TAB
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Cybersicherheit in der Nahrungsmittelversorgung

TAB-Fokus Nr. 47 zum Arbeitsbericht Nr. 213 Oktober 2024

In Kürze

- Mit der Digitalisierung und Vernetzung technischer Systeme steigt die Verwundbarkeit von Unternehmen der Nahrungsmittelkette gegenüber Bedrohungen aus dem Cyberraum.
- Im landwirtschaftlichen Sektor könnten sich vor allem Supply-Chain-Angriffe auf die Hersteller von Betriebstechnik oder externe Dienstleister auf die Produktion und Lieferung von Lebensmitteln auswirken.
- Verarbeitung, Logistik und Handel haben einen vergleichsweise höheren Digitalisierungsgrad erreicht und weisen eine höhere Konzentration auf. Ohne Zugriff auf zentrale IT-Systeme können notwendige Dienste oft nicht mehr erbracht werden.
- Mit der Umsetzung der NIS-2-Richtlinie in deutsches Recht werden externe Dienstleister, Anbieter kritischer IT-Technik und Lieferanten stärker in die Pflicht genommen, der Anwendungsbereich von Cybersicherheitspflichten auf mittlere Betriebe erweitert und der Fokus auf die Lieferketten gestärkt. Diese Maßnahmen sollen die identifizierten Risiken verringern.
- Um das Risiko von Cyberangriffen auf eine Vielzahl kleinerer Betriebe und ihre Dienstleister zu reduzieren, wären Maßnahmen umzusetzen, die diese in die Lage versetzen, sich vor Cyberangriffen besser zu schützen, ohne unnötigen bürokratischen Aufwand zu schaffen.
- Die Wissenslücken über den Stand der Cybersicherheit sind insgesamt groß. Die Datenlage zur Verbreitung digitaler Technologien, zu Störfällen und Schutzniveaus ist verbesserungswürdig.

Worum es geht

Mit der Digitalisierung und Vernetzung technischer Systeme steigt die Verwundbarkeit von Unternehmen der Nahrungsmittelkette gegenüber Bedrohungen aus dem Cyberraum. Die Bedrohungslage für die IT-Sicherheit im Jahr 2023 war höher als je zuvor. Der Sektor Ernährung (Lebensmittelproduktion, -verarbeitung und -handel) gehört zu den kritischen Infrastrukturen, die besonders zu schützen sind. Im Hinblick auf die Informationssicherheit geschieht dies durch das BSI-Gesetz, das große Unternehmen im Ernährungssektor verpflichtet, ihre IT-Systeme nach dem Stand der Technik abzusichern. Allerdings sind gerade die Landwirtschaft und das Lebensmittelhandwerk stark von kleinen und mittleren Unternehmen geprägt, für welche die Verpflichtungen des BSI-Gesetzes bisher nicht galten. Mit der Umsetzung der Richtlinie (EU) 2022/2555 (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 kritischer Infrastrukturen, sondern auch mittlere Unternehmen in die Pflicht genommen, ihre Systeme gegen IT-Sicherheitsvorfälle abzusichern. Im TAB-Arbeitsbericht werden die Vulnerabilitäten der Nahrungsmittelversorgung in Deutschland vor dem Hintergrund möglicher Bedrohungen aus dem Cyberraum beleuchtet und Handlungsoptionen zur Stärkung der Cyberresilienz des Sektors skizziert.

Landwirtschaftliche Systeme

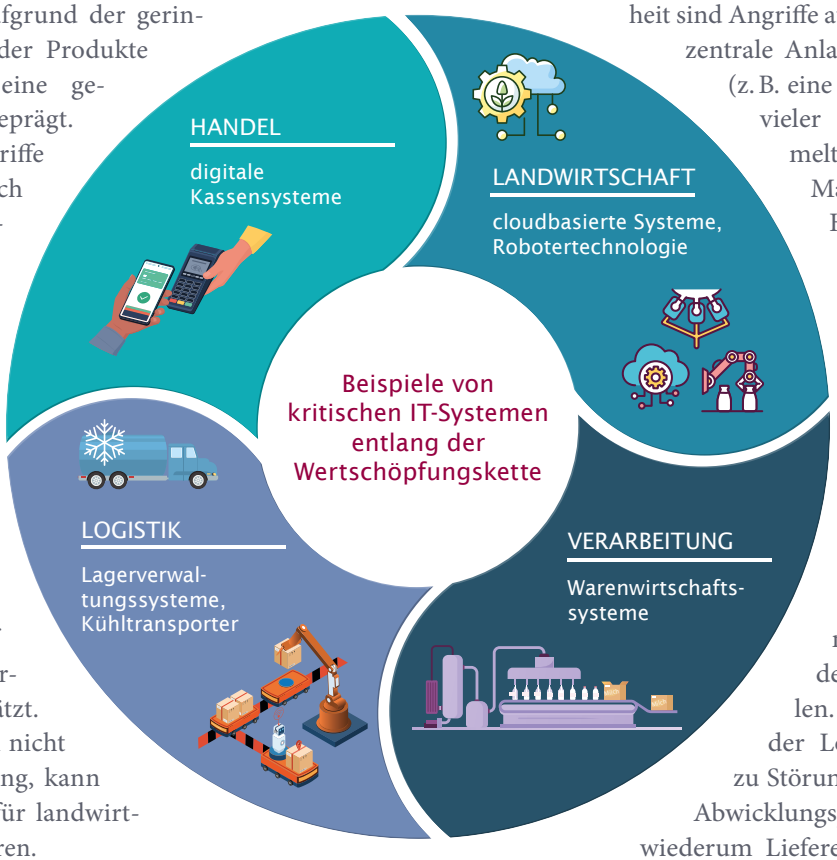
Auch wenn die Landwirtschaft bisher nicht das Hauptziel ausgeklügelter Angriffe auf die Betriebstechnik war, könnte sich dies durch die rasche Digitalisierung landwirtschaftlicher Betriebe ändern. Aufgrund der hohen Anzahl kleiner und mittlerer Betriebe in der Landwirtschaft kann nahezu ausgeschlossen werden, dass Angriffe auf einzelne Betriebe sich auf die Lebensmittelversorgung insgesamt auswirken würden. Viel eher könnte ein Angriff auf die Hersteller der eingesetzten Betriebstechnik oder auf externe Dienstleister mit hoher Marktdurchdringung die Versorgung mit Produkten aus der Landwirtschaft beeinträchtigen.

In der Nutztierhaltung gilt dies für IT-Dienstleister wie Cloudhostingplattformen, die Speicherplatz, Rechenleistung und Datenbanken zur Verfügung stellen, sowie Anbieter

Auftraggeber
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung
+49 30 227-32861
bildungundforschung@bundestag.de

cloudbasierter Systeme. Ähnlich problematisch kann sich der Ausfall von Internet- oder Labordiensten auswirken. Neben indirekten Angriffen auf Dienstleister mit hohem Marktanteil können auch solche IT-Systeme direkt angegriffen werden, die standardmäßig in der Nutztierhaltung eingesetzt werden und eine hohe Kritikalität aufweisen. Dazu zählen insbesondere die auf Robotertechnologie basierenden Bewässerungssysteme im pflanzlichen Anbau und Stallbelüftungs- sowie automatische Melksysteme in Milchviehbetrieben.

Der Pflanzenbau ist aufgrund der geringeren Verderblichkeit der Produkte grundsätzlich durch eine geringere Kritikalität geprägt. Dennoch bergen Angriffe auf die Lieferkette auch in der Pflanzenproduktion ein relevantes Gefahrenpotenzial. Dies betrifft Angriffe auf Händler von Saatgut und Düngemitteln während der Aussaat- und Pflanzsaison. Darüber hinaus werden Angriffe auf die Flotten von Landtechnikherstellern bzw. auf Landmaschinen als wahrscheinlich eingeschätzt. Stehen Erntemaschinen nicht rechtzeitig zur Verfügung, kann dies zum Totalverlust für landwirtschaftliche Betriebe führen.



Verarbeitung

Im Vergleich zu einem Ausfall der Technik in der Landwirtschaft kann ein Ausfall der Technik in der Lebensmittelverarbeitung schneller weitreichende Auswirkungen haben. Grund dafür ist, dass viele kritische Prozesse der Verarbeitung durch eine hohe Abhängigkeit von IT-Systemen – zunehmend auch vom Internetzugang – gekennzeichnet sind. Ohne Zugriff auf die zentralen Systeme, insbesondere auf das Warenwirtschaftssystem, können die erforderlichen Dienste oft nicht mehr erbracht werden. Die Auswirkungen von Produktionsausfällen auf die Ernährungssicherheit hängen insbesondere von der Verderblichkeit der betroffenen Produkte und der Anzahl der zu versorgenden Personen ab. Besonders bedrohlich für die Versorgungssicherheit sind Angriffe auf Unternehmen, die als zentrale Anlaufpunkte für Produkte (z. B. eine Molkerei, die die Milch vieler Milcherzeuger sammelt) fungieren. Eine hohe Marktkonzentration gibt Hinweise auf mögliche Schwachstellen.

Logistik

Angriffe auf IT-Systeme, die logistische Prozesse unterstützen, werden als besonders schwerwiegend eingestuft. Denn die Logistik kann einen neuralgischen Punkt in der Lieferkette darstellen. Beeinträchtigungen der Logistiksysteme können zu Störungen im Transport- und Abwicklungsprozess führen, was wiederum Lieferengpässe und eine Beeinträchtigung der Produktverfügbarkeit zur Folge haben kann. Besonders kritisch ist der Ausfall von zentralen Steuerungssystemen, wie Warenwirtschafts- oder Lagerverwaltungssysteme, wodurch z. B. Aufträge im Logistiklager (Abb.) nicht mehr bearbeitet werden können.

Typische Einfallstore für großangelegte Cyberattacken

Zu den häufigsten und gefährlichsten Angriffsarten zählen insbesondere Ransomware, Phishing sowie (D)DoS-Angriffe.

- Ransomware: Unter Ransomware wird eine Manipulation, Zerstörung oder Verschlüsselung von Daten verstanden, verbunden mit der Aufforderung zur Zahlung eines Lösegelds. 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.
- 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 ver-

Illustration: morepiixel, bsd studio, Sergii Pavlovskyi, Sarawut, Siberian Art, elenabsl (alle Adobe Stock)

Auch die Vernetzung von Systemen zwischen Handelspartnern entlang der Wertschöpfungskette birgt neue Risiken für Logistikunternehmen, da sich Vorfälle aufgrund schwacher Cybersicherheitsmaßnahmen bei einem Lieferanten schneller als in der Vergangenheit auf Partner in der Lieferkette ausbreiten können. Der steigende Zugriff auf Clouddienste für die Speicherung von Daten zwischen Handelspartnern wird in dieser Hinsicht als besonders problematisch angesehen. Dass Störungen weitreichende Konsequenzen haben können, liegt auch daran, dass viele Logistikprozesse so aufeinander abgestimmt werden, dass Waren in der exakten Menge und zum richtigen Zeitpunkt am richtigen Ort sind, 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 Kühlfahrzeugen oder die Fernwartung von Kühlhäusern sein.

Abb. Lagersystem der Ocado-Gruppe im Onlinehandel

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 über den Angriffsvektor Phishing, wodurch Datenschutzverletzungen entstehen können. In der Regel bleibt die Verfügbarkeit der Kerndienste auch bei Datenschutzverletzungen unberührt. Unter den Angriffen, die auf informationstechnische Systeme (IT-Systeme) des Handels stattfinden können, stellen solche auf zentrale Verwaltungssysteme, aber auch auf digitale Kassensysteme derzeit die größte Gefahr für den Einzelhandel dar. Entsprechende Vorfälle können prinzipiell den Zugang zu Lebensmitteln erschweren. Bisher konnten die Folgen einzelner Störungen durch das dichte Supermarktnetz in Deutschland abgefedert werden, allerdings besteht durch die starke Konzentration des Lebensmittelhandels in Deutschland die Gefahr einer Homogenisierung der eingesetzten Systeme, wodurch skalierte Angriffe über Softwareupdates gefährlich werden könnten. Noch problematischer kann sich ein indirekter Angriff auf einen externen IT-Dienstleister erweisen, wenn die Mehrzahl der Einzelhandelsfilialen auf den gleichen Service 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 Anbindung an das Internet eine neue Angriffsfläche für Hacker bieten, zu einer erhöhten Verletzlichkeit führen.

Für den Onlinehandel stellen Angriffe von Cyberkriminellen eine besonders große Gefahr dar, denn dabei spielen Webserver und Automatisierung der Logistik eine zentrale Rolle. Ihr Ausfall bringt eine Bedrohung für die Verfügbar-

leitet 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, das 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. Eindämmung und Abwehr von (D)DoS-Angriffen stellen für Unternehmen eine große Herausforderung dar.

Abb.: Rodríguez García, M.; Agmoni, E. (2024): The Warehouse of the Future: Toward Highly Automated, Interconnected, Sustainable Warehouses. MIT Center for Transportation & Logistics

keit der Kernleistungen mit sich. 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 entscheidender Bedeutung und sollten daher in hohem Maße geschützt werden. Sicherheitsmaßnahmen können jedoch hohe Kosten verursachen. Es ist daher notwendig, die größten Bedrohungen zu identifizieren, um Anhaltspunkte für angemessene Vorkehrungen zu finden, die einen ausreichenden Schutz gewährleisten. Um die Nahrungsmittelversorgung zu sichern, müssen u. a. die Versorgung mit Energie bzw. Strom, mit Wasser für den Anbau von Pflanzen und für die Tierhaltung sowie eine funktionierende Infrastruktur der Informations- und Kommunikationstechnik (IKT) gewährleistet sein. Darüber hinaus kann ein Angriff auf IT-Systeme insbesondere dann weitreichende Folgen haben, wenn:

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

Die hohe Vielfalt der Produkte und Unternehmen im Ernährungssektor sorgte dafür, dass der Ausfall eines Anbieters bzw. eines Betriebs in den meisten Fällen keine gravierenden Folgen für die Versorgung der Bevölkerung hat. Daher sind 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 steigender Risiken durch die Vernetzung und Integration von Systemen und Daten sowohl innerhalb einzelner Betriebe als auch entlang der Wertschöpfungskette sowie der Möglichkeiten, Angriffe auf eine Vielzahl kleinerer Betriebe oder durch Supply-Chain-Angriffe mittels KI leichter durchzuführen, ist eine Absenkung der Schwellenwerte und eine stärkere Fokussierung auf die Lieferketten sinnvoll. 2022 wurde die NIS-2-Richtlinie veröffentlicht. Die Umsetzung in Deutschland (derzeit im Gesetzgebungsverfahren) wird die Cybersicherheit des Sektors erhöhen. Insgesamt erfordert eine höhere Cybersicherheit in der Lebensmittelversorgung, dass externe Dienstleister und Anbieter kritischer IT-Technik stärker in die Pflicht genommen werden. Kleinere Betriebe müssen zu mehr Cybersicherheit motiviert und das Wissen über den Verbreitungsgrad von IT-Systemen, Störfälle und Schutzniveaus in der Branche sowie über Risiken durch neue Technologien verbessert werden. Besonders wichtig erscheinen auch Maßnahmen zur Verringerung des Mangels an IT-Fachkräften und zur Schärfung des Bewusstseins für Cyberrisiken.

TAB-Arbeitsbericht Nr. 213
Cybersicherheit in der Nahrungsmittelversorgung
Pauline Riousset

Projektinformationen
www.tab-beim-bundestag.de/cybersicherheit-ernaehrung

Projektleitung und Kontakt
Dr. Pauline Riousset
+49 30 28491-105
riousset@tab-beim-bundestag.de

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) berät das Parlament und seine Ausschüsse seit 1990 in Fragen des wissenschaftlich-technischen Wandels. Das TAB ist eine organisatorische Einheit des Instituts für Technikfolgenabschätzung und Systemanalyse (ITAS) im Karlsruher Institut für Technologie (KIT). Zur Erfüllung seiner Aufgaben kooperiert es seit September 2013 mit dem IZT – Institut für Zukunftsstudien und Technologiebewertung gGmbH sowie der VDI/VDE Innovation + Technik GmbH. Der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung entscheidet über das Arbeitsprogramm des TAB, das sich auch aus Themeninitiativen anderer Fachausschüsse ergibt. Die ständige »Berichterstattergruppe für TA« besteht aus dem Ausschussvorsitzenden Kai Gehring (Bündnis 90/Die Grünen) sowie je einem Mitglied der Fraktionen: Dr. Holger Becker (SPD), Lars Rohwer (CDU/CSU), Laura Kraft (Bündnis 90/Die Grünen), Prof. Dr. Stephan Seiter (FDP), Prof. Dr. Michael Kaufmann (AfD).