerung von Netzwerken oder Software für Kartenzahlungsterminals könnte auch die wachsende Nutzung von cloudbasierten Anwendungen, die

durch die Verbindung mit dem Internet neue Angriffsfläche für Hackerattacken bieten, zu einer erhöhten Verletzlichkeit führen.

Wo Webserver im Spiel sind, stellen Angriffe von Cyberkriminellen meist eine große Gefahr dar. Das betrifft vor allem Unternehmen, deren Kerngeschäft im Onlinehandel liegt und für die der Ausfall der Server eine Bedrohung für die Verfügbarkeit der Kernleistungen mit sich bringt. Gezielt gehören dazu Identitätsdiebstahl, Betrug, (D)DoS- und Virenangriffe sowie Phishing. Angriffe können für die einzelnen Betriebe und den Plattformbetreiber finanzielle Verluste und einen Rufschaden zur Folge haben (Kuruwitaarachchi et al. 2019, S. 2 f.). Die Attacke auf den Onlineessensbestelldienst Foodora (ehemaliges Tochterunternehmen der deutschen Delivery Hero) 2016 führte beispielsweise zu Datenschutzverletzungen, die über 700.000 Kunden betrafen (Ahmed 2020). Ein ähnlicher Fall ist der Angriff auf den niederländischen Essenslieferdienst Just Eat Takeaway. Der Angriff hatte nicht nur erhebliche Auswirkungen auf die Kunden, sondern auch auf die mehr als 15.000 Restaurants, die das Unternehmen für die Essenslieferung nutzen (Ilascu 2020). In beiden Fällen ist nicht öffentlich bekannt, ob Lösegelder gezahlt wurden. Jedes Unternehmen, das auf Onlinesysteme zur Abwicklung seiner Geschäfte angewiesen ist, ist für diese Art von Angriffen anfällig.

Die sichere Gestaltung digitaler Plattformen erfordert dementsprechend eine konsequente Gewährleistung der Transaktions- und Systemsicherheit (z. B. Sicherheit der Server, Datenbank und Kommunikationskanäle) sowie des Datenschutzes. Trotz der verheerenden Auswirkungen auf die einzelnen Betriebe ist ein Ausfall des Onlinegeschäfts in der Regel kein gravierendes Problem für die Versorgungssicherheit insgesamt, denn der Onlinehandel hat bisher nur einen relativ kleinen Marktanteil und stellt für die meisten Lebensmitteleinzelhändler nicht den primären Vertriebskanal dar. Der Zugang zu Lebensmitteln über andere Vertriebswege wie Supermärkte bleibt von einem Ausfall des Onlineangebots unberührt (Teuteberg/Anton 2023, S. 57 ff.).

4.5 Schlussfolgerungen

Auch wenn die offiziellen Meldungen den Anschein erwecken, dass der Ernährungssektor im Sektorenvergleich wenig von Cyberanfällen betroffen ist (9 Meldungen gegen 132 im Gesundheitssektor; BSI 2023), zeigt die Datenauswertung durch Teuteberg und Anton (2023) ein alarmierendes Bild. Mehr als zwei Drittel der 2018/2019 befragten Unternehmen im Sektor Landwirtschaft und Ernährung gaben an, bereits Opfer eines oder mehrerer Angriffe worden zu sein. Die meisten Vorfälle lassen sich Ransomware, Schadsoftware und Phishing zuordnen. Zu vermuten ist, dass die tatsächliche Zahl der Vorfälle im Ernährungssektor weitaus höher ist, als es die öffentlich bekannt gewordenen Fälle suggerieren. Auch die Fallstudienanalysen und Experteninterviews, die im

Rahmen des Projekts durchgeführt wurden, deuten darauf hin, dass die Nahrungsmittelindustrie, insbesondere in den letzten Jahren, verstärkt in das Visier von Cyberkriminellen geraten ist, wobei wirtschaftliche Motive vorherrschend waren (Teuteberg/Anton 2023, S. VI ff.).

Zwar hatte der Großteil der identifizierten Angriffe auf den Sektor Landwirtschaft und Ernährung keine unmittelbaren Auswirkungen auf die Ernährungssicherheit, es resultierten jedoch unternehmensbezogene Konsequenzen wie Datenschutzverletzungen, kurzzeitige Produktionsausfälle oder Lieferverzögerungen (Teuteberg/Anton 2023, S. 8). Außerdem ist künftig davon auszugehen, dass die Häufigkeit und die Auswirkungen von Angriffen zunehmen werden. Zum einen schreitet die Vernetzung von Systemen innerhalb von Unternehmen, aber auch zwischen Handelspartnern entlang der Wertschöpfungskette rasch voran. Neue Informationsschnittstellen werden geschaffen und mit IT-Lösungen geschlossen. Zum anderen steigt durch die Vernetzung das Risiko von Supply-Chain-Angriffen. Werden zentrale IT-Dienstleistungen über einen externen IT-Dienstleister durchgeführt, so besteht hier bei einem komplexen Angriff auf diesen Dienstleister immer das Risiko, dass sich diese Angriffe auch auf seine Kunden auswirken. Äußerst kritisch für die Nahrungsmittelversorgung ist dies an denjenigen Stellen, wo IT-Dienstleister oder Anbieter von IT-Lösungen annähernd marktbeherrschende Stellungen einnehmen. Schließlich eröffnen sich Angreifern mittels KI neue Möglichkeiten, komplexere Attacken gezielt durchzuführen. Perspektivisch dürfte neben den Fortschritten im Bereich KI auch das Quantencomputing neue Herausforderungen für die Cybersicherheit mit sich bringen.

Wie weitreichend die Auswirkungen eines Cyberangriffs sein können, hängt zum einen von der Verderblichkeit der betroffenen Produkte ab. Produkte, die eine hohe Verderblichkeit aufweisen, sind in der Regel gegenüber Ausfällen vulnerabler. Ein Ausfall des Systems kann schneller dazu führen, dass die Produkte verderben bzw. aus Sicherheitsgründen auf dem Markt nicht mehr verkauft werden dürfen. Besonders bei Frischeprodukten, z. B. Rohmilch, stellen Produktionsausfälle aufgrund begrenzter Lagermöglichkeiten ein größeres Problem dar bzw. haben unmittelbare Auswirkungen auf Lieferungen. Ausfälle, die Produkte mit längerer Haltbarkeit betreffen, die sich besser lagern lassen und solche, die für die Ernährung nicht unabdingbar sind, verursachen geringere Auswirkungen auf die Nahrungsmittelversorgung der Gesamtbevölkerung. Zum anderen hängt die Reichweite von folgenden Faktoren maßgeblich ab:

- *Aufwand und Schadenshöhe*: Die Wahrscheinlichkeit eines Angriffs steigt mit der zu erwartenden Schadenshöhe. Beispielsweise nimmt die Gefahr eines Angriffs auf Landmaschinen während der Aussaat- und Erntezeit zu. Gleichzeitig ist für Angreifer, besonders wenn wirtschaftliche Motive die Hauptrolle spielen, auch der Aufwand relevant, der für Planung und Durchführung des Cyberangriffs erforderlich ist. Liegen dem Angriff geopoliti-

sche Motive zugrunde, kann ggf. ein hohes Budget für die Planung und Durchführung des Angriffs zur Verfügung gestellt werden.

- *Kritikalität und Vernetzungsgrad des betroffenen IT-Systems*: Supply-Chain-Angriffe stellen dann ein Risiko für die Versorgungssicherheit dar, wenn zahlreiche Betriebe einer Branche ähnliche IT-Systeme einsetzen bzw. diese Systeme von wenigen Herstellern angeboten werden. Die Angriffsfläche ist dann besonders groß, wenn die kritischen IT-Systeme aktiv vernetzt sind und diese nur vernetzt bedient werden können. Ein potenziell größerer Schaden für die Lebensmittelversorgung kann immer dann entstehen, wenn IT-Systeme betroffen sind, die zum guten Funktionieren betrieblicher Prozesse unabdingbar sind (z. B. Melk- und Kühlsysteme, Energieversorgung) und bei einem Ausfall mit der auf dem Betrieb vorhandenen Arbeitskraft nicht substituiert werden können.
- *Marktstellung des Unternehmens*: Wird ein Unternehmen, das über einen hohen Marktanteil im Segment verfügt, angegriffen, kompromittiert und für eine gewisse Zeit ausgeschaltet (z. B. Molkerei, Schlachtungsbetrieb, Lebensmitteleinzelhandel), kann der Ausfall unter Umständen durch Mitbewerber nicht abgefedert werden. Zugleich schützt auch die Fragmentierung einer Branche aufgrund des steigenden Risikos von Supply-Chain-Angriffen und der Möglichkeit, Angriffe mittels KI zu automatisieren, immer weniger vor weitreichenden Auswirkungen auf die Versorgungssicherheit.
- *Umsetzung von IT-Cybersicherheitsmaßnahmen*: Es liegt auf der Hand, dass die Konsequenzen eines Angriffs umso höher sind, je ungeschützter ein System ist. Wie leicht ein System angegriffen werden kann, hängt vom Umfang der umgesetzten Cybersicherheitsmaßnahmen in den Betrieben ab. Die Daten aus der Befragung von 2018/2019 sowie die anekdotischen Evidenzen, die durch beide Gutachterteams erhoben wurden, deuten darauf hin, dass der Grad der Cybersicherheit vor allem bei kleinen und mittleren Betrieben Lücken aufweist.

5 Handlungsoptionen

Kritische Dienstleistungen sind für das Funktionieren unserer Gesellschaft von essenzieller Bedeutung, weswegen sie einem hohen Schutz unterliegen sollen. Allerdings können Sicherheitsmaßnahmen hohe Kosten verursachen. Deswegen gilt es abzuwägen, wo die größten Bedrohungen bestehen, um Anhaltspunkte für angemessene Vorkehrungen zu identifizieren, die zugleich einen ausreichenden Schutz sicherstellen. Bisher stand die Lebensmittelversorgung im Vergleich zu anderen kritischen Sektoren weniger im Fokus sowohl von Angreifern als auch von Regulierungsbemühungen zum Schutz der Infrastruktur.

Das liegt zum einen daran, dass eine hohe Abhängigkeit der Lebensmittelversorgung von anderen kritischen Sektoren besteht (BBK 2019, S. 95 ff.). Um die Lebensmittelversorgung zu sichern, muss u. a. die Versorgung mit Energie bzw. Strom, mit Wasser für den Anbau von Pflanzen und für die Tierhaltung sowie mit einer funktionierenden IKT-Infrastruktur gewährleistet sein. Der Schutz der entsprechenden Dienstleistungen bzw. kritischen IKT-Elemente, wie beispielsweise Serverfarmen (Hosting) und Rechenzentren (Housing), wird in der BSI-Kritisverordnung[17] für den Sektor IKT[18] geregelt, in der schützenswerte Anlagentypen sowie Schwellenwerte definiert werden. Konkrete Maßnahmen zu Sprachkommunikations-, Internetzugangs-, Datenübertragungs- und E-Maildiensten sind im Telekommunikationsgesetz[19] enthalten. Für die Verteilung von Lebensmitteln sind hauptsächlich Logistiksysteme bzw. Leistungen zum Transport von Gütern maßgeblich. Diese werden teilweise von Regulierungen zum Schutz des Sektors »Transport und Verkehr« abgedeckt.[20] Der Schutz von digitalen Kassen- bzw. POS-Systemen ist wiederum im Rahmen des Schutzes kritischer Dienstleistungen im Sektor »Finanz- und Versicherungswesen« geregelt.[21]

Zum anderen sorgte die hohe Vielfalt der Produkte und Unternehmen im Ernährungssektor dafür, dass der Ausfall eines Anbieters bzw. eines Betriebes in den meisten Fällen keine gravierenden Folgen für die Versorgung der Bevölkerung hat (BBK 2019, S. 148). Daher wurden bislang in diesem Sektor vor allem Betreiber größerer kritischer Anlagen ab einem gesetzlich definierten Schwellenwert dazu verpflichtet, ihre IT-Systeme und Netzwerke gegenüber Cyberangriffen zu schützen.[22] Vor dem Hintergrund wachsender Gefahren durch die Vernetzung und Integration von Systemen und Daten sowohl inner-

17 BSI-Kritisverordnung vom 22.4.2016, zuletzt am 29.11.2023 geändert
18 Anhang 4 (zu § 1 Nummer 4 und 5, § 5 Absatz 4 Nummer 1 und 2) der BSI-KritisV
19 Telekommunikationsgesetz vom 23.6.2021, zuletzt am 14.3.2023 geändert
20 Anhang 7 der BSI-KritisV benennt kritische Systeme und Schwellenwerte für einzelne Anlagenkategorien.
21 Anhang 6 (zu § 1 Nummer 4 und 5, § 7 Absatz 7 Nummer 1 und 2) der BSI-KritisV
22 Anhang 3 (zu § 1 Nummer 4 und 5, § 4 Absatz 3 Nummer 1 und 2) definiert relevante Anlagenkategorien und Schwellenwerte im Sektor Ernährung.

halb einzelner Betriebe als auch entlang der Wertschöpfungskette sowie der Möglichkeiten, Angriffe auf zahlreiche kleinere Betreiber bzw. durch Supply-Chain-Angriffe mittels KI leichter durchzuführen, ist eine Absenkung der Schwellenwerte und ein stärkerer Fokus auf Lieferketten sinnvoll. Denn Supply-Chain-Angriffe auf IT-Dienstleister (z. B. für die Überwachung und Verwaltung von Rechnersystemen und Netzwerken) und Hersteller von Betriebstechnik mit hoher Marktdurchdringung (z. B. automatische Melksysteme) standen lange Zeit wenig im Fokus der Regulierung. Drei Handlungsoptionen lassen sich aus der Analyse ableiten:

- externe Dienstanbieter und Anbieter kritischer IT-Technik in die Pflicht nehmen,
- kleine Betreiber zu mehr Cybersicherheit bewegen sowie
- Wissenslücken schließen.

Auf die zahlreichen Handlungsoptionen, die zu einem höheren Schutz des Ernährungssektors beitragen würden, aber nicht sektorenspezifisch sind, wird in diesem Kapitel nicht näher eingegangen. Dazu gehören insbesondere *Maßnahmen zur Reduzierung des IT-Fachkräftemangels*, zur Erhöhung von Effizienz und Effektivität in den *Sicherheits- und Strafverfolgungsbehörden* sowie zur Stärkung des *Bewusstseins für Cyberrisiken*.[23] Im Folgenden wird auf zu erwartende gesetzliche Regulierungen sowie auf darüberhinausgehende Handlungsoptionen hingewiesen.

5.1 Externe Dienstanbieter, Anbieter kritischer IT-Technik und Lieferanten stärker in die Pflicht nehmen

Um ihre eigenen Systeme und Daten zu schützen, müssen Unternehmen im Ernährungssektor nicht nur sicherstellen, dass ein ausreichendes Niveau an Cybersicherheit im eigenen Unternehmen gewährleistet ist, sondern auch, dass ihre Partner in der Lieferkette über angemessene Cybersicherheitsvorkehrungen verfügen. Das gilt für Lieferanten und externe Dienstanbieter, denn eine Sicherheitsverletzung bei einem Partner in der Lieferkette kann zu einer Verletzung der eigenen Systeme und Daten führen. Um dagegen geschützt zu sein, ist die Umsetzung von Cybersicherheitsmaßnahmen bei den Geschäftspartnern von zentraler Bedeutung (Teuteberg/Anton 2023, S. 64).

23 Gemäß Art. 20 der NIS-2-Richtlinie wird es künftig für Mitglieder der Leitungsebene von mittleren und großen Betrieben verpflichtende Schulungsmaßnahmen im Bereich der Informationssicherheit geben, außerdem sollen die Betreiber aufgefordert werden, entsprechende Schulungsmaßnahmen regelmäßig allen Mitarbeiter/innen anzubieten.

Vertragliche Vereinbarungen mit Lieferanten und externen Dienstleistern

Die NIS-2-Richtlinie sieht vor, dass Betreiber wesentlicher und wichtiger Einrichtungen dazu angehalten werden sollen, Risikomanagementmaßnahmen bei der Cybersicherheit in die vertraglichen Vereinbarungen mit ihren direkten Lieferanten und Diensteanbietern einzubeziehen. Es ist also davon auszugehen, dass durch die Umsetzung der NIS-2-Richtlinie in das deutsche Recht mittlere und große Betreiber kritischer Infrastrukturen in Deutschland stärker dazu angehalten werden, für die Einhaltung von Cybersicherheitsmaßnahmen durch Lieferanten und Dienstleister zu sorgen. Der Entwurf eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (BMI 2024a) zur Anpassung des deutschen Rechts an die europäischen Anforderungen befindet sich derzeit im Gesetzgebungsverfahren. Um externe Dienstleister stärker in die Pflicht zu nehmen, könnten außerdem für kleine und mittlere Betriebe Mustervorlagen für Lastenhefte und andere vergaberelevante Unterlagen bereitgestellt werden. Das BSI hat bereits »Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen« herausgegeben (UP KRITIS 2023). Ob diese den Bedarfen und Ressourcen kleinerer Unternehmen gerecht werden, wäre zu überprüfen.

Ergänzend könnte die Einhaltung von Mindestsicherheitsstandards durch die Einführung einer Zertifizierungspflicht für (externe) IT-Dienstleister gewährleistet werden, die im Auftrag von Anbietern kritischer Dienstleistungen (hier insbesondere kleine und mittlere Unternehmen) die Verantwortung für das Setup, den Betrieb und/oder die Überwachung der IT-Netze übernehmen und/oder cloudbasierte Anwendungen konfigurieren und zur Verfügung stellen. Ein Modell für eine solche Zertifizierung ist das Schweizer Gütesiegel »CyberSeal« (Allianz Digitale Sicherheit o. J.). Durch dieses wird bestätigt, dass ein IT-Dienstleister, der mit kleinen und mittleren Unternehmen zusammenarbeitet, ausreichende technische und organisatorische Maßnahmen umsetzt, um die Cybersicherheit der Systeme zu gewährleisten.

Außerdem wäre zu prüfen, ob und welche Lieferanten und Dienstleister durch ihren privilegierten Zugang zu Unternehmen und die dort eingesetzte IT-Technik perspektivisch mit ähnlichen Anforderungen wie Betreiber kritischer Infrastrukturen in die Pflicht zu nehmen wären (z. B. Hersteller von Landmaschinen und Landtechnik).

Normen und Standards für kritische Produkte, Dienste oder Prozesse weiterentwickeln

Der Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (§ 57 (3); BMI 2024b) sieht vor, dass per Rechtsverordnung definiert wird, welche Produkte, Dienste und Prozesse, die in kritischen Infrastrukturen eingesetzt

werden, über eine Zertifizierung verfügen müssen. Welche IT-Komponenten hierzu gehören, weil sie direkt oder indirekt mit einem anderen Gerät oder einem Netz verbunden sowie im Sektor weit verbreitet und zum Betrieb von Anlagen kritisch sind, sollte für den Ernährungssektor zeitnah identifiziert werden. Der vorliegende Bericht liefert hierzu für jede Wertschöpfungsstufe Ansatzpunkte.

Besonders schützenswerte Systeme, die branchenübergreifend eingesetzt werden und für einen ordnungsgemäßen Produktionsbetrieb im Unternehmen wesentlich, aber nicht branchenspezifisch sind, wie z. B. Warenwirtschaftssysteme, sind bereits Gegenstand allgemein gültiger Sicherheitsstandards (z. B. IT-Grundschutz, ISO/IEC 27001). Für viele Produkte und operative Technologien, die in der Branche breit eingesetzt werden, existieren solche Standards allerdings noch nicht. So schließen Cybersicherheitsstandards, die für die Zulassung neuer Fahrzeuge im Straßenverkehr (ISO 21434) gelten, landwirtschaftliche Fahrzeuge beispielsweise derzeit nicht ein. Eine Anpassung dieser Standards auf Landmaschinen würde zur Erhöhung der IT-Sicherheit in der Landwirtschaft beitragen. Aktuell wird an einem solchen Vorschlag gearbeitet (ISO 2022). Es wäre an den Branchenarbeitskreisen des UP KRITIS, Vorschläge zu erarbeiten, zu welchen IT-Produkten Cybersicherheitsstandards prioritär erarbeitet werden sollten.

5.2 Kleine Unternehmen zu mehr Cybersicherheit bewegen

Die NIS-2-Richtlinie erweitert den Anwendungsbereich von Cybersicherheitspflichten auf mittlere Betriebe sowie bestimmte Einrichtungen und Branchen unabhängig von der Größe[24] (z. B. besonders wichtige digitale Infrastrukturen und öffentliche Verwaltung). Kleinst- sowie kleine Unternehmen sind bis auf wenige Ausnahmen von dieser Richtlinie ausgeschlossen. So wird es auch nach Überführung der Vorgaben der NIS-2-Richtlinie in deutsches Recht für die große Zahl an kleinen Betrieben in der Landwirtschaft und Ernährungsindustrie keine gesetzlichen Vorgaben zur Informationssicherheit geben. Allerdings nimmt im Zuge der Digitalisierung die Wahrscheinlichkeit gleichzeitig auftretender betriebskritischer IT-Störungen bei mehreren kleinen Betrieben, beispielsweise durch parallel ausgeführte Cyberangriffe, tendenziell zu. Um einem solchen Szenario vorzubeugen, wäre die Unterstützung freiwilliger Maßnahmen weiter zu fördern und der Wissenstransfer aus der Forschung in die unternehmerische Praxis sicherzustellen. Dafür spielen die Transferstelle IT-Sicherheit im Mittelstand und die bestehende Förderlandschaft des Bundesministeriums

24 für eine übersichtliche Darstellung der betroffenen Unternehmen siehe OpenKRITIS (o. J.)

für Wirtschaft und Klimaschutz ebenso wie europäische Förderangebote für Cybersicherheit im Mittelstand eine wesentliche Rolle.

Grundsätzlich ist das Bewusstsein für zunehmende Bedrohungen durch Cyberangriffe in den Kleinst- und kleinen Unternehmen noch nicht stark ausgeprägt, weswegen mit Aufklärungs- und Informationskampagnen darauf hingewirkt werden könnte, das Wissen besonders in den Bereichen zu erhöhen, die bisher weniger exponiert waren (z. B. Landwirtschaft).

5.3 Wissenslücken schließen

Die Wissenslücken zum Stand der Cybersicherheit sind insgesamt sehr groß. Dies gilt auch und besonders für den Ernährungssektor. Um eine ausreichende Cybersicherheit zu gewährleisten, ist es wichtig,

- Daten zur Verbreitung von Technologien zu erheben,
- Störfälle und Schutzniveaus systematischer zu erfassen sowie
- die Chancen und Risiken neuer Technologien systematisch zu bewerten.

Daten zur Verbreitung von Technologien erheben

Um mit der schnellen Verbreitung digitaler Lösungen und den sich daraus ergebenden Risiken umzugehen, braucht es genaueres Wissen dazu, welche digitalen Technologien und Produkte für die Erbringung kritischer Dienstleistungen im Sektor Landwirtschaft und Ernährung verbreitet sind. Erforderlich wäre eine kontinuierliche Marktüberwachung, welche IT-Systeme (kritische IKT-Dienste, -Systeme oder -Produkte) von welchen Herstellern eingesetzt werden, um potenzielle Marktkonzentrationen bzw. systemische Schwachstellen frühzeitig zu erkennen. In der Landwirtschaft gehören aktuell vornehmlich moderne Landmaschinen und Robotertechnologien zu den kritischen, zu beobachtenden Systemen, perspektivisch aber auch Drohnen, digitale Zwillinge und KI-gestützte Anwendungen. Außerdem ist eine solche Marktüberwachung für Technologien relevant, die Schnittstellen zwischen Handelspartnern entlang der Wertschöpfungskette schaffen, wie beispielsweise zum Tracking von Informationen oder zur Verknüpfung von Prozessen entlang der Wertschöpfungskette. Einen Anknüpfungspunkt schafft dafür § 7a des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, nach welchem das BSI zu marktgängigen IT-Produkten und Systemen Auskünfte von Herstellern verlangen darf.

Störfälle und Schutzniveaus systematisch und regelmäßig erfassen

Die Datenlage zur Cybersicherheit im Ernährungssektor ist sehr lückenhaft, insbesondere zu Störungen bzw. Cyberangriffen in der Landwirtschaft. Der Fokus

von Analysen lag lange Zeit vor allem auf der sozioökonomischen Resilienz sowie der Resilienz gegenüber den Folgen des Klimawandels (Hanuschik/Moritz 2023; Kuntke et al. 2022). Um die Diskrepanz zwischen den offiziell gemeldeten Vorfällen und der empirisch erfassten hohen Anzahl tatsächlich beobachteter Cyberangriffe zu verringern und so Hinweise auf Cybersicherheitsrisiken zu erhalten, könnten Meldewege zu IT-Störungen und Cyberangriffen beim BSI einfacher und unbürokratischer gestaltet und in den betroffenen Branchen bekannt gemacht werden. Die Bemühungen des BMI, eine zentrale Meldestelle zu schaffen (Stiebel 2024a), die auch von kleinen und mittleren Unternehmen in Anspruch genommen werden könnte, ist ein Schritt in diese Richtung. Um das Wissen über das Schutzniveau in der Branche genauer zu erfassen und zielgerichtete Maßnahmen für einen besseren Schutz zu planen, wären außerdem regelmäßige Datenerhebungen zum Bewusstsein für Cybersicherheitsrisiken und zum Stand der Umsetzung entsprechender Maßnahmen bei Unternehmen durchzuführen.

Forschung zu Cybersicherheit neuer Technologien weiter fördern

Die Fortschritte der KI eröffnen ganz neue Möglichkeiten für Cyberangriffe und schaffen neue Vulnerabilitäten für kritische Systeme, wenn diese in kritische Anlagen eingesetzt werden (BSI o. J.). Je mehr KI-Systeme in kritische Anwendungen implementiert werden, desto wichtiger wird es sein, frühzeitig Schwachstellen solcher Systeme zu erkennen und umfassende Detektions- und Schutzmechanismen umzusetzen. Der Schutz von KI-Systemen, die in kritischen Infrastrukturen eingesetzt werden, ist im Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz erfasst (EK 2021). KI-Systeme mit hohem Risiko müssen nach Art. 5 widerstandsfähig gegen Cyberangriffe unter Ausnutzung von KI-spezifischen Schwachstellen gemacht werden. Aktuell besteht der praktikabelste Ansatz in der Analyse möglicher Bedrohungen in dem jeweiligen Anwendungsfall und der Entwicklung entsprechender Schutzmaßnahmen (Adilova et al. 2022). Vor diesem Hintergrund ist es wichtig, Best-Practice-Beispiele und Lösungsansätze zu erforschen und zu entwickeln. Partnerschaften mit White-Hat-Hackern, die ihre Fähigkeiten dazu einsetzen, Sicherheitslücken in IT-Systemen aufzudecken, könnte die Bewertung der Anfälligkeit von KI-gestützten Anwendungen für Cyberangriffe unterstützen, um Risiken frühzeitig abzuschätzen und Anpassungsstrategien zu entwickeln (Tzachor et al. 2022). Durch die Förderrichtlinie »Sichere Zukunftstechnologien in einer hypervernetzten Welt: Künstliche Intelligenz – Vernetzung und Sicherheit digitaler Systeme« (BMBF 2023) und die Entwicklung eines Frühwarnradars für zukünftige Cyberkriminalität (Cyberagentur 2024) könnten wichtige Beiträge in dieser Hinsicht geleistet werden. Neben den Gefahren durch KI könnte Quantencomputing für die Sicherheit von Industrial

Control Systems (ICS) in Zukunft besonders relevant werden, denn diese ICS erfordern nicht nur eine besonders hohe Sicherheit bei einem Einsatz in kritischen Infrastrukturen, sondern werden oft über einen längeren Zeitraum eingesetzt. Deswegen wären die Risiken durch solche zukünftigen Bedrohungen regelmäßig zu bewerten.

6 Literatur

6.1 In Auftrag gegebene Gutachten

Hoffmann, C.; Haas, R. (2023): Cybersicherheit in der Nahrungsmittelversorgung (Schwerpunkt Landwirtschaft) – Identifizierung von Risikoelementen, hypothetische Angriffsszenarien und Auswirkungen auf die Ernährungsversorgung. oeconos GmbH, Dettingen

Teuteberg, F; Anton, E. (2023): Cybersicherheit im Bereich Nahrungsmittelverarbeitung- und -handel sowie Kühllogistik von Milch und Milchprodukten: Vulnerabilitätsanalyse und Handlungsfelder zur Stärkung der Resilienz. synovacom GmbH, Osnabrück

6.2 Weitere Literatur

Abrams, L. (2021): Dutch supermarkets run out of cheese after ransomware attack. BleepingComputer, https://www.bleepingcomputer.com/news/security/dutch-supermarkets-run-out-of-cheese-after-ransomware-attack/ (28.5.2024)

Acar, C. (2021): Technologie Trends im Handel 2021. EHI Retail Institute, https://www.ehi.org/produkt/studie-technologie-trends-im-handel-2023-pdf/ (28.5.2024)

Acar, C.; Hahn, I. (2024): POS-Systeme 2024. EHI Retail Institute, https://www.ehi.org/wp-content/uploads/Downloads/Leseproben/EHI-Studie_POS-Systeme-2024_Leseprobe.pdf (28.5.2024)

Acar, C.; Hahn, I.; Spaan, U. (2023): Technologie Trends im Handel 2023. EHI Retail Institute, https://www.ehi.org/produkt/studie-technologie-trends-im-handel-2023-pdf/ (28.5.2024)

Ahmed, D. (2020): Foodora suffers data breach 700,000+ users in 14 countries affected. HACKREAD, https://www.hackread.com/foodora-data-breach-14-countries-users-affected/ (28.5.2024)

Allianz Digitale Sicherheit Schweiz (o. J.): CyberSeal – das Gütesiegel. https://www.digitalsecurityswitzerland.ch/de/cyberseal (28.5.2024)

Ashibani, Y.; Mahmoud, Q. (2017) Cyber physical systems security: Analysis, challenges and solutions. https://doi.org/10.1016/j.cose.2017.04.005 (28.5.2024)

Baker, L.; Green, R. (o. J.): Cyber Security in UK Agriculture. NCC Group, https://research.nccgroup.com/wp-content/uploads/2020/07/agriculture-white paper-final-online.pdf (28.5.2024)

Baumann, S. (2022): Wegen Putin! Unsere Kühe haben kein Internet. BILD.de, https://www.bild.de/news/inland/news-ausland/schwarzwald-bauernhof-wegen-putin-unsere-kuehe-haben-kein-internet-79574296.bild.html (28.5.2024)

Bendel, P. (2024): Cyberphysische Systeme. Gabler, https://wirtschaftslexikon.gabler.de/definition/cyberphysische-systeme-54077 (28.5.2024)

Bitkom e. V. (2022): Jedes fünfte Logistikunternehmen setzt Künstliche Intelligenz ein. https://www.bitkom.org/Presse/Presseinformation/Logistikunternehmen-Kuenstliche-Intelligenz-KI (28.5.2024)

Bitkom e. V. (2023): Ohne Online-Angebot kommt praktisch kein Händler mehr aus. https://www.bitkom.org/Presse/Presseinformation/Ohne-Online-Angebot-kommt-Haendler-aus (28.5.2024)
Bitkom e. V. (2024): Schnell-Lieferdienste werden immer beliebter. https://www.bitkom.org/Presse/Presseinformation/Schnell-Lieferdienste-werden-immer-beliebter (28.5.2024)
BITO (BITO-Lagertechnik Bittmann GmbH) (2020): Trends in der temperaturgeführten Lebensmittellogistik. https://www.bito.com/de-de/fachwissen/artikel/trends-in-der-temperaturgefuehrten-lebensmittellogistik/ (28.5.2024)
BKA (Bundeskriminalamt) (2022): Cybercrime: Bundeslagebild 2021. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=6 (28.5.2024)
BMI (Bundesministerium des Innern und für Heimat) (2024a): Entwurf eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes. https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html (28.5.2024)
BMI (2024b): Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz). Referentenentwurf des Bundesministeriums des Innern und für Heimat. Bearbeitungsstand: 7.5.2024, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE.pdf?__blob=publicationFile&v=3 (28.5.2024)
BMWK (Bundesministerium für Wirtschaft und Klimaschutz) (o. J.): REIF – Resource-efficient, Economic and Intelligent Foodchain, https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/KuenstlicheIntelligenzProjekte/KuenstlicheIntelligenz_ErsterFoerderaufruf/ki-projekt_reif.html (28.5.2024)
Bongs, K., Bennett, S., Lohmann, A. (2023): Quantum sensors will start a revolution – if we deploy them right. https://doi.org/10.1038/d41586-023-01663-0 (28.5.2024)
Brewster, T. (2021): Fraudsters Cloned Company Directors Voice In $35 Million Heist, Police Find. Forbes, https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=19dd6fc87559 (28.5.2024)
BSI (Bundesamt für Sicherheit in der Informationstechnik) (2021a): Prävention und Erste Hilfe bei Webseiten Kompromittierung oder Defacement. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Hilfe_Website_Kompromittierung.pdf?__blob=publicationFile&v=4 (7.8.2024)
BSI (2021b): Sicherer, robuster und nachvollziehbarer Einsatz von KI: Probleme. Maßnahmen und Handlungsbedarfe. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.pdf?__blob=publicationFile&v=6 (28.5.2024)
BSI (2023) Die Lage der IT-Sicherheit in Deutschland 2023. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=8 (28.5.2024)
BSI (o. J.) Faktor Mensch. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/faktor-mensch.html?nn=523048 (28.5.2024)

Büscher, W.; Haidn, B.; Häuser, S.; Klindtworth, K.; Mohr, U.; Pfeiffer, J. (2021): Digitale Anwendungen für das Herdenmanagement in der Milchviehhaltung. DLG e. V., https://www.dlg.org/fileadmin/downloads/landwirtschaft/themen/publikationen/merkblaetter/dlg-merkblatt_466.pdf (28.5.2024)
BVE (Bundesvereinigung der Deutschen Ernährungsindustrie e. V.) (2020): Branchenspezifische Sicherheitsstandard (B3S) für die Ernährungsindustrie. Berlin
BVE (2023): Jahresbericht 2023. https://www.bve-online.de/download/bve-jahresbericht-ernaehrungsindustrie-2023 (28.5.2024)
BWL-Lexikon.de (o. J.): First In – First Out (FiFo). https://www.bwl-lexikon.de/wiki/first-in-first-out-fifo/ (28.5.2024)
Chaykin, A. (2023): How ChatGPT is lowering the entry barrier to cybercrime. https://www.controlrisks.com/our-thinking/insights/how-chat-gpt-is-lowering-the-entry-barrier-to-cybercrime?utm_referrer=https://techmonitor.ai (28.5.2024)
Cheung, K.-F.; Bell, M.; Bhattacharjya, J. (2021): Cybersecurity in logistics and supply chain management: An overview and future research directions. https://doi.org/10.1016/j.tre.2020.102217 (28.5.2024)
Cimpanu, C. (2021): Supermarket chain Coop closes 800 stores following Kaseya ransomware attack. The Record, https://therecord.media/supermarket-chain-coop-closes-800-stores-following-kaseya-ransomware-attack (28.5.2024)
CISSM (Center for International Security Studies at Maryland) (o. J.): Cyber Events Database. https://cissm.umd.edu/cissm-cyber-events-database (28.5.2024)
CLAAS KGaA mbH (o. J.): Mit CLAAS ist Smart Farming einfach. https://www.claas.de/produkte/digitale-loesungen (28.5.2024)
Claroty Ltd. (2023): State of XIoT Security Report: 2H 2022. https://web-assets.claroty.com/state-of-xiot-security-report-2h-2022-(2).pdf (28.5.2024)
Cyber Centre (Canadian Centre for Cyber Security) (2022) An Introduction to the Cyber Threat Environment. https://www.cyber.gc.ca/sites/default/files/ncta-2022-intro-e.pdf (28.5.2024)
DBV (Deutscher Bauernverband e. V.) (2023): Situationsbericht 2022/23. https://magazin.diemayrei.de/storage/media/1ed75fd6-6af3-6bec-b3d0-5254a201e2da/Sit_2023_Kapitel1.pdf (28.5.2024)
Destatis (Statistisches Bundesamt) (2008): Klassifikation der Wirtschaftszweige (WZ 2008). https://www.destatis.de/DE/Methoden/Klassifikationen/Gueter-Wirtschaftsklassifikationen/klassifikation-wz-2008.html (28.5.2024)
Destatis (2024): Rund 7.800 landwirtschaftliche Betriebe weniger seit dem Jahr 2020. https://www.destatis.de/DE/Presse/Pressemitteilungen/2024/01/PD24_021_41.html (28.5.2024)
DLG e. V. (2023): DLG-ImageBarometer 2022/23: Welche Marken sind im Trend? https://www.dlg.org/de/landwirtschaft/themen/dlg-imagebarometer/dlg-imagebarometer-2022-2023 (28.5.2024)
Dragos Inc. (2023): ICS/OT Cybersecurity. Year in Review 2022. https://hub.dragos.com/ics-cybersecurity-year-in-review-2022 (28.5.2024)
Dreißigacker, A.; von Skarczinski, B.; Wollinger, G. (2020): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019, Kriminologisches Forschungsinstitut Niedersachsen e. V., KFN-Forschungsbericht Nr. 152, Hannover
EDEKA-Verbund (2022): Lunar läuft bei EDEKA Südwest. https://verbund.edeka/presse/pressemeldungen/lunar-l%C3 %A4uft-bei-edeka-s%C3 %BCdwest.html (28.5.2024)

EHI (2023): Seamless Checkout: angesagt und notwendig. https://www.ehi.org/presse/seamless-checkout-angesagt-und-notwendig/ (28.5.2024)
Eikenberg, R. (2023): ChatGPT als Hacking-Tool: Wobei die KI unterstützen kann. https://www.heise.de/hintergrund/ChatGPT-als-Hacking-Tool-Wobei-die-KI-unterstuetzen-kann-7533514.html (28.5.2024)
Eikenberg, R.; Königstein, A. (2021): Gute Tools, böse Tools. Hacking-Werkzeug für Fortgeschrittene. https://www.heise.de/select/ct/2021/23/2124514385122190550 (28.5.2024)
EK (Europäische Kommission) (2021): Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimm-ter Rechtsakte der Union. COM(2021) 206 final, Brüssel
FBI (Federal Bureau of Investigation) (2022): Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons. https://www.ic3.gov/Media/News/2022/220420-2.pdf (28.5.2024)
Fitzmaurice, G. (2024): NSA: Benefits of generative AI in cyber security will outweigh the bad, ITPro. https://www.itpro.com/security/nsa-benefits-of-generative-ai-in-cyber-security-will-outweigh-the-bad (28.5.2024)
Fortinet Inc. (2021): Causes and Consequences of IT and OT Convergence. https://whitepaperseries.com/wp-content/uploads/2023/12/132140_wpotnetworkconvergence.pdf (28.5.2024)
Forum Moderne Landwirtschaft e.V. (o. J.): Feldroboter »Dino« und die moderne Landwirtschaft. https://blog.moderne-landwirtschaft.de/feldroboter-dino-und-die-moderne-landwirtschaft (28.5.2024)
Gardizy, A. (2022): Hackers hit Hood. Dairy shut down milk production this week after »cyber security event«. The Boston Globe, https://www.bostonglobecom/2022/03/18/business/school-milk-could-be-short-supply-after-hood-plants-hit-by-cyber-event/ (28.5.2024)
Garnett, P.; Doherty, B.; Heron, T. (2020): Vulnerability of the United Kingdoms food supply chains exposed by COVID-19. https://doi.org/10.1038/s43016-020-0097-7 (28.5.2024)
Gehlot, A. et al. (2022): Dairy 4.0: Intelligent Communication Ecosystem for the Cattle Animal Welfare with Blockchain and IoT Enabled Technologies. https://doi.org/10.3390/app12147316 (28.5.2024)
Göggerle, T. (2024a): Fendt Traktor mit dem Smartphone steuern – autonomer Vario im Einsatz. agrarheute, https://www.agrarheute.com/technik/traktoren/fendt-traktor-smartphone-steuern-autonomen-vario-einsatz-615874 (28.5.2024)
Göggerle, T. (2024b): Traktorzulassung 2023: enges Rennen zwischen John Deere und Fendt. agrarheute, https://www.agrarheute.com/technik/traktoren/traktorzulassung-2023-enges-rennen-zwischen-john-deere-fendt-615229 (28.5.2024)
Grothmann, A. et al. (2010): Automatische Fütterungssysteme (AFS) – Optimierungspotenzial im Milchviehstall. https://doi.org/10.15150/lt.2010.610 (28.5.2024)
Haas, R.; Hoffmann, C. (2020): Cyber Threats and Cyber Risks in Smart Farming. https://doi.org/10.51202/9783181023747-37 (28.5.2024)
Hanuschik, S.; Moritz, J. (2023): Cyberresilienz in der Landwirtschaft. Whitepaper – Landwirtschaftliche Betriebe besser gegen Cyberattacken schützen. Bitkom e. V., https://www.bitkom.org/sites/main/files/2023-08/bitkom-whitepaper-cyberresilienz-in-der-landwirtschaft.pdf (28.5.2024)

Hao, K. (2021): A new generation of AI-powered robots is taking over warehouses. MIT Technology Review. https://www.technologyreview.com/2021/08/06/1030802/ai-robots-take-over-warehouses/ (28.5.2024)
Hardy, J.; Larson, E. (2021): Cyberattack targets JBS beef plants impacting Nebraska operations. KLKN-TV, https://www.klkntv.com/cyberattack-targets-jbs-beef-plants-impacting-nebraska-operations/ (28.5.2024)
Harry, C.; Gallagher, N. (2018) Classifying Cyber Events: A Proposed Taxonomy. Center for International Security Studies at Maryland, https://cissm.umd.edu/sites/default/files/2019-07/Cyber-Taxonomy-101918.pdf (28.5.2024)
Haufe-Lexware GmbH & Co. KG. (o. J.): Handelstrends: Wie Händler mit Cloud-ERP erfolgreich durchstarten. 1.1.2024, https://www.haufe-x360.de/blog/blog-detail/handelstrends-wie-haendler-mit-cloud-erp-erfolgreich-durchstarten (28.5.2024)
HDE (Handelsverband Deutschland) (2023a): Jahrespressekonferenz Handelsverband Deutschland. https://einzelhandel.de/images/presse/Pressekonferenz/2023/HDE-Pressekonferenz-Charts.pdf (28.5.2024)
HDE (2023b): Künstliche Intelligenz im Handel. Umfrage zum KI-Einsatz in 2023. https://einzelhandel.de/images/europawahl2024/KI_Umfrage_HDE_Safaric_2023_1904_as.pdf (28.5.2024)
Hofer, S. (2022): »You are fucked«: Wie Hacker SalzburgMilch lahmlegten. profil, https://www.profil.at/gesellschaft/you-are-fucked-wie-hacker-salzburgmilch-lahmlegten/401471785 (28.5.2024)
Holzner, J.; Hümmer, C. (2023): Perspektiven der Milchproduktion und -verarbeitung in Deutschland bis 2030. Hochschule Weihenstephan-Triesdorf, Freising
IBISWorld (o. J.): Herstellung von Düngemitteln in Deutschland. Marktforschung, Kennzahlen, Statistiken, Studien und Analysen. https://www.ibisworld.com/de/branchenreporte/herstellung-duengemitteln/224/ (28.5.2024)
IDG (IDG Business Media GmbH): (2019): Studie Virtual Reality/Augmented Reality 2019. https://www.ptc.com/-/media/Files/PDFs/Augmented-Reality/19-08-ARVR-Studie-2019-V4.pdf (28.5.2024)
Ilascu, I. (2020): Food Delivery Service in Germany Under DDoS Attack. BleepingComputer, https://www.bleepingcomputer.com/news/security/food-delivery-service-in-germany-under-ddos-attack/ (28.5.2024)
IONOS (2021): POS-Systeme im Überblick – Definition, Funktionsweise und Vergleich. https://www.ionos.de/digitalguide/online-marketing/verkaufen-im-internet/pos-system/ (28.5.2024)
IPES-Food & ETC Group (2021): A Long Food Movement: Transforming Food Systems by 2045. https://www.ipes-food.org/_img/upload/files/LongFoodMovementEN.pdf (28.5.2024)
James, D. (2019a): Computer virus sparks chaos for National Milk Records. Farmers Weekly, https://www.fwi.co.uk/livestock/dairy/computer-virus-sparks-chaos-for-national-milk-records (28.5.2024)
James, D. (2019b): Police probe virus attack on National Milk Records systems. Farmers Weekly, https://www.fwi.co.uk/livestock/dairy/police-probe-virus-attack-on-national-milk-records-systems (28.5.2024)
JGPR (John Guilfoil Public Relations) (2022): ConVal School District to be Impacted by Milk Shortage Due to Cyber Attack at Dairy Supplier. https://jgpr.net/2022/03/16/conval-school-district-to-be-impacted-by-milk-shortage-due-to-cyber-attack-at-dairy-supplier/ (28.5.2024)

Kantale, R. et al. (2022): SCADA-Automation Key Concept of Dairy Industrial Control System. Vigyan Varta 3(12), S. 45–50
KonBriefing (2022): Cyberangriffe 2021 auf Unternehmen im FMCG-Markt. https://konbriefing.com/de-topics/cyber-angriffe-2021-fmcg.html (28.5.2024)
KonBriefing (2024): Bedeutende Cyberangriffe auf die Lebensmittelbranche 2023. https://konbriefing.com/de-files/cyberangriffe/2023-ind-lebensmittel-tl-de-hires.png (28.5.2024)
Kreutz, H. (2021): Digitale Plattformen. Vertrieb regionaler Lebensmittel erleichtert. Bundeszentrum für Ernährung, https://www.bzfe.de/service/news/aktuelle-meldungen/news-archiv/meldungen-2021/juni/standard-titel/ (28.5.2023)
Kroh, M. (2022): Mit dem digitalen Zwilling in die Logistik von morgen. https://www.ey.com/de_de/consulting/mit-dem-digitalen-zwilling-in-die-logistik-von-morgen (28.5.2024)
Kühl, E. (2021): Ein Hackerangriff, der um die Welt geht. https://www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187 (28.5.2024)
Kuruwitaarachchi, N. et al. (2019): A Systematic Review of Security in Electronic Commerce Threats and Frameworks. Global Journal of Computer Science and Technology 19(1), S. 1–8
Levi, A. (2015): CS 432 Computer and Network Security. https://slideplayer.com/slide/5774818/ (28.5.2024)
LVN (Landesvereinigung der Milchwirtschaft Niedersachsen e. V.) (2020): Melkroboter entlasten von Routinearbeiten. https://milchland.de/melkroboter-entlasten-von-routinearbeiten/ (28.5.2023)
LZ direkt (Lebensmittel-Zeitung) (2022): Digitale Preisschilder: Flexibilität in Nullkommanichts. https://www.lzdirekt.de/pos-wissen/news/elektronische-preisauszeichnung-esl-839 (28.5.2024)
LZ (2023): Top 10 Geflügelwirtschaft 2023. https://www.lebensmittelzeitung.net/industrie/rankings/ranking-top-10-gefluegelwirtschaft-2023-174684 (28.5.2024)
Mai, K. et al. (2023): Warning: Humans cannot reliably detect speech deepfakes. https://doi.org/10.1371/journal.pone.0285333 (28.5.2024)
Martens, N. (2023): Die 7 besten Warenwirtschaftssysteme im Vergleich. OMR Reviews, https://omr.com/de/reviews/contenthub/beste-warenwirtschaftssysteme (28.5.2024)
Mayerhofer, L. (2022): Störungen bei Kartenzahlungen dauern an: Auch Aldi und Edeka betroffen. Merkur, https://www.merkur.de/wirtschaft/stoerung-kartenzahlung-loesung-supermarkt-anbieter-ec-kredikarte-baeckerei-edeka-aldi-tankstelle-zr-91574321.html (28.5.2024)
McCrea, B. (2022): Semiconductor Shortage Drives More Counterfeiting. Supply Chain Connect, https://www.supplychainconnect.com/counterfeit/article21237233/semiconductor-shortage-drives-more-counterfeiting (28.5.2024)
McKay, T. (2021): Ransomware Jerks Helped Cause the Cream Cheese Shortage. GIZMODO, https://gizmodo.com/ransomware-jerks-helped-cause-the-cream-cheese-shortage-1848195368 (28.5.2024)
Melnyk, S. et al. (2022): New challenges in supply chain management: cybersecurity across the supply chain. https://doi.org/10.1080/00207543.2021.1984606 (28.5.2024)
Microsoft (2022): Microsoft Digital Defense Report 2022: Illuminating the threat landscape and empowering a digital defense. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us (28.5.2024)

Milchindustrie-Verband e. V. (2020): Milch und mehr – die deutsche Milchwirtschaft auf einen Blick. https://milchindustrie.de/wp-content/uploads/2020/09/Fakten-Milch-September-2020.pdf (28.5.2024)
Milchindustrie-Verband e. V. (o. J.): Molkerei. https://milchindustrie.de/milkipedia/molkerei/ (28.5.2024)
Monteiro, A.; Santos, S.; Gonçalves, P. (2021): Precision Agriculture for Crop and Livestock Farming. https://doi.org/10.3390/ani11082345 (28.5.2024)
Muncaster, P. (2020): Americold Operations Downed by Cyber-Attack. Infosecurity Magazine, https://www.infosecurity-magazine.com/news/americold-operations-downed-by/ (28.5.2024)
Nikander, J.; Manninen, O.; Laajalahti, M. (2020): Requirements for cybersecurity in agricultural communication networks. https://doi.org/10.1016/j.compag.2020.105776 (28.5.2024)
Noss, M.; Machemehl, N.; Donie, W. (2022): Lebensmittellogistik. NORD/LB, https://www.nordlb.de/meine-nordlb/download/research-dokument-10789?cHash=f5b9c0da45f298267bbf158d86659cbe (28.5.2024)
Nourian, A., Madnick, S. (2018) A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet. https://doi.org/10.1109/TDSC.2015.2509994 (28.5.2024)
Nusser, B. (2024): Rewe schiebt sich vor Edeka. doi.org/10.51202/0947-7527-2024-11-040 (28.5.2024)
O'Flaherty, K. (2024): AI threats: The importance of a concrete strategy in fighting novel attacks. ITPro, https://www.itpro.com/technology/artificial-intelligence/ai-threats-the-importance-of-a-concrete-strategy-in-fighting-novel-attacks (28.5.2024)
Oladimeji, S.; Kerner, S. (2023): SolarWinds hack explained: Everything you need to know. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (28.5.2024)
OpenKRITIS (o. J.): EU NIS 2 Cybersecurity. https://www.openkritis.de/eu/eu-nis-2-direktive-kritis.html (28.5.2024)
Paul, S.; Scheible, P.; Wiemer, F. (2022): Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication. https://doi.org/10.3233/JCS-210037 (28.5.2024)
Pohlink, C. (2022): Eine Quantum Journey – Von der Technologie zum konkreten Use Case. In: Wilms, A.; Neukart, F. (Hg.): Chancen und Risiken von Quantentechnologien. Wiesbaden, S. 101–114
Pöllinger-Zierler, A. et al. (2021): Sammelroboter zur Entmistung in Rinderlaufställen – Chancen und Grenzen!? https://oekl-bauen.at/dateien/EIP/2021_poellinger.pdf (28.5.2024)
Pollmer, U. (2017): Wenn Traktoren gehackt werden. Deutschlandfunk, https://www.deutschlandfunkkultur.de/mahlzeit-wenn-traktoren-gehackt-werden-100.html (28.5.2024)
QTRADO Logistics GmbH & Co. KG (2023): Food Logistics. https://qtrado-logistics.de/wiki/food-logistics/ (28.5.2024)
Remondino, M.; Zanin, A. (2022): Logistics and Agri-Food: Digitization to Increase Competitive Advantage and Sustainability. https://doi.org/10.3390/su14020787 (28.5.2024)
Rodríguez García, M.; Agmoni, E. (2024): The Warehouse of the Future: Toward Highly Automated, Interconnected, Sustainable Warehouses. MIT Center for

Transportation & Logistics, https://ctl.mit.edu/pub/report/warehouse-future (28.5.2024)
Rohleder, B.; Meinel, T. (2022): Die Digitalisierung der Landwirtschaft. Bitkom e. V., https://www.bitkom.org/sites/main/files/2022-05/Bitkom-Charts%20Landwirtschaft.pdf (28.5.2024)
Rohleder, B.; Minhoff, C. (2019): Ernährung 4.0 – Status Quo, Chancen und Herausforderungen. Bitkom e. V.; BVE, https://www.bitkom.org/sites/main/files/2019-03/Bitkom-Charts%20190326%20Digitalisierung%20der%20Ern%C3%A4hrungsindustrie.pdf (28.5.2024)
SAP SE (o. J.): What is ERP? https://www.sap.com/products/erp/what-is-erp.html (28.5.2024)
Schimak, F. (2022): Kassensystem abgestürzt: Mehrere dm-Filialen in Deutschland komplett dicht. Hallo München, https://www.hallo-muenchen.de/ratgeber/verbraucher/dm-maerkte-geschlossen-kassensystem-abgestuerzt-mehrere-filialen-in-deutschland-dicht-zr-91609713.html (28.5.2024)
Schirrmacher, D. (2023): secIT 2023: Überfluten von ChatGPT erzeugte Trojaner das Internet? heise online, https://www.heise.de/news/secIT-2023-Ueberfluten-von-ChatGPT-erzeugte-Trojaner-das-Internet-7494341.html (28.5.2024)
Schlatt, V. et al. (2023): Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. https://doi.org/10.1016/j.ijinfomgt.2022.102470 (28.5.2024)
Schrauf, S. et al. (2020): Connected and autonomous supply chain ecosystems 2025. PricewaterhouseCoopers GmbH, https://www.pwc.de/de/digitale-transformation/connected-and-autonomous-supply-chain-ecosystems-2025-web.pdf (28.5.2024)
Schrode, A. et al. (2019): Transformation des Ernährungssystems: Grundlagen und Perspektiven. Umweltbundesamt, Texte 84, Dessau-Roßlau
Schwartz, M. (2023): Malware Taps Generative AI to Rewrite Code, Avoid Detection. https://www.bankinfosecurity.com/malware-taps-generative-ai-to-rewrite-code-avoid-detection-a-21972 (28.5.2024)
Seals, T. (2020): Food-Supply Giant Americold Admits Cyberattack. Threatpost, https://threatpost.com/food-supply-americold-cyberattack/161402/ (28.5.2024)
Sen, R. (2018): Challenges to Cybersecurity: Current State of Affairs. https://doi.org/10.17705/1CAIS.04302 (28.5.2024)
Shepel, J. (2021): Schreiber Foods hit with cyberattack; plants closed. Wisconsin State Farmer, https://eu.wisfarmer.com/story/news/2021/10/26/schreiber-foods-hit-cyberattack-plants-closed/8558252002/ (28.5.2024)
Sherstobitoff, R. (2021): JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified. SecurityScorecard, https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march (28.5.2024)
Sinnott, A.; Kennedy, E.; Bokkers, E. (2021): The effects of manual and automated milk feeding methods on group-housed calf health, behaviour, growth and labour. https://doi.org/10.1016/j.livsci.2020.104343 (28.5.2024)
Smetana, S.; Aganovic, K.; Heinz, V. (2021): Food Supply Chains as Cyber-Physical Systems: a Path for More Sustainable Personalized Nutrition. https://doi.org/10.1007/s12393-020-09243-y (28.5.2024)
Spohrer, S. (2023): Intelligente Bewässerung: Wasser und Energie effizienter einsetzen. https://www.bauernzeitung.de/agrarpraxis/intelligente-bewaesserung-wasser-und-energie-effizienter-einsetzen/ (28.5.2024)

Statista (2023): Techniktrends im Handel. https://de.statista.com/statistik/studie/id/25040/dokument/techniktrends-im-handel-statista-dossier/ (28.5.2024)
Statista (2024): Milchverarbeitung in der EU. https://de.statista.com/statistik/studie/id/31541/dokument/milchverarbeitung-in-der-eu-statista-dossier/ (28.5.2024)
Stock, I. (2024): Stuxnet: Wie ein Ingenieur das iranische Atomprogramm sabotiert haben soll. Heise online, https://www.heise.de/news/Stuxnet-Niederlaendischer-Geheimdienst-half-wohl-bei-Sabotage-im-Iran-9596851.html (28.5.2024)
Stupp, C. (2019): Fraudsters Used AI to Mimic CEOs Voice in Unusual Cybercrime Case. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (28.5.2024)
Stygar, A. et al. (2021): A Systematic Review on Commercially Available and Validated Sensor Technologies for Welfare Assessment of Dairy Cattle. https://doi.org/10.3389/fvets.2021.634338 (28.5.2024)
Symantec Corporation (2014): Attacks on point-of-sales systems. https://docs.broadcom.com/doc/attacks-on-point-of-sale-systems-en (28.5.2024)
TAB (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag) (2010): Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung. https://doi.org/10.5445/IR/1000103291 (28.5.2024)
TAB (2021): Digitalisierung der Landwirtschaft. Technologischer Stand und Perspektiven. https://doi.org/10.5445/IR/1000142950 (28.5.2024)
TAB (2023): Chancen und Risiken der Digitalisierung kritischer kommunaler Infrastrukturen an den Beispielen der Wasser- und Abfallwirtschaft. https://doi.org/10.5445/IR/1000163177 (28.5.2024)
Taddeo, M.; McCutcheon, T.; Floridi, L. (2019): Trusting artificial intelligence in cybersecurity is a double-edged sword. https://doi.org/10.1038/s42256-019-0109-1 (28.5.2024)
Tangalakis-Lippert, K. (2022): Russische Truppen stahlen in der Ukraine teure Landmaschinen – doch der Hersteller John Deere legte sie per Fernsteuerung still. Business Insider, https://www.businessinsider.de/wirtschaft/russische-truppen-stahlen-in-der-ukraine-landmaschinen-hersteller-john-deere-legte-sie-per-fernsteuerung-komplett-still-d/ (28.5.2024)
taz (2021). Nach Hackerangriff auf IT-Firma Kaseya:Bis zu 1.500 Firmen betroffen: https://taz.de/Nach-Hackerangriff-auf-IT-Firma-Kaseya/!5784244/ (12.8.2024)
TeamViewer (2024): Vandemoortele setzt für Digitalisierung in der Lagerlogistik auf TeamViewers Vision-Picking-Lösung. https://www.teamviewer.com/de/global/company/press/2024/teamviewer-improves-warehouse-operations-at-vandemoortele-with-vision-picking/ (28.5.2024)
Tropé, V. (2022): Warehouse-Management-Systeme: Damit läufts im Lager. OMR Reviews, https://omr.com/de/reviews/contenthub/warehouse-management-system (28.5.2023)
trusted (o. J.) Beste Point of Sale (POS) Software 2024 »29 Tools im Vergleich. https://trusted.de/pos-point-of-sale (28.5.2024)
TÜV Rheinland i-sec GmbH (2019): Industrielle Robotertechnik und Cybersecurity. https://www.tuv.com/content-media-files/master-content/services/industrial-services/pdf/tuv-rheinland-de21_i07_fscs_2100131_de_whitepaper_fscs_a4_web.pdf (28.5.2024)
UP KRITIS (2023): Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen. Ver-

sion 4.0. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-anforderungen-lieferanten.pdf?__blob=publicationFile&v=14 (28.5.2024)
VDM (Verband deutscher Mühlen) (o. J.): Mühlen in Deutschland. Stand: September 2023, https://www.muehlen.org/branche/muehlen-in-deutschland (28.5.2024)
von Skarczinski, B.; Raschke, M.; Teuteberg, F. (2023): Modelling maximum cyber incident losses of German organisations: an empirical study and modified extreme value distribution approach. https://doi.org/10.1057/s41288-023-00293-x (28.5.2024)
VuMA (Arbeitsgemeinschaft Verbrauchs- und Medienanalyse) (2021): Bevölkerung in Deutschland nach Häufigkeit der Nutzung von Lieferdiensten für fertige Mahlzeiten (Pizza etc.) in den Jahren 2018 bis 2021. Statista, https://de.statista.com/statistik/daten/studie/290947/umfrage/umfrage-in-deutschland-zu-haeufigkeit-der-nutzung-von-pizza-lieferdiensten/ (28.5.2024)
Wolfangel, E. (2021): Wenn die Ernte plötzlich ausfällt. In: MIT Technology Review 7, S. 56–59
Yaseen, A.; Channi, H.; Sharma, A. (2022): PLC/ SCADA Based Automation of Milk Processing (Pasteurization) Plants. In: Recent Trends in Instrumentation and Control (RTIC 2022), Chennai, S. 92–100

7 Anhang

7.1 Abbildungen

7.2 Kästen

BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG BEIM DEUTSCHEN BUNDESTAG

Karlsruher Institut für Technologie

Neue Schönhauser Straße 10
10178 Berlin

Telefon: +49 30 28491-0
E-Mail: buero@tab-beim-bundestag.de
Web: www.tab-beim-bundestag.de
Twitter: @TABundestag