CYBERSECURITY & RESILIENCE

CII WHITE PAPER

Zahlen, Anforderungen und Maßnahmen:

Cybersicherheit für Waren- und Handelsgesellschaften im Ernährungssektor

Prof. Dr. Dennis-Kenji Kipker

Powered by: AWADO

CYBER|INTELLIGENCE .Institute

Inhalt

Über den Autor

Prof. Dr. Dennis-Kenji Kipker ist wissenschaftlicher Direktor des cyber-intelligence.institute in Frankfurt a.M., Vorstand der Strategieberatungs-gesellschaft CERTAVO AG sowie Gastprofessor an der privaten, durch die Soros Foundation begründeten Riga Graduate School of Law in Lettland. Hier forscht er zu Themen an der Schnittstelle von Recht und Technik in der Cybersicherheit, Konzernstrategie sowie zu digitaler Resilienz im Kontext globaler Krisen mit einem Forschungs-schwerpunkt insbesondere im chinesischen und US-amerikanischen IT-Recht.

Kontakt: dennis.kipker@cyberintelligence.institute

Executive Summary

Die zunehmende Digitalisierung im Ernährungssektor macht Cybersicherheit zu einer zentralen Herausforderung – nicht nur für Kritische Infrastrukturen, sondern für eine Vielzahl von Unternehmen entlang der Wertschöpfungskette. Die europäische NIS-2-Richtlinie, die bis Oktober 2024 in deutsches Recht umzusetzen war, verpflichtet auch mittlere Unternehmen zur Einführung angemessener technischer, organisatorischer und personeller Maßnahmen im Bereich der Informationssicherheit.

Besonders betroffen ist der Bereich „Produktion, Verarbeitung und Vertrieb von Lebensmitteln“, der zu den kritischen Sektoren zählt. Der Anwendungsbereich reicht dabei weit über große Konzerne hinaus: Auch kleinere Agrarbetriebe, genossenschaftlich organisierte Handelsunternehmen oder gewerbliche Lebensmittelhändler unterliegen – abhängig von Größe, Relevanz oder Lieferkettenintegration – neuen Compliance-Anforderungen.

Die betrieblichen Voraussetzungen zur Erfüllung dieser Anforderungen unterscheiden sich erheblich. Während größere Unternehmen oft über strukturierte IT-Umgebungen, ERP-Systeme und interne IT-Sicherheitsbeauftragte verfügen, fehlen in kleinen und mittleren Betrieben häufig grundlegende Maßnahmen wie IT-Notfallpläne, dokumentierte Risikoanalysen oder strukturierte Berichtssysteme. Eine branchenspezifische Gap-Analyse zeigt insbesondere im genossenschaftlichen Sektor bestehende Schwächen in den Bereichen Dokumentation, Vorfallsmanagement und IT-Governance.

Herausfordernd ist zudem die zunehmende Cloud-Nutzung, die Kontrolle über externe IT-Dienstleister und die Sicherstellung von Cybersicherheit über die gesamte digitale Lieferkette hinweg. Die Heterogenität der IT-Systeme – etwa durch Eigenentwicklungen oder stark variierende Digitalisierungsgrade – erschwert zudem eine standardisierte Umsetzung. Dennoch ist ein ganzheitliches Risikomanagement essenziell: Informationssicherheit muss als fortlaufender betrieblicher Prozess verstanden werden, der technische, personelle und organisatorische Aspekte integriert.

Um den neuen Anforderungen gerecht zu werden, bedarf es insbesondere in kleinen und mittleren Unternehmen aus dem agrargenossenschaftlichen Umfeld eines pragmatischen, ressourcenschonenden Ansatzes – etwa durch die Nutzung externer Informationssicherheitsbeauftragter, digitaler GRC-Tools oder der Etablierung branchenspezifischer Sicherheitsstandards.

Teil 1

NIS-2 und die Bedeutung der EU-Richtlinie zur allgemeinen unternehmensbezogenen Cybersicherheit

Die Cybersicherheit ist eine Grundvoraussetzung für die ordnungsgemäße Funktion des Wirtschaftslebens. Diese Erkenntnis ist mittlerweile bei einem Großteil der deutschen Unternehmen angelangt. Der BSI-Lagebericht aus dem Jahr 2023 spiegelt diese Entwicklung in aktuellen Zahlen wider: So sehen 80 % der Unternehmen die Funktionsfähigkeit ihrer IT als essenziell für einen reibungslosen Geschäftsablauf an. Zitiert wird ebenso eine Umfrage des TÜV-Verbands aus dem Jahr 2023, in welcher 95 % der befragten Unternehmen feststellen, dass Cybersicherheit ein Muss für den Schutz der Unternehmensdaten ist.[1] Im BSI-Lagebericht aus dem Jahr 2024 wird deshalb zu Recht dazu aufgerufen, Angriffsflächen im Unternehmen zu ermitteln und zu schützen, denn mit der stetig zunehmenden allgemeinen Digitalisierung erhöht sich zwangsläufig ebenso der Handlungsbedarf für die Cybersicherheit, denn Angreifer suchen beständig nach neuen Angriffsvektoren.[2] Deutlich wird damit, dass die IT-Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Nichtabstreitbarkeit eine Dimension besitzen, die über die abstrakte Gewährleistung der Aufrechterhaltung von Betriebsabläufen hinausgehen und auch über eine Relevanz für die Einhaltung von rechtlichen Vorgaben wie zum Beispiel dem Datenschutz verfügen.

> **Die IT-Schutzziele umfassen alle Maßnahmen, die getroffen werden, um Daten und Informationen vor schädlichen Einflüssen zu schützen. Insoweit haben sie eine wesentliche Bedeutung für Unternehmen.** HARRY KLEINGARN

Diese Entwicklung zeichnet sich auch bei den unternehmerischen Entscheidungen in der Cybersicherheit zunehmend deutlich ab. So sind die Ausgaben für das IT-Sicherheitsbudget der Unternehmen seit dem Jahr 2020 laut BSI kontinuierlich und signifikant gestiegen: 2022 wurden in etwa 7.8 Milliarden Euro in die Cybersicherheit investiert – ein Betrag so hoch wie nie zuvor. Das Statistische Bundesamt geht zusätzlich von einer jährlichen Wachstumsrate von 10,5 % aus.[3]

Diese Entwicklung ist bemerkenswert, denn bis zum Jahr 2015 war Cybersicherheit vor allem eines: ein branchenspezifisches Fachthema. Eigenständige Gesetzgebung war in diesem Zusammenhang weitestgehend unbekannt, und die technisch-organisatorische Absicherung von Datenverarbeitungsprozessen war vor allem an den technischen Datenschutz angeknüpft. Erstmalig änderte sich diese Wahrnehmung mit dem ersten IT-Sicherheitsgesetz aus dem Jahr 2015, das die IT-sicherheitsbezogene Regulierung der Kritischen Infrastrukturen in Deutschland mit sich brachte. Ergänzt wurden die nationalen Vorgaben sodann um die europäische NIS-1-Richtlinie aus 2016, die daneben nun auch eine Regulierung der Anbieter von digitalen Diensten (Cloud Computing, Online-Marktplätze, Online-Suchmaschinen) vorsah. Mit dem deutschen IT-Sicherheitsgesetz 2.0 aus 2021 wurde Cybersicherheit dann erstmals von einer Aufgabe ausschließlich für KRITIS-Betreiber zur Gewährleistungsverantwortung im Bereich des allgemeinen Wirtschaftsschutzes erhoben. Als sog. „Artikelgesetz“, das verschiedene nationale Rechtsvorschriften zur Cybersicherheit novellierte, schuf es nicht nur neue Befugnisse für die nationale deutsche Cybersicherheitsbehörde, das Bundesamt für Sicherheit in der Informationstechnik (BSI) und brachte zusätzliche Pflichten für die ohnehin schon regulierten KRITIS-Betreiber mit sich, sondern regulierte erstmals

1 BSI, Die Lage der IT-Sicherheit in Deutschland 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html
2 BSI, Die Lage der IT-Sicherheit in Deutschland 2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html
3 BSI-Lagebericht 2023, S. 55

ebenfalls die „Unternehmen im besonderen öffentlichen Interesse“. Über diese Kategorie u.a. solcher Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung sind, wurde der rechtlich regulierte Cyberschutz in Deutschland erstmals auch jenseits der Kritischen Infrastrukturen in den Rang einer allgemeinen Management-Aufgabe erhoben. Hinzu kam seinerzeit neuerdings ebenso, dass mit den Zulieferern, die wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind, die Lieferkette reguliert wurde. Diese Entwicklung von Cybersecurity Compliance als nahezu ausschließlicher KRITIS-Aufgabe hin zu einer Aufgabe des allgemeinen Wirtschaftsschutzes setzt sich schließlich mit der europäischen NIS-2-Richtlinie fort.

Die NIS-2-Richtlinie (Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 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) wurde Ende Dezember 2022 im Amtsblatt der Europäischen Union veröffentlicht und löst die erste EU NIS-Richtlinie aus dem Jahr 2016 ab. Da es sich um eine EU-Richtlinie und nicht um eine EU-Verordnung handelt, ist sie durch die europäischen Mitgliedstaaten bis zum 17. Oktober 2024 in das nationale Recht umzusetzen. In Deutschland ist die Umsetzung verzögert. Ursprünglich sollte diese durch das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz oder kurz auch NIS2UmsuCG) erfolgen. Durch ein umfassendes NIS-2-Umsetzungsgesetz würde das nationale deutsche Cybersicherheitsrecht komplett umgestellt, insbesondere das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das die zentralen Befugnisse des BSI und die Cybersecurity-Pflichten u.a. für KRITIS-Betreiber und für die teilweise neu betroffenen Sektoren mit „hoher Kritikalität“ und „sonstige kritische Sektoren“ enthält. Diese Sektoren nach den Anhängen I und II der NIS-2-Richtlinie untergliedern sich im Allgemeinen wie folgt:

Sektoren nach Anhang I (Sektoren mit hoher Kritikalität)	**Sektoren nach Anhang II (sonstige kritische Sektoren)**
→ Energie	→ Post- und Kurierdienste
→ Verkehr	→ Abfallbewirtschaftung
→ Bankwesen	→ Produktion, Herstellung und Handel mit chemischen Stoffen
→ Finanzmarktinfrastrukturen	
→ Gesundheitswesen	→ **Produktion, Verarbeitung und Vertrieb von Lebensmitteln**
→ Trinkwasser	
→ Abwasser	→ Verarbeitendes Gewerbe/Herstellung von Waren
→ Digitale Infrastruktur	
→ Verwaltung von IKT-Diensten	→ Anbieter digitaler Dienste
→ Öffentliche Verwaltung	→ Forschungseinrichtungen
→ Weltraum	

Um als Einrichtung bzw. Wirtschaftsbetrieb von den Cybersecurity Compliance-Anforderungen nach NIS-2 betroffen zu sein, muss grundsätzlich zusätzlich zur qualitativen, d.h. sektoralen Betroffenheit, auch das Kriterium einer quantitativen, d.h. zahlenmäßigen Betroffenheit erfüllt sein. Diese zahlenmäßige Betroffenheit ergibt sich aus der Empfehlung 2003/361/EG betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (sog. „Size-Cap-Rule"). In Anlehnung daran liegt eine NIS-2-Betroffenheit grundsätzlich dann vor, wenn ein Unternehmen über mindestens 50 Beschäftigte verfügt oder einen Jahresumsatz und eine Jahresbilanz von über 10 Mio. Euro erzielt. Mit Blick sowohl auf das qualitative wie auch auf das quantitative Kriterium wird deutlich, dass sich mit NIS-2 bzw. mit dessen nationaler Umsetzung Cybersecurity Compliance zu einer branchenübergreifenden Aufgabe weit jenseits Kritischer Infrastrukturen entwickelt, die bis hin zu den mittelständischen Unternehmen reicht. Demgemäß wird in aktuellen Schätzungen auch von einer Betroffenheit von ca. 30.000–40.000 Unternehmen durch NIS-2 allein in Deutschland ausgegangen. Mit der qualitativen Bezugnahme auf den Ernährungssektor über die sonstigen kritischen Sektoren „Produktion, Verarbeitung und Vertrieb von Lebensmitteln" wird deutlich, dass mit NIS-2 nicht nur Kritische Infrastrukturen aus diesem Bereich, sondern ebenso mittelständische Unternehmen mit neuen Pflichten zur Cybersecurity Compliance konfrontiert werden, die durch die Betriebs- bzw. Geschäftsleitung auszusteuern und zu überwachen sind.

> **Eine digitale Lieferkette vernetzt sämtliche Beteiligte und Prozesse innerhalb der Wertschöpfungskette mit Unterstützung von fortschrittlichen (digitalen) Technologien.** HARRY KLEINGARN

Eine zu berücksichtigende Besonderheit von NIS-2 ist außerdem, dass mit den neuen Vorgaben zum Risikomanagement im Bereich der Cybersicherheit auch die digitale Lieferkette erfasst wird und somit Betriebe, die eigentlich vielleicht sogar aus dem Anwendungsbereich herausfallen, im Rahmen dieser digitalen Lieferkette zu zusätzlichen Maßnahmen in der Cybersicherheit verpflichtet werden, dies kann beispielsweise durch Vertragswerke zwischen NIS-2-Unternehmen und ihren Zulieferern geschehen. Begrifflich umschreibt diese Vorgabe die „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern".

Teil 2
Anwendungsbereich, Fragestellung und Zielsetzung

Diese Studie verfolgt das Ziel, für den weit gefassten Ernährungssektor einerseits den Rahmen der Umsetzung der europäischen NIS-2-Richtlinie aufzuzeigen, andererseits aber auch Ansätze in der Cybersicherheit zu ermitteln, die über den Kontext von NIS-2 hinausgehen, da sich insbesondere der Ernährungssektor infolge seiner hohen betrieblichen Diversität von Kritischen Infrastrukturen über Großunternehmen bis hin zu kleinen und familiär betriebenen landwirtschaftlichen Unternehmungen erstreckt.

SILAS KÄMPCHEN:
Leiter IT-Spezialisten, AWADO

Das breite Branchenspektrum und die Produktvielfalt innerhalb der genossenschaftlichen Gruppe bedingen eine hohe Heterogenität der IT-Umgebungen. Grundlegende Prozesse sind regelmäßig vergleichbar, unterscheiden sich jedoch in Abhängigkeit der Unternehmensgrößen. Besonders die organisatorische Ausstattung der Genossenschaften ist regelmäßig geringfügiger ausgebaut als bei anderen Rechtsformen. Dies führt dazu, dass zwar oftmals branchenspezifische Schwellenwerte überschritten werden, diese jedoch mit wenig komplexen IT-Systemen und einer geringen Organisationsgröße erreicht werden. Damit wird diese betriebliche Diversität zu einer bedeutenden Herausforderung bei der Umsetzung gesetzlicher Mindestanforderungen.

Basierend auf dem Rechtsstand der Umsetzung des IT-Sicherheitsgesetzes 2.0 (IT-SiG 2.0) aus 2021 wurden in Deutschland die Kritischen Infrastrukturen als Einrichtungen, Anlagen oder Teile davon definiert, die unter anderem dem Sektor Ernährung angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Dieser allgemeine Zuschnitt des Anwendungsbereichs hat durch die BSI-Kritisverordnung (BSI-KritisV) Konkretisierung erfahren. Bestimmt wurde hier, dass die Lebensmittelversorgung – verstanden als Versorgung der Allgemeinheit mit Lebensmitteln – aufgrund ihrer besonderen Bedeutung eine kritische Dienstleistung im Sinne des IT-Sicherheitsrechts darstellt. Die Lebensmittelversorgung wird dabei in den Bereichen der Lebensmittelherstellung, -behandlung und dem Lebensmittelhandel erbracht. Bereits hier wird deutlich, dass die landwirtschaftliche Wertschöpfungskette im Ernährungssektor nicht nur komplex, sondern höchst divers mit Betrieben unterschiedlichster Größenordnung und IT-Nutzung ausgestaltet ist. In der BSI-KritisV werden die im Einzelnen erfassten Bereiche anhand des Schwellenwerts der Versorgungsgrenze von 500.000 zu versorgenden Personen konkretisiert:

Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Lebensmittelversorgung**		
1.1	Lebensmittelherstellung und -behandlung		
1.1.1	Anlage oder System zur Herstellung von Lebensmitteln	Hergestellte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		hergestellte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.1.2	Anlage oder System zur Behandlung von Lebensmitteln	Behandelte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		behandelte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.1.3	Anlage oder System zur Distribution von Lebensmitteln	Umgeschlagene Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		umgeschlagene Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.1.4	Anlage oder System zur zentralen Steuerung oder Überwachung	Hergestellte, behandelte, umgeschlagene, bestellte oder in Verkehr gebrachte Lebensmittel außer Getränke aller durch die Anlage oder das System gesteuerten oder überwachten Anlagen in Tonnen/Jahr oder	434 500
		hergestellte, behandelte, umgeschlagene, bestellte oder in Verkehr gebrachte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent aller durch die Anlage oder das System gesteuerten oder überwachten Anlagen in Liter/Jahr	350 000 000
1.2	Lebensmittelhandel		
1.2.1	Anlage oder System zur Behandlung von Lebensmitteln	Behandelte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		behandelte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.2.2	Anlage oder System zur Distribution von Lebensmitteln	Umgeschlagene Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		umgeschlagene Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.2.3	Anlage oder System zur Bestellung von Lebensmitteln	Bestellte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		bestellte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.2.4	Anlage oder System zum Inverkehrbringen von Lebensmitteln	In Verkehr gebrachte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		in Verkehr gebrachte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.2.5	Anlage oder System zur zentralen Steuerung oder Überwachung	Behandelte, umgeschlagene, bestellte oder in Verkehr gebrachte Lebensmittel außer Getränke aller durch die Anlage oder das System gesteuerten oder überwachten Anlagen in Tonnen/Jahr oder	434 500
		behandelte, umgeschlagene, bestellte oder in Verkehr gebrachte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent aller durch die Anlage oder das System gesteuerten oder überwachten Anlagen in Liter/Jahr	350 000 000

Diese skizzierten bislang bereits seit mehreren Jahren bestehenden regulatorischen Vorgaben werden durch die NIS-2-Richtlinie und ihre nationale Umsetzung für den Ernährungssektor aktualisiert und erweitert. Infolge der Bezugnahme auf die Empfehlung 2003/361/EG sind deshalb längst nicht mehr nur die Kritischen Infrastrukturen vom Anwendungsbereich umfasst. Überdies können die Anforderungen aus NIS-2 auch unabhängig von der Größe der betrieblichen Einrichtung gelten, sollte diese beispielsweise in einem Mitgliedstaat der einzige Anbieter eines bestimmten Dienstes sein, dessen Funktion für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist. Denkbar sind außerdem Fälle, in denen eine IT-bedingte Nichtfunktion wesentliche systemische Risiken mit grenzübergreifenden Auswirkungen zur Folge haben könnte.

Der Ernährungssektor wird im Rahmen von NIS-2 in Anhang II der Richtlinie („Sonstige kritische Sektoren“) als „Produktion, Verarbeitung und Vertrieb von Lebensmitteln“ konkretisiert. Bezeichnet sind hier Lebensmittelunternehmen im Sinne des Art. 3 Nr. 2 der Verordnung (EG) Nr. 178/2002, die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind. Demnach umfasst sind alle Lebensmittelunternehmen, gleichgültig, ob sie auf Gewinnerzielung ausgerichtet sind oder nicht oder ob sie öffentlich der privat sind, die eine mit der Produktion, der Verarbeitung und dem Vertrieb von Lebensmitteln zusammenhängende Tätigkeit ausführen.

Ein inhaltlicher Fokus dieser Studie liegt auf dem Agrarhandel und dem gewerblichen Handel mit Lebensmitteln und dessen Best Practices in der Cybersicherheit. Der Begriff des „Agrarhandels“ adressiert vor allem die Primärproduktion, so zum Beispiel die Tierhaltung oder den Gemüseanbau, aber darüber hinaus ebenso die nachgelagerten Verarbeitungsschritte der ersten Stufe wie die Zerlegung und die Veredelung, so zum Beispiel zur Herstellung von Fleischerzeugnissen oder von Brot- und Backwaren und Tiefkühlerzeugnissen in der Gemüseproduktion. Ebenso umfasst ist nach begrifflicher Definition dieser Studie der Handel mit Agrarprodukten. Dazu gehören Düngemittel und der Handel mit Futtermitteln, Weizen, Mais, Vieh, Obst und Gemüse. Unter Futtermitteln zu verstehen sind verarbeitete, teils verarbeitete oder unverarbeitete Stoffe oder Erzeugnisse zur Tierfütterung. In der Betrachtung explizit ausgeklammert wird die Stufe der Lebensmittelzubereitung wie beispielsweise in gastronomischen Betrieben, die mit Blick auf die Cybersicherheit eigenen Anforderungen und Maßstäben unterliegen, die an Größe und Betriebsstruktur anknüpfen.

In der Studie betrachtet wird ebenso der gewerbliche Handel mit Lebensmitteln, der inhaltlich vom zuvor skizzierten Agrarhandel abzugrenzen ist. Der gewerbliche Handel mit Lebensmitteln umfasst sowohl den Groß- wie auch den Einzelhandel. Zum Großhandel gehören zum Beispiel die BÄKOZENTRALE eG als genossenschaftlich organisierter Fachgroßhandel für die Bäckereien und Konditoreien, die im Food-Segment vertretenen Großhandelsmärkte der Metro AG oder die Zentralgenossenschaft des europäischen Fleischergewerbes ZENTRAG mit ihren Gilde-Shops. Der Einzelhandel mit Lebensmitteln wird unter anderem durch die Edeka-Gruppe als ebenfalls genossenschaftlich organisierter kooperativer Unternehmensverbund oder die Rewe Group als international tätiger Handelskonzern mit genossenschaftlichen Strukturen in den einzelnen Bundesländern abgebildet. In der Zusammenschau wird somit deutlich, dass im Ernährungssektor aufgrund der Vielzahl von Akteuren, deren systematisches Zusammenwirken erforderlich ist, vor allem das einwandfreie Funktionieren der Lieferkette von herausragender Bedeutung ist, um Prozesssicherheit und damit die Funktionsfähigkeit zu gewährleisten. So kann zum Beispiel ein erfolgreicher Cyberangriff auf eine Molkerei nicht nur zur Folge haben, dass der Milchviehbetrieb stillsteht, sondern die Milch kann ebenso nicht den weiteren Prozess- bzw. Veredelungsschritten zugeführt werden, sodass schließlich auch der gewerbliche Handel mit Lebensmitteln nicht mehr beliefert wird. Darüber hinaus können falsch automatisierte Dosierungen von Düngemitteln oder Pestiziden zur Folge haben, dass die Ernte mangelhaft ist und nicht weiterverarbeitet werden kann. Selbst im finalen Prozessschritt der Lebensmittelveredelung können Fehldosierungen nicht nur zur Ungenießbarkeit von Produkten führen, sondern auch Gesundheitsrisiken hervorrufen, sodass Produkte letztlich nicht mehr dem gewerblichen Handel mit Lebensmitteln zugeführt werden können. Deutlich wird damit ebenso, dass im Ernährungssektor „security“ – sprich Cybersicherheit – und „safety“, also die Produktsicherheit, untrennbar miteinander verknüpft sind.

Teil 3
Der Ernährungssektor im Fokus

Der Ernährungssektor ist Kritische Infrastruktur und mit der zusätzlichen Ausdehnung des Anwendungsbereichs der betroffenen Betriebe durch NIS-2 ist Cybersecurity Compliance weit über den KRITIS-Sektor hinaus relevant. Infolge der erheblichen sektoralen Abhängigkeit von der Lieferkette ist das Funktionieren der Nahrungsmittelversorgung überdies von einer Vielzahl kleiner und mittelständischer Betriebe abhängig, die weder Kritische Infrastruktur noch wesentliche bzw. wichtige Einrichtung im Sinne der NIS-2-Richtlinie sind. So bewirtschafteten in Deutschland im Jahr 2020 rund 262.800 landwirtschaftliche Betriebe ca. 16,6 Millionen Hektar landwirtschaftlich genutzte Fläche. Ein ganz überwiegender Anteil dieser Betriebe war ebenso im Jahr 2020 mit einer Gesamtsumme von 256.800 als natürliche Person organisiert bzw. 228.300 Betriebe als Einzelunternehmen.[4] Gerade für das Segment der durch natürliche Personen bzw. Einzelunternehmer organisierten betrieblichen Strukturen existieren in den allermeisten Fällen kaum bzw. keine Best Practices in der Cybersicherheit und IT-Notfallpläne – gleichwohl können auch solche Betriebe von Cybervorfällen betroffen und die betrieblichen sowie wirtschaftlichen Auswirkungen enorm sein (jüngst beispielsweise Neue Zürcher Zeitung: „Ein Landwirt aus Zug wird gehackt.“, 06.08.2024). Demgegenüber steht die Erkenntnis, dass 79 % der Landwirte in Deutschland mindestens eine digitale Technologie bzw. ein digitales Verfahren nutzen und damit automatisch eine Abhängigkeit vom einwandfreien Funktionieren der IT-Systeme besteht.[5]

In diesem Zusammenhang auffällig ist auch die Zahl registrierter KRITIS-Betreiber im Ernährungssektor in Deutschland. Da hierzulande im Sinne des „Anlagenbegriffs“ nicht auf die Zahl der Betreiber, sondern auf die Zahl der Kritischen Infrastrukturen abgestellt wird, kommt es durchaus häufiger vor, dass ein rechtlicher Betreiber mehrere KRITIS-Anlagen betreibt. Dennoch zeigt sich bei einem Blick in die aktuellen Statistiken zum Stichtag 30.06.2024[6], dass in Deutschland im Vergleich der kritischen Anlagen nach Sektoren nicht nur die Zahl der Anlagen mit 100 Stück im Sektor Ernährung am niedrigsten ist, sondern auch die Zahl der KRITIS-Betreiber mit 57 Stück von allen Sektoren den geringsten Wert aufweist. Gemessen an der Relevanz dieses Sektors für die ausreichende und stets gewährleistete Versorgung der Bevölkerung mit Nahrungsmitteln und seiner daraus zwangsläufig resultierenden Lebensnotwendigkeit ist dieser zahlenmäßige Wert gering – auch im Hinblick auf die zuvor skizzierten Herausforderungen und die Relevanz der Lieferkette speziell im Ernährungssektor.

Das wiederum deckt sich mit der Erkenntnis, dass jenseits von KRITIS im Ernährungssektor eine Vielzahl weiterer Unternehmen von Herausforderungen für die Cybersicherheit betroffen ist – wenn nicht als spezialgesetzliche Anforderung, dann zumindest als allgemeine unternehmerische Sorgfaltspflicht nach dem § 43 GmbHG, dem § 91 AktG oder aber speziell für den in der Praxis ganz zentralen genossenschaftlich organisierten Bereich gem. § 34 GenG, der bestimmt, dass Vorstandsmitglieder der Genossenschaften bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden haben. In § 53 GenG wird überdies festgeschrieben, dass die Ordnungsmäßigkeit der Geschäftsführung explizit Gegenstand der jährlich stattfindenden Prüfung ist.

Die nach verschiedenen rechtlichen Grundlagen zu überprüfenden und nachzuweisenden Sorgfaltspflichten der Geschäftsleitung umfassen nicht nur Pflichten zur ordnungsgemäßen Buchführung, sondern ebenso Maßnahmen zur Umsetzung adäquater Maßnahmen

4 Bundesministerium für Ernährung und Landwirtschaft, Daten und Fakten: Land-, Forst- und Ernährungswirtschaft mit Fischerei und Wein- und Gartenbau, Stand Mai 2022, https://www.bmel.de/SharedDocs/Downloads/DE/Broschueren/daten-fakten-2022.html

5 bitkom, Whitepaper „Cyberresilienz in der Landwirtschaft: Landwirtschaftliche Betriebe besser gegen Cyberattacken schützen“, 2023, https://www.bitkom.org/sites/main/files/2023-08/bitkom-whitepaper-cyberresilienz-in-der-landwirtschaft.pdf

6 BSI, KRITIS in Zahlen, https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html

zur Cybersicherheit, wenn der Betrieb von IT abhängig ist. Und dabei geht die Zahl von Genossenschaften im Ernährungssektor weit über die Zahl der in Deutschland registrierten KRITIS-Betreiber hinaus: So sind im Genossenschaftsverband Genoverband e.V. mit Stand 2023 2.583 Mitgliedsgenossenschaften registriert, von denen 501 Agrargenossenschaften und 399 landwirtschaftliche Waren- und Dienstleistungsgenossenschaften sind.[7] Deutlich wird damit, dass weder der Blickwinkel auf KRITIS noch auf NIS-2 allein ausreichend sein kann, um die Bedeutung der Cybersicherheit im ernährungs- und landwirtschaftlichen Sektor angemessen wiederzugeben.

7 GENOVERBAND, Transparenzbericht für das Geschäftsjahr 2023, Publikationsdatum 29.04.2024

Teil 4
IT-Besonderheiten in der untersuchten Branche

Obwohl die betriebliche Cybersicherheit stets einzelfallbezogen umgesetzt und bewertet werden muss, gibt es einige Grundsätze, die als Compliance Pflicht formuliert auch gesetzlich festgeschrieben sind. Diese sog. „Cyberresilienz" ist Ausgangspunkt der weiteren Betrachtung, bevor auf die Spezifika der Cybersicherheit im Ernährungssektor vertiefend eingegangen wird. Cyberresilienz kann verstanden werden als die Fähigkeit eines IT-Systems, trotz negativer Einflüsse von außen weiterhin funktionsfähig zu bleiben und sich möglichst schnell von eventuellen Schäden zu erholen. Dies umfasst sowohl die Prävention, also die Vermeidung von negativen Cybereereignissen, aber auch die richtige Reaktion auf eingetretene Cybervorfälle und die anschließende Stabilisation nicht nur im Sinne der möglichst raschen Wiederherstellung der Geschäftstätigkeit, sondern auch im Sinne der Vermeidung künftiger Cyberangriffe.[8] Damit verbunden ist folglich die Anforderung, Cybersicherheit als laufenden betrieblichen Prozess umzusetzen.

Dieses prozessuale Verständnis von Cybersicherheit ist nicht neu. Bereits das erste nationale IT-SiG enthielt die Vorgabe für die Kritischen Infrastrukturen, betriebliche Cybersicherheit nach dem „Stand der Technik" zu realisieren. Dieser sog. „unbestimmte Rechtsbegriff" ist auf eine Rechtsprechung des Bundesverfassungsgerichts aus dem Jahr 1978 zurückzuführen und gliedert sich in eine Begriffstrias zwischen den „allgemeinen und anerkannten Regeln der Technik" und dem „Stand der Wissenschaft und Forschung" ein, die jeweils unterschiedliche Technologiestände wiedergeben. Der „Stand der Technik" liegt in seinem Entwicklungsgrad zwischen beiden vorgenannten Anforderungen, wobei der Stand der Wissenschaft das höchste Anforderungsniveau beschreibt. Deutlich wird damit, dass sich eine gesetzlich geforderte Erfüllung des Stands der Technik im Mittelfeld dieser beiden Anforderungsniveaus zu bewegen hat, weshalb die Einführung eines Informationssicherheitsmanagementsystems (ISMS) und eines Business Continuity Management Systems (BCMS) auch geeignet sein kann, den Stand der Technik in der praktischen Umsetzung abzubilden. Definitorisch ist der „Stand der Technik" der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, die nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt.[9]

> **In der heutigen digitalen Welt ist ein funktionierendes ISMS inklusive BCMS als Teil davon im Ernährungssektor von entscheidender Bedeutung. Unternehmen müssen proaktiv handeln und robuste Sicherheitsstrategien entwickeln, um sich gegen potenzielle Bedrohungen zu schützen und das Vertrauen der Verbraucher zu bewahren.**
>
> CHRISTIAN DICKE

Im Speziellen bezogen auf die Cybersicherheit findet sich der Stand der Technik auch sektoren- und branchenübergreifend allgemein formuliert in der NIS-2-Richtlinie wieder. Art. 21 NIS-2 beschreibt die Risikomanagementmaßnahmen in der Cybersicherheit. So sind von den durch die Richtlinie betroffenen Einrichtungen nicht nur geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zur Cybersicherheit zu ergreifen, sondern diese Maßnahmen müssen unter Berücksichtigung ebenjenes Stands der Technik ein Sicherheitsniveau gewährleisten, das dem bestehenden Risiko angemessen ist. Damit wird deutlich, dass NIS-2 als Rechtsvorschrift selbst keinen absoluten Maßstab der Cybersicherheit enthält, sondern das jeweilige Risiko betriebs- und branchenspezifisch zu definieren ist und dabei durchaus auch Wirtschaftlichkeitsaspekte in die Betrachtung ein-

8 bitkom, Whitepaper „Cyberresilienz in der Landwirtschaft: Landwirtschaftliche Betriebe besser gegen Cyberattacken schützen", 2023

9 Kipker, Cybersecurity, Kap. 4

fließen dürfen. Deutlich wird damit aber ebenso, dass Cybersecurity Compliance zuvorderst die Vermeidung von Cybervorfällen und die technische, operative und organisatorische Reaktion darauf zum Gegenstand hat. Cyberpolicen von Versicherern allein können deshalb nicht geeignet sein, diesen gesetzlich geforderten Stand der Technik zu erfüllen.

Die zuvor skizzierten Cybersecurity-Herausforderungen für die IT-Landschaft im Ernährungssektor lassen sich aufgrund vielfach fehlender Erhebungen bei Klein- und Familienbetrieben in Deutschland bislang noch nicht vollumfänglich statistisch belastbar abbilden. Hilfreich bei der Einschätzung ist jedoch ein im Oktober 2024 veröffentlichter Bericht des Büros für Technikfolgen-Abschätzung (TAB) beim Deutschen Bundestag zur Cybersicherheit in der Nahrungsmittelversorgung. Dieser hebt nicht nur die zunehmende Digitalisierung auch in der Landwirtschaft, verteilt über alle Stufen der Ernährungsversorgung hervor, sondern skizziert auch die Diversität der dabei verwendeten technischen Infrastruktur und den zunehmenden Übergang in das Cloud Computing.

> **In unserem Mandantenkreis ist die ERP-Plattform „Gevis“ das führende System. Hier wird eine intensive Cloud-Strategie verfolgt mit dem Zweck, die Wartbarkeit und die Ressourcenbelastungen der Anwendung zu reduzieren.**
>
> SILAS KÄMPCHEN

Überdies spielen insbesondere in der industriellen Produktionsumgebung auch hier Systeme des Industrial Internet of Things (IIoT) eine gewichtige Rolle. Hinzu tritt, dass im Rahmen der für den Ernährungssektor zwingend notwendigen Logistikketten eine Vielzahl sensibler und auch personenbezogener Daten verarbeitet werden. Der TAB-Bericht gelangt in der aktuellen Einschätzung zu der Erkenntnis, dass sich insbesondere in den vergangenen Jahren auch die Cyberbedrohungslage speziell im Ernährungssektor verschärft hat. Die Gründe hierfür sind jedoch mit den Cyberangriffen auf andere Sektoren und Branchen vergleichbar, indem vor allem monetäre Werte eine Rolle spielen. Als besondere technisch-organisatorische Gefahren werden dabei zusätzlich die immer schwierigere physische Trennung von IT- und Betriebstechnologien sowie Supply-Chain-Angriffe über externe IT-Dienstleister genannt, deren Cybersicherheitsstandards sich durch die Auftraggeber, wenn überhaupt nur eingeschränkt überprüfen lassen. Abschließend enthält der Bericht Prognosen, wie sich der Ausfall von IT-Systemen letztlich auch auf die Versorgungssicherheit auswirken kann, dies im Hinblick auf die gesamte Lieferkette unter Einbeziehung von Landwirtschaft, Verarbeitung, Logistik und Handel. Die NIS-2-Richtlinie soll dabei unterstützen, diese festgestellten digitalen Vulnerabilitäten im Ernährungssektor signifikant zu reduzieren.[10]

Im europäischen Ausland ist die Cybersicherheit in der Landwirtschaft bereits Gegenstand eingehender wissenschaftlicher und behördlicher Befassung. So haben Forscher der University of Cambridge eine Publikation veröffentlicht, die sich mit der Risikoabschätzung für den Einsatz autonomer Maschinen in der Landwirtschaft befasst.[11] Die britische Cybersicherheitsbehörde hat überdies einen Leitfaden für die Cybersicherheit von Landwirten veröffentlicht, der grundlegende Hinweise zu Softwareupdates, Datenspeicherungen, Datensicherheit, Malware, Passwörtern, Authentisierungsverfahren, Spam-Mails und Phishing enthält.[12] Diese vorgenannten Maßnahmen dürften für sich genommen aber nicht ausreichend sein, um beispielsweise die gesetzlich definierten Anforderungen aus NIS-2 zu erfüllen.

10 Riousset, Cybersicherheit in der Nahrungsmittelversorgung, Endbericht zum TA-Projekt, TAB-Arbeitsbericht Nr. 213, 2024, https://www.tab-beim-bundestag.de/themenfeld-landwirtschaft-und-ernaehrung_cybersicherheit-in-der-nahrungsmittelproduktion.php

11 Tzachor et al., „Responsible artificial intelligence in agriculture requires systemic understanding of risks and externalities“, Nature Machine Intelligence 4, 104-109 (2022), https://www.nature.com/articles/s42256-022-00440-4

12 NCSC, „Cyber security for farmers: Practical tips on how to stay safe“, https://www.ncsc.gov.uk/files/NCSC_Cyber%20Security%20Guide%20for%20Farmers-%20digital.pdf

Für die Kritischen Infrastrukturen unter anderem im Ernährungssektor unterhält das BSI eine Statistik zu den Reifegraden der umgesetzten Managementsysteme.[13] Dabei werden durch die Behörde nachfolgende Reifegrade beschrieben:

- Reifegrad 1: Ein ISMS/BCMS ist zwar geplant, aber bisher nicht etabliert.
- Reifegrad 2: Ein ISMS/BCMS ist weitestgehend etabliert.
- Reifegrad 3: Ein ISMS/BCMS ist etabliert und dokumentiert.
- Reifegrad 4: Zusätzlich zum Reifegrad 3 wurde das ISMS/BCMS regelmäßig auf Effektivität überprüft.
- Reifegrad 5: Zusätzlich zum Reifegrad 4 wurde das ISMS/BCMS regelmäßig verbessert.[14]

> **Die NIS-2-Richtlinie bietet eine hervorragende Gelegenheit für Unternehmen im Ernährungssektor, ihre Cybersicherheitspraktiken und somit den Reifegrad der Cybersicherheit zu verbessern. Durch die Zusammenarbeit mit Experten und die Implementierung bewährter Verfahren können betroffene Betriebe ihre Widerstandsfähigkeit gegenüber Cyberangriffen erheblich steigern.** CHRISTIAN DICKE

Hieraus geht hervor, dass sich die Reifegrade im Sektor Ernährung für das ISMS und BCMS größtenteils im Reifegrad 3 und damit im Mittelfeld befinden. Eine vergleichbare Situation ergibt sich für die Sektoren Energie sowie Transport und Verkehr, wobei bei letzterem zusätzlich ein Schwerpunkt im Reifegrad 2 liegt. Über im Schnitt höhere Reifegrade verfügen hingegen die Sektoren Wasser, Informationstechnik- und Telekommunikation sowie Finanz- und Versicherungswesen. Im Gesundheitssektor liegt ein deutlicher Schwerpunkt im Reifegrad 2. Auffällig ist im Hinblick auf die dem BSI gemeldeten cybersicherheitsbezogenen Störungen im zweiten Quartal 2024, dass der Ernährungssektor insgesamt über die geringste Anzahl gemeldeter Störungen im sektoralen Vergleich verfügt, so wurden insgesamt nur drei Meldungen getätigt. Ein niedriges oder hohes Meldeaufkommen ist jedoch nicht zwangsläufig ein Indikator für den Stand der Informationssicherheit, zumal, wie festgestellt, die Zahl der registrierten KRITIS-Betreiber im Ernährungssektor ebenfalls den geringsten Wert aufweist und eine Vielzahl von Betrieben in diesem Sektor nicht den Schwellenwert für die Eingruppierung als Kritische Infrastruktur erreicht.

Für die Kritischen Infrastrukturen im Sektor Ernährung wurden zur Umsetzung der Cybersecurity Compliance bislang zwei sog. „Branchenspezifische Sicherheitsstandards“ (B3S) vorgelegt, so für den Lebensmittelhandel mit einer Gültigkeit bis März 2027 und für die Ernährungsindustrie mit einer Gültigkeit bis April 2025, die sich für die jeweiligen Bereiche inhaltlich mit der Einrichtung von IT-Sicherheitsprozessen und eines ISMS befassen, um eine Erbringung der kritischen Dienstleistungen sicherzustellen. Gerade im Bereich der Warenwirtschaft im Ernährungssektor besteht die Besonderheit, dass die durch die Unternehmen eingesetzten IT-Systeme eine erhebliche Heterogenität aufweisen, sodass einerseits zwar das Risiko flächendeckender Ausfälle infolge der Abhängigkeit von einem einzelnen Provider reduziert wird, andererseits aber die Herstellung eines einheitlichen IT-Sicherheitsniveaus mit größeren Schwierigkeiten verbunden ist. Beispiele für relevante Komponenten sind hier Bezahlsysteme, Kühlanlagen, Logistikkomponenten, Überwachungssysteme, Automatisierungsvorrichtungen und die Sensorik sowie deren Programmierung und Parametrierung. Dies legt auch nahe, weshalb in der Abgrenzung zwischen der Informationstechnologie (IT) und der Betriebstechnologie (OT) unterschieden werden muss.

In der Wertschöpfungskette im Ernährungssektor zur Versorgung mit Lebensmitteln stellt der Lebensmittelhandel den letzten Schritt dar. Die Prozesse im Lebensmittelhandel untergliedern sich in die Beschaffung, Lagerung, Kommissionierung, den Versand, Vertrieb und die Entsorgung.[15] Aufgrund der Verderblichkeit von Waren ist hier ein schnelles Prozessmanagement notwendig. Deshalb spielen sog. „Enterprise-Resource-

13 BSI, KRITIS in Zahlen, https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html

14 Bundesamt für Sicherheit in der Informationstechnik, Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG, 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-nachweise.pdf

15 Rothländer, „Logistik im Lebensmittelhandel: Prozesse, Strukturen und Informationssysteme“, 2023

Planning“ (ERP)-Systeme in diesem Bereich eine herausgehobene Rolle.

> **Ein ERP-Softwaresystem besteht aus integrierten Anwendungen oder Modulen zur Verwaltung der wichtigsten Geschäftsprozesse eines Unternehmens. Das System kann z.B. die Finanzbuchhaltung, die Materialwirtschaft, das Controlling oder die Personalwirtschaft abdecken.**
> HARRY KLEINGARN

Hinzu tritt die Herausforderung, dass außerhalb der Kernprozesse des Lebensmittelhandels für die Herstellung der Versorgungssicherheit häufig Drittunternehmen und externe (IT)-Dienstleistungen einbezogen sind, was z.B. in der Zahlungsabwicklung, im E-Commerce und genossenschaftlichen Bereich der Fall ist, soweit Einzelunternehmen selbstständig Handel betreiben. Diese Verantwortungsverteilung darf im Ergebnis keine Verantwortungsdiffusion in der Cybersicherheit zur Folge haben.

Unternehmungen im Ernährungssektor sind überdies höchst divers in ihrer IT-Infrastruktur aufgestellt, was unterschiedliche Komplexitätsgrade zur Folge hat. So arbeiten größere Unternehmen bereits deutlich digitalisierter, um den Marktanforderungen gerecht werden zu können. Hierzu gehört auch ein unternehmensübergreifender elektronischer Austausch standardisierter Geschäftsdaten (Electronic Data Interchange, EDI) mit Partnerunternehmen oder Kunden und Lieferanten.

SILAS KÄMPCHEN:
Leiter IT-Spezialisten, AWADO

EDI steht für „Electronic Data Interchange“, dabei geht es um den automatisierten Austausch strukturierter Daten. Die wesentlichen Risiken liegen dabei einerseits in der Öffnung des eigenen Systems zur Anbindung außenstehender IT-Systeme für den Datenaustausch und andererseits in einer hochautomatisierten Verarbeitung der Daten. Grundvoraussetzung dafür ist daher eine belastbare Integrität der Daten.

Insbesondere bei diesen Unternehmen ist infolge der erhöhten Komplexität der IT-Infrastruktur auch von größeren Risiken in der Cybersicherheit im Hinblick auf die Geschäftsprozesse auszugehen. Überdies betreiben größere Unternehmen im Ernährungssektor regelmäßig Extranet-Auftritte, um Vertrags- und Geschäftspartnern Informationen bereitzustellen oder Bestellungen digital abzuwickeln. Derlei Systeme sind naturgemäß exponierter und stellen daher ein größeres Cybersicherheitsrisiko dar. Die IT-Komplexität von größeren Unternehmen im Ernährungssektor beschränkt sich darauf jedoch nicht, so wird ebenso eine größere Anwendungslandschaft mit einem höheren Spezialisierungsgrad vorgehalten. Dies führt unter anderem zu Eigenentwicklungen, die das Erfordernis besonderer IT-Schutzmaßnahmen nach sich ziehen.

In einer Gesamtbetrachtung ebenfalls nicht unberücksichtigt bleiben darf die physische Sicherheit der informationstechnischen Infrastruktur. Diese betrifft die Stromversorgung, die Absicherung von Telefon- und Datenleitungen, Verkabelungen, Informations- und Kommunikationstechnik und den physischen Schutz von Serverräumen und informationsverarbeitenden Anlagen vor unberechtigtem Zugang und Zugriff. Hier kommt es in der Umsetzung beispielsweise auf geeignete Zutrittsschutzsysteme, eine sinnvolle IT-Raumplanung sowie entsprechende Überwachungssysteme an.

Teil 5
Cybersecurity-Anforderungen, Maßnahmen, Dokumentations- und Meldepflichten in der untersuchten Branche

Die branchenspezifischen Anforderungen an die Cybersicherheit im Ernährungssektor sind wie gezeigt wurde weit gefasst und höchst divers, indem sie an die individuellen betrieblichen Strukturen, deren Leistungsfähigkeit, Risikoexposition und Unternehmensgröße anknüpfen. Die NIS-2-Richtlinie steckt mit ihrem Maßnahmen-Anforderungskatalog zum Cybersecurity-Risikomanagement zwar einen allgemeinen Rahmen fest, der aber unter den Gesichtspunkten von Angemessenheit und Verhältnismäßigkeit individuell zu bewerten ist. Dabei einzubeziehen sind auch die Schwere von Sicherheitsvorfällen einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen. Der unternehmerische Handlungsrahmen sollte deshalb darauf abzielen, nicht nur die IT-Systeme selbst, sondern auch ihre physische Umwelt vor Sicherheitsvorfällen zu schützen, indem ein Mindestkatalog an Sicherheitsmaßnahmen vorgeschlagen wird, der nachfolgende Punkte adressiert:

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
- Bewältigung von Sicherheitsvorfällen;
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Laut NIS-2 können diese allgemein gehaltenen Anforderungen durch Durchführungsrechtsakte weiter konkretisiert werden, wobei eine Orientierung an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen der jeweiligen Branche weitestgehend möglich erfolgt. Eine ganz zentrale Erkenntnis auch bei jeder individuellen betrieblichen Umsetzung von NIS-2 ist jedoch: Ausschließlich durch den Bezug einzelner Produkte und Dienste zur Cybersicherheit ist es nicht möglich, ein nachhaltiges und gleichbleibend hohes Resilienzniveau zu gewährleisten, denn die Produkte und Dienste müssen letztlich dazu verwendet werden, um ein Managementsystem zur Informationssicherheit zu errichten. Insoweit kann der in der NIS-2-Richtlinie bezeichnete Katalog bei einer abstrakten Betrachtung zunächst auch irreführend sein, suggeriert er doch, lediglich durch bestimmte Einzelmaßnahmen

ein angemessenes Niveau nachhaltiger betrieblicher Cybersicherheit realisieren zu können.

Insbesondere für den Agrarhandel und den gewerblichen Handel mit Lebensmitteln sind bereits seit mehreren Jahren technische Spezifikationen vorhanden, die die IT-Infrastruktur im Bereich der Warenwirtschaft zum Gegenstand haben und nicht nur für Kritische Infrastrukturen oder durch NIS-2 betroffene Unternehmen, sondern auch außerhalb dieses Adressatenkreises Verwendung finden können, indem sie die Wirtschaftlichkeit und Verhältnismäßigkeit zu treffender Maßnahmen aktiv berücksichtigen. Die Anforderungen orientieren sich dabei an den nachfolgenden Maßgaben zur IT-Basissicherheit unter Einbeziehung auch der Sicherheit von personenbezogenen Daten:

- Gesetze, Wirtschaftsprüfer (ISA DE 315), Versicherungen/Banken, BSI-Grundschutz
- IDW PH 9.860.4 (9/2024) zur Prüfung der Einhaltung der Grundsätze der ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD-Compliance)
- Räumlichkeiten und Hardware-Redundanz, Verfügbarkeit, Wartung
- Datenschutzbeauftragter
- IT-Sicherheitscheck
- Datensicherung, Bandüberprüfungen
- Zertifizierung zum Systemkoordinator
- Virenschutz, Firewall, Sicherheitsupdates
- Software-Lizenzierung
- Monitoring
- Risiko-Analyse und Notfallplan

Der jeweilige Prüfmaßstab variiert in der Praxis aber deutlich und ist in erster Linie von der Komplexität des IT-Systems und der Unternehmensgröße abhängig. Wie bereits dargelegt wurde, ist jedoch stets die Verschränkung von Compliance, Risikomanagementsystemen und den technischorganisatorischen Maßnahmen zur Cybersicherheit der Ausgangspunkt der Betrachtungen und hierbei zeigt sich auch im genossenschaftlichen Bereich die besondere Herausforderung von Cybersicherheit als interdisziplinärer Aufgabe zwischen Recht, Normen und Standards, Technik sowie betriebswirtschaftlichen Erwägungen. Im genossenschaftlichen Bereich gilt hierbei die Besonderheit, dass der BSI-Grundschutz bei in etwa 80 % der Genossenschaften nur eine geringe Relevanz besitzt, was vor allem auf eine technisch einfach strukturierte Finanzbuchhaltung auf der Basis von DATEV-Diensten oder Haufe-Buchhaltungssystemen zurückzuführen ist. Zusätzlich wird häufig auf regionale IT-Dienstleister zurückgegriffen. Nur wenige Genossenschaften verfügen über eine komplexe IT-Infrastruktur mit eigenen personellen Ressourcen, in denen individuell skalierte Maßnahmen aus dem BSI-Grundschutz realisiert werden. Ebenso zeigt sich diese branchenspezifische Besonderheit im Großhandel: Hier werden aufgrund des Streckengeschäfts einerseits zwar regelmäßig hohe Umsatzerlöse generiert und damit die quantitativen Anforderungen an eine NIS-2-Betroffenheit erfüllt, andererseits jedoch wird ein nach wie vor einfaches IT-System vorgehalten und damit die Relevanz von betrieblicher Cybersicherheit noch nicht erkannt.

Gemessen am individuellen betrieblichen Risiko wird eine regelmäßige Gap-Analyse durchgeführt, bei der es als betriebswirtschaftliches Planungs- und Kontrollinstrument darum geht, die Abweichung zwischen dem vorhandenen Istwert und dem angestrebten Sollwert in der Cybersicherheit zu ermitteln.

CHRISTIAN DICKE:
Direktor IT-Prüfung und Beratung, AWADO

Eine Gap-Analyse ist ein Soll-Ist-Abgleich hinsichtlich der zu erfüllenden Anforderungen und soll potenziellen Handlungsbedarf bei der Etablierung eines effektiven ISMS aufzeigen. Voraussetzung für eine effiziente Gap-Analyse ist eine angemessene Dokumentation des Ist-Zustands. Empfehlenswert ist deshalb der Einsatz eines externen Beraters, der branchentypische Best Practices kennt und einbringen kann.

Bei dieser Gap-Analyse können bestimmte Fragen relevant sein, wie zum Beispiel:

- Sind Richtlinien und Anweisungen zur Erkennung, Analyse, Bewertung und Behandlung von betrieblichen IT-Risiken vorhanden?
- Werden die Verfahren zur Erkennung, Analyse, Bewertung und Behandlung von IT-Risiken regelmäßig durchgeführt, um interne und externe Veränderungen zu berücksichtigen?
- Werden erkannte Risiken dokumentiert, bewertet und mit Maßnahmen zur Risikominderung versehen?
- Wird die Unternehmensleitung regelmäßig über den Status der erkannten Risiken und die Maßnahmen zu deren Minderung informiert?

Basierend auf den ermittelten Anforderungen werden konkrete Maßgaben und Vorschläge für den Aufbau eines Risikomanagementsystems skalierbar nach der Größe des Unternehmens bestimmt, Vorgaben zum Umgang mit Sicherheitsvorfällen definiert und auch Regelungen zur Einhaltung von Meldepflichten festgelegt, um ein BCM in der Cybersicherheit aufzubauen.

Für den in dieser Studie untersuchten genossenschaftlichen Bereich stellt sich nach Abschluss der Gap-Analyse regelmäßig heraus, dass nur in seltenen Fällen ein angemessen ausgestaltetes Risikomanagement zur Cybersicherheit vorhanden ist. Das bedeutet, dass IT-Risiken – wenn überhaupt – nur rudimentär und nicht im Detail erfasst wurden. Entsprechend lässt sich die Geeignetheit und Angemessenheit der Maßnahmen im Kontext nicht beurteilen. Problematisch ist zudem, dass in den allermeisten Fällen keine angemessene Protokollierungsinfrastruktur zur Cybersicherheit abgebildet ist. Ebenso wenig wird ein Penetration Testing oder ein Schwachstellenmanagement durchgeführt.

> **Ein Penetration Test zeigt auf, ob die getroffenen Maßnahmen im Rahmen einer ISMS-Etablierung effektiv implementiert sind und weist auf etwaige Schwachstellen und Sicherheitslücken hin, aus denen sich weitere Maßnahmen zur kontinuierlichen Verbesserung der IT-Sicherheit ableiten lassen.** CHRISTIAN DICKE

Da viele Betriebe mittlerweile von der digitalen Lieferkette abhängig sind, ergeben sich auch an dieser Stelle neue Herausforderungen für die Cybersicherheit. So hosten immer weniger Betriebe ihre IT-Dienste „on premise“, sondern lagern diese deutlich zunehmend in Cloud-Lösungen aus. Wo im Jahr 2020/2021 aus der Beratungserfahrung heraus der Anteil an selbst gehosteten IT-Diensten noch bei ca. 80 % lag, liegt er mittlerweile bei 50 % oder weniger mit weiterhin fallender Tendenz. Das führt dazu, dass auch im genossenschaftlichen Bereich von Raiffeisen, Agrar und Lebensmitteln die digitale Lieferkette perspektivisch eine immer höhere Relevanz hat. Ein Auslagerungsmanagement zur Überwachung der Sicherheit und Vertraulichkeit in der Lieferkette wird hingegen nicht etabliert. Hinzu tritt, dass regelmäßig erhebliche Probleme im Hinblick auf die Nachweisbarkeit getroffener Cybersicherheitsmaßnahmen bestehen und kaum Maßnahmen zur Dokumentation betrieben werden. Ebenso wenig finden sich ausgereifte Prozesse zum Vorfalls-, Notfall- und Krisenmanagement.

SILAS KÄMPCHEN:
Leiter IT-Spezialisten, AWADO

Erster Fokus bei der Bewältigung eines IT-Notfalls sollte es sein, die Auswirkungen einzugrenzen und die Betriebsfähigkeit der Systeme zumindest im Notfallbetrieb wiederherzustellen. Grundvoraussetzung dafür ist ein konzeptionell detailliert geplantes und vor allem erprobtes Vorgehen. Das Notfallhandbuch dient dabei als Leitrahmen, um ein strukturiertes Vorgehen zu gewährleisten und somit Zeitverluste zu reduzieren.

Insbesondere die beiden letztgenannten Punkte sind nicht auf die Erfordernisse aus einer individuellen Risikoanalyse ausgerichtet, da eine solche regelmäßig nicht vorhanden ist. Weitere Umsetzungsschwierigkeiten ergeben sich bei einer Betrachtung der betriebsinternen Kommunikation zur Cybersicherheit bei Genossenschaften und gewerblichen Handels- und Dienstleistungsgesellschaften. Grundsätzlich gilt aus der Perspektive der betrieblichen Compliance, dass bei Vorhandensein eines Aufsichtsrats dieser turnusgemäß

über alle relevanten Risiken und damit auch die IT-Risiken aktiv zu informieren ist, um die Ordnungsmäßigkeit der Geschäftsführung des Unternehmens zu überwachen. In der Praxis wird dies nur in etwa der Hälfte der Fälle realisiert – primär abhängig von der Größenordnung des Unternehmens. Das hat zur Folge, dass nicht nur etablierte innerbetriebliche Kommunikationsprozesse zur Cybersicherheit fehlen, sondern stärker Ad hoc kommuniziert wird. Damit ist auch eine Stabsstelle zur Überwachung der Cybersicherheit wie beispielsweise ein Informationssicherheitsbeauftragter eher selten vorzufinden und vor allem Gegenstand des Cybersicherheitsmanagements nur von größeren Unternehmungen.

Dieses Ergebnis einer Gap-Analyse im genossenschaftlichen Sektor führt zu verschiedenen Schlussfolgerungen: Die Sensibilität für Cybersicherheit als Erfordernis zwingender betrieblicher Notwendigkeit ist nach wie vor noch sehr unterschiedlich ausgeprägt und von der Größe des Unternehmens und der Sensibilität der Geschäftsleitung und/oder des Aufsichtsrates abhängig. Teilweise fehlt nach wie vor das tiefergehende Bewusstsein der Geschäftsführung, den Einsatz von betrieblicher IT-Infrastruktur nicht ausschließlich als gewinnbringende Maßnahme, sondern auch als Geschäftsrisiko zu betrachten. Hiermit einhergehend sind auch bestehende budgetäre Defizite für IT-Investitionen und personelle Ressourcen. Damit verbundene typische Probleme in der genossenschaftlichen IT sind eine zu geringe Personaldecke mit nur ein bis zwei zuständigen Mitarbeitern, einer zu starken Skalierung von Maßnahmen und einem regelmäßigen akuten Personal- und Zeitmangel. Im Hinblick auf die Umsetzung von NIS-2 folgt daraus, dass wenn von Unternehmen die betriebliche Relevanz der Richtlinie erkannt wurde, man zumeist noch im Stadium der Gap-Analyse befindlich ist und daraus resultierend der Reifegrad der Cybersicherheit besonders hinsichtlich der Dokumentation und der Risikomanagementmaßnahmen eher gering einzustufen ist. Dies führt insgesamt zu der Erkenntnis, dass die individuelle Wahrnehmung der Cybersicherheit im Ernährungssektor – wie in zahllosen weiteren Sektoren und Branchen auch – regelmäßig nicht mit der objektiven Gefährdungslage einhergeht. So ist die IT-Abhängigkeit von Geschäftsprozessen in den letzten Jahren gestiegen. Regelmäßig wird jedoch nach wie vor argumentiert, dass das Kerngeschäft lediglich die Bewegung physischer Waren ist. Dass aber diese Bewegung physischer Güter durch die Digitalisierung der mit ihr verbundenen Infrastruktur z.B. durch digitale Bestellungen, Lieferscheine, Waagen etc. mittlerweile in ganz erheblicher Weise von IT abhängig ist, ist regelmäßig noch nicht in der betrieblichen Wahrnehmung angelangt.

Soweit folglich betriebliche Cybersicherheit nach NIS-2 in den skizzierten Betriebsformen realisiert werden soll, sind hiermit nicht selten erhebliche strukturelle, personelle und wirtschaftliche Herausforderungen verbunden. Zuvorderst kommt es hierbei auf das Verständnis der Geschäftsleitung an, Cybersicherheit als betrieblich notwendige Risikoinvestition zu betrachten, denn Compliance, Sorgfaltspflichten und Haftungsfragen sind in erster Linie Anforderungen, die durch das Management zu adressieren sind. Speziell für den landwirtschaftlichen Handel stellt sich ein weiteres Problem in der Umsetzung von Cybersicherheit: Zwar sind die Umsatzgrößen hoch, die Margen regelmäßig aber nur recht gering. Dementsprechend sind die personellen Ressourcen oftmals nicht ausreichend, um aus eigener Kraft und Know-how ein angemessenes und umfangreiches Managementsystem nach NIS-2 abzubilden, da die Organisationsgrößen regelmäßig auch keine weiteren Stellen begründen und finanzieren. Hier bieten sich jedoch zumindest teilweise optional ausgelagerte IT-Services wie externe Informationssicherheitsbeauftragte (ISB), Risikomanager oder Sicherheitsdienstleister an, um die wirtschaftlichen Realisierungsaufwände für eine betroffene Gesellschaft im leistbaren Rahmen zu halten. Gleichwohl ist anzumerken, dass durch eine vollständige Auslagerung von IT-Kapazitäten der Aufbau eines fortlaufenden Managements zur Cybersicherheit auch deutlich erschwert werden kann.

HARRY KLEINGARN:
IT-Spezialist Prüfung und Beratung, Genoverband e.V.

Der Informationssicherheitsbeauftragte (ISB) wirkt darauf hin, dass das gewünschte IT-Sicherheitsniveau eines Unternehmens erreicht werden kann und greift bei Abweichungen ein. Er sollte idealerweise in diesem Bereich einschlägige Berufserfahrungen vorweisen und auch Praxiserfahrungen im Aufbau und der Steuerung von IT-Sicherheitsprozessen haben.

Damit ein betriebliches Risikomanagement zur Cybersicherheit aufgebaut werden kann, muss in einem ersten Ansatz eine Risikoinventur unter Berücksichtigung der G0-Gefährdungen vorgenommen werden, um einen Überblick über bestehende IT-Risiken im Geschäftsmodell zu erhalten. Bei den G0-Gefährdungen handelt es sich um „elementare Gefährdungen", die das BSI im IT-Grundschutz-Kompendium in einer Liste mit insgesamt 47 solcher Gefährdungen zusammengetragen hat.[16] Hierzu gehören nicht nur Katastrophenereignisse, sondern ebenso mutwillige Beeinträchtigungen der Cybersicherheit durch unbefugte und/oder kriminell agierende Akteure. Diese Risikoinventur verfolgt das Ziel, einen Überblick über bestehende IT-Risiken im konkreten Geschäftsmodell zu erhalten. Nach der vollständigen Erfassung der Risiken sollten diese entsprechend der jeweiligen Schutzziele des Unternehmens bewertet werden. Aus den bewerteten Risiken werden sodann die notwendigen Maßnahmen abgeleitet. Im unternehmerischen Kontext stellt das IT-Risikomanagement in aller Regel nur einen zu beschreibenden Abschnitt im Risikomanagementhandbuch dar – aber das bedeutet auch, dass eine solche Risikoinventur nicht nur einmalig durch einen IT-Sicherheitsverantwortlichen zu erstellen ist, sondern regelmäßig durchgeführt und damit „gelebt" werden muss. Das hat den Grund, dass sich betriebliche und personelle Strukturen im Zeitverlauf verändern, neue Produkte und Dienstleistungen in das Portfolio aufgenommen werden können und sich hierdurch auch die individuelle betriebliche Risikoprävalenz durchaus verändern kann. Doch für ein erfolgreiches unternehmerisches Risikomanagement in der Cybersicherheit ist es auch erforderlich, Risiken nicht nur zu identifizieren, sondern darauf basierend auch mitigierende Maßnahmen abzuleiten – und genau dieser Aspekt der realen Umsetzung ist tatsächlich nur selten bis gar nicht vorzufinden. Die größte Herausforderung wird deshalb mit Sicherheit die Implementierung eines solchen unternehmensweiten Risikomanagements sein, das ebenso ein Risikomanagement zur Cybersicherheit beinhaltet. Die Umsetzung der technisch-organisatorischen Maßnahmen, die sich daraus ableiten, dürfte zwar teilweise arbeitsintensiv sein und einen zusätzlichen Kostenfaktor in der betrieblichen IT zur Folge haben, jedoch ist der größere Aufwand zur Ausarbeitung der Konzepte, Prozess- und Kontrolldokumentationen sowie der Etablierung eines Gesamtverständnisses für die Notwendigkeit von Cyberhygiene und IT-Sicherheitsmaßnahmen essenziell.

Risikomanagement in der Cybersicherheit bedeutet jedoch nicht nur die Gewährleistung digitaler Sicherheit, sondern ebenso den Schutz der physischen (IT-) Infrastruktur. Um beispielsweise das Inventar, Außenstellen, Lager oder Produktionsstätten zu schützen, ist der erste Schritt die Einführung eines Asset-Managements. Im Rahmen einer Strukturanalyse werden hierbei die notwendigen Assets und deren Schutzbedarf in den Kontext der Geschäftsprozesse gesetzt. Abhängig von der jeweiligen Risikosituation sind entsprechende Maßnahmen zum Schutz der physischen Infrastruktur zu treffen. Beispielsweise ist ein Zutrittsschutzkonzept mit definierten Sicherheitsbereichen und fortdauernden Kontrollen zur Einhaltung der definierten Zutrittsberechtigungen regelmäßig eine der ersten Maßnahmen. Darüber hinaus sind auch physische Sicherungsmaßnahmen wie Brandschutz, Wasserschutz oder Schutz vor Manipulation umzusetzen. Diese sind ebenfalls in Abhängigkeit der ermittelten Risiken zu realisieren. Die Erfahrungen im landwirtschaftlichen und genossenschaftlichen Sektor sind hier durchaus divers, so ist von professionell betriebenen Rechenzentren bis hin zu Servern auf weitestgehend ungesicherten Büroflächen nahezu alles vertreten. Nicht selten zeigt sich hierbei auch eine gewisse Kohärenz in Eigenschaften und Anforderungen, indem das Maß der physischen Absicherung dem Grad der Digitalisierung des Unternehmens entspricht. Der Bedarf nach physischer Absicherung unternehmenseigener IT-Infrastruktur wird sich in den kommenden Jahren perspektivisch noch weiter verändern, indem durch die Cloudifizierung die Relevanz der IT-Infrastruktur vor Ort weiter reduziert wird.

Um das Management zur Cybersicherheit nach NIS-2 und auch darüber hinaus erfolgreich umzusetzen, kommt es nicht nur auf die Entwicklung und Umsetzung von Konzepten und Prozessen, sondern auch auf deren Dokumentation und damit Nachweisbarkeit an. Gerade den beiden letztgenannten Punkten wurde in der Vergangenheit immer wieder zu wenig Aufmerksamkeit geschenkt.

16 Bundesamt für Sicherheit in der Informationstechnik, Elementare Gefährdungen, 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/Elementare_Gefaehrdungen.pdf

HARRY KLEINGARN:
IT-Spezialist Prüfung und Beratung, Genoverband e.V

Was leider oft vergessen wird: Ohne eine Dokumentation und entsprechende Nachweise kann das Management die an die Mitarbeiterinnen und Mitarbeiter übertragenen Aufgaben nicht effektiv überprüfen. Hier können deshalb schnell Fälle des Organisationsverschuldens der Geschäftsleitung relevant werden. Ebenso ist es ohne eine ordnungsgemäße Dokumentation nicht möglich, die Betrachtung der IT-Risiken mit Bezug auf die eingeleiteten Maßnahmen (Brutto-/Netto-Betrachtung) durchzuführen.

Da die IT vielfach nach dem Prinzip des „Daily Business“ betrieben wird, fehlt ein strategischer und damit auch für Dritte und Außenstehende nachvollziehbarer Ansatz. Einerseits ist dieser Missstand dadurch begründet, dass die Aufmerksamkeit der Geschäftsleitung zumeist auf andere betriebliche Prozesse gerichtet ist, andererseits muss IT zumeist nur nach den Betriebsanforderungen funktionieren – weitere eigentlich relevante Umstände werden damit bewusst oder unbewusst ausgeklammert. Die Relevanz dieser Problematik geht inhaltlich weit über die Cybersicherheit hinaus und kann neben Fragen der IT-Kompatibilität auch wirtschaftliche Fragen zukunftsgerichteter und nachhaltiger IT-Anschaffung betreffen.

Die Nachweisbarkeit eines betrieblichen Managements zur Cybersicherheit kann auf verschiedenen Wegen erfolgen. Von ausschließlich tabellenbasierten Auswertungen und Analysen ist jedoch abzuraten – das nicht nur wegen der Fehleranfälligkeit und schlechteren Nachvollziehbarkeit, sondern auch weil in den meisten Fällen kein Versionsmanagement vorhanden ist. Überdies stellen sich Fragen der Betriebskontinuität, falls beispielsweise der zuständige Mitarbeiter das Unternehmen verlässt. Nicht zuletzt fehlen Möglichkeiten zur Selbstbewertung für die zuständigen Mitarbeiter. Zur Unterstützung eines vollumfänglichen Risikomanagements auch in der Cybersicherheit kann beispielsweise die GRC-Anwendung „CRISAM“ zum Einsatz kommen, in deren Anwendungskontext vordefinierte Strukturen und Musterrisiken zur Verfügung gestellt werden können. Die Risikoanalyse für IT-Assets bemisst sich dabei anhand des auch von NIS-2 vorausgesetzten und in dieser Studie bereits beschriebenen Stands der Technik. Die in der Software enthaltene Logik erleichtert es Unternehmen, eine Risikobewertung anhand gängiger Standards durchzuführen und den Stand der Technik festzustellen. Der in der Anwendung enthaltene Self Assessment-Ansatz zur Risikobewertung bietet überdies die Möglichkeit, den Aufwand für die Risikobewertung auf mehrere Zuständigkeiten zu verteilen. Auf diese Weise können besonders die einzelnen Fachbereiche eines Unternehmens in die Risikobewertung zur betrieblichen Cybersicherheit einbezogen werden.

Die AWADO bedient sich der Anwendung „CRISAM“, um den skizzierten Risikomanagementprozess zur Cybersicherheit bestmöglich zu unterstützen. Auch bietet die AWADO ein Dienstleistungsmodell an, um vor allem kleineren Unternehmen mit nur begrenzten wirtschaftlichen Ressourcen das Risikomanagement als Servicedienstleistung zu ermöglichen. Neben der allgemeinen IT-Risikoanalyse werden auch korrespondierende Konzepte und Leitlinien erstellt, die für die Bewertung der Risiken wesentlich sind. Hier sind vor allem die Definition der Schutzziele in der IT-Sicherheitsleitlinie sowie die Definition von tolerierbaren Ausfallzeiten und Datenverlusten zu nennen. Die Ergebnisse einer Bewertung der laufenden IT-Risikoanalyse und der aktuellen Sicherheitslage werden über ein entsprechendes Berichtswesen mit den relevanten Stellen im Unternehmen wie beispielsweise der Geschäftsführung und dem Aufsichtsrat geteilt. Hierfür ist ein entsprechender Prozess zum Berichtswesen aufzubauen. Dabei liegt der Fokus auf der realen Abbildung tatsächlicher Risikosituationen und der gemeinsamen Entwicklung pragmatischer Maßnahmen zur IT-Risikomitigation.

Fallbeispiel

NIS-2-Umsetzung und ISMS-Aufbau mit CRISAM am Beispiel der Uelzena

© Uelzena eG, Uelzen

Die Uelzena eG, ein mittelgroßes genossenschaftliches Unternehmen mit 845 Mitarbeitenden, verarbeitete im Jahr 2023 knapp 860 Millionen Kilogramm flüssige Milchrohstoffe und erzielte einen Umsatz von 929 Millionen Euro, sodass eine NIS-2-Betroffenheit naheliegt.

In Vorbereitung auf die Umsetzung der korrespondierenden gesetzlichen Anforderungen und zur Stärkung der Resilienz wurde zusammen mit der Uelzena eG ein Projekt zur Etablierung eines Informationssicherheitsmanagementsystem (ISMS) aufgesetzt. Die gemeinsame Aufgabe lag dabei nicht nur in der technischen Erfassung der Unternehmensstruktur, sondern vor allem in der Verbesserung und Dokumentation von Prozessen, Verantwortlichkeiten und Strukturen – sowohl in der Muttergesellschaft als auch in den Tochtergesellschaften.

Bei der Implementierung des ISMS wurden gezielte Interviews mit Stakeholdern, zur Risikoanalyse, zum Maßnahmen-Management und zur Richtlinienverwaltung durchgeführt, um Anforderungen und Risiken umfassend festzustellen und in CRISAM zu dokumentieren. Die Bewertung der Risikoobjekte erfolgt anwendungsgestützt anhand von Kontrollzielfragen, die über Workflows direkt von den Verantwortlichen in den Fachbereichen beantwortet werden konnten.

Ein entscheidender Erfolgsfaktor des Projekts war der Einsatz des GRC-Tools CRISAM. Die Plattform verfügt über die Fähigkeit, komplexe Unternehmensstrukturen transparent und normenkonform gemäß ISO/IEC 27001 abzubilden. Die modulare Struktur und die integrierten Content-Bibliotheken ermöglichten eine zielgerichtete Berücksichtigung der spezifischen Anforderungen aus der NIS-2-Richtlinie sowie des branchenspezifischen Kontextes der Uelzena-Gruppe.

CRISAM ermöglichte es, die heterogene Struktur präzise zu modellieren und die jeweiligen Risiken pro Gesellschaft differenziert und effizient zu bewerten. Die Risikoobjekte konnten dynamisch nach ihren Abhängigkeiten verknüpft werden, was ein aktives Informationsrisikomanagement erlaubt, das die Angemessenheit der ergriffenen technischen und organisatorischen Maßnahmen gemäß dem Stand der Technik belegen kann.

Über das CII

Neue Zeiten brauchen eine neue Form der Forschung: das cyberintelligence.institute (CII) – ein Ort, an dem sich Innovation, Technologie, Strategie und Resilienz treffen. An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Start-up entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Kerngedanken sind die Kooperation, der Dialog und der interdisziplinäre und globale Informations- und Wissensaustausch, um Staat, Wirtschaft und Gesellschaft resilienter zu machen. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein.

Weitere Informationen gibt es auf der Website des CII unter www.cyberintelligence.institute.

CYBERINTELLIGENCE
.Institute

cyberintelligence.institute
MesseTurm
Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

www.cyberintelligence.institute
info@cyberintelligence.institute

+49 69 505034602

Diese Studie wurde erstellt mit Unterstützung des CII-Fördermitglieds: AWADO

Date of Publication: 09/2025