Schutz vor Angriffen aus dem Netz

Die Zahl der Cyberangriffe wächst. Ausfälle gefährden Lieferketten und die öffentliche Versorgung. Daher hat die EU mit NIS-2 ein Regelwerk geschaffen, das auch Fleischereibetriebe bald zu Maßnahmen verpflichtet. Die Vorgaben betreffen Unternehmen sogenannter wesentlicher und wichtiger Branchen.

Die NIS-2-Richtlinie der EU, die im Oktober 2024 in Kraft treten wird, verpflichtet auch zahlreiche Betriebe der Fleischbranche, Maßnahmen gegen Cyberattacken und zum Schutz sensibler Daten zu ergreifen. Thapana_Studio – stock.adobe.com

Eine Ransomware kann ganze Betriebe als Geisel nehmen. Das tückische Schadprogramm sperrt den Computer und verschlüsselt Daten. Von den Festplatten sind dann meist schon Kopien zu den Tätern übertragen worden. Diese fordern für die Wiederherstellung ein Lösegeld und drohen mit Veröffentlichung der oft sensiblen Informationen. Nicht nur Datenabfluss ist ein Problem bei einem Cyberangriff. Schlecht ist auch, wenn Kriminelle auf Geräte zugreifen, von denen beispielsweise die Kühlkette abhängt oder über die Maschinen ferngewartet werden.

Für 2022 verzeichnet das Bundeskriminalamt (BKA) 136.865 Cyberangriffe – zwar 6,5 Prozent weniger als im Vorjahr, dafür liegen die Schäden mit 203 Milliarden Euro rund doppelt so hoch wie 2019. Die Gefahr bleibt hoch und die Dunkelziffer nach BKA-Schätzung mit 90 Prozent riesig. Oft kommt der Angriff per Mail. 66 Prozent aller Spam-Mails sind Betrugs- oder Erpressungsversuche, berichtet das Bundesamt für die Sicherheit (BSI) in der Informationstechnik. Dessen Spezialisten finden täglich eine Viertelmillion Schadprogramme auf Datenträgern. Über die Hälfte aller Unternehmen (52 %) wurde nach Angaben des Digitalverbands Bitkom 2022 mit Ransomware angegriffen – 23 Prozent mit Schaden, 29 Prozent ohne. Und europaweit ist das kaum anders.

EU-Richtlinie beachten

Um das Risiko zu senken, verpflichtet die EU-Kommission zahlreiche Unternehmen, die Network-and-Information-Security-Richtlinie 2.0 (NIS2) umzusetzen. Die NIS-2-Richtlinie macht Unternehmen wesentlicher sowie wichtiger Branchen umfangreiche Vorgaben. Die Vorgaben werden auch zahlreiche Fleischereiunternehmen betreffen – die sollten sich zügig kümmern. Ob sie betroffen sind, müssen sie selbst herausfinden.

Bis Oktober 2024 soll NIS-2 in nationales Recht umgesetzt sein. Eine Übergangs- oder Schonfrist gibt es nicht. Die Bundesregierung befasst sich derzeit noch mit dem NIS-2-Umsetzungsgesetz. Loslegen sollten Unternehmen trotzdem schon jetzt, rät Benjamin Richter, geschäftsführender Gesellschafter der Cyber Complete GmbH im nordrhein-westfälischen Schmallenberg. „Solange sie sich an der EU-Richtlinie orientieren, werden sie keine größeren Fehler machen." Und der Zeitplan ist knapp. „Schon wegen des Fachkräftemangels in den Betrieben, aber auch bei Dienstleistern", sagt Richter. Laut Bitkom fehlen 149.000 IT-Fachkräfte.

Betroffen sind Fleischereibetriebe von der EU-Richtlinie grundsätzlich in jedem Fall. Als wesentliche Einrichtungen gelten mit Blick auf NIS-2 Unternehmen aus den Bereichen Energie, Verkehr, Wasserversorgung, digitale Infrastruktur und IT-Dienste, elektronische Kommunikationsdienste, Internet- sowie Telekommunikations- und -netzanbieter, Bank- und Finanzwesen, Gesundheit, Forschungseinrichtungen, öffentliche Verwaltung und Raumfahrt. Und als wichtig stuft der EU-Gesetzgeber Unternehmen aus dem Bereich der Abfallwirtschaft, Chemie, Post- und Kurierdienstleistung, Lebensmittel, Hersteller von Computern, Elektronik, Optik, Maschinen, Kraftfahrzeugen und Anhängern und Transportmittel, digitale Anbieter sowie Forschungseinrichtungen ein.

Auch Größengrenzen zieht die EU-Richtlinie. Als mittlere Unternehmen gelten solche mit 50 bis 250 Mitar-

beitern, zehn bis 50 Millionen Euro Umsatz und einer Bilanzsumme kleiner als 43 Millionen Euro jährlich. Als große Unternehmen gelten Betriebe mit mehr als 250 Mitarbeitern, mehr als 50 Millionen Euro Umsatz sowie einer Bilanzsumme von mehr als 43 Millionen Euro. Denkbar ist, dass die Anforderungen aber auch Unternehmen unterhalb dieser Größenordnungen betreffen, ist André Glenzer überzeugt, Partner bei PwC für Cyber Security & Privacy – als Zulieferer oder wichtiger Dienstleister. „Ein Kunde, den NIS-2 betrifft, wird irgendwann fragen, wie Sie die NIS-2-Anforderungen erfüllen", sagt Glenzer.

Risikomanagement ist Pflicht

Die neue EU-Richtlinie schreibt ein umfassendes Cyber-Risikomanagement vor, Dokumentation und Schulung der Beschäftigten, Sicherheit in der Lieferkette, ein ausgefeiltes Risiko- und Business Continuity Management, Verschlüsselung und diverse technische Maßnahmen, Authentifizierung, Zutrittsbeschränkungen, Abhilfemaßnahmen für den Fall von Sicherheitsverstößen sowie Berichterstattung an die Behörde.

Der Ansatz ist umfassend und die Umsetzung in höchstem Maß anspruchsvoll. Aber sinnvoll. Praktisch kein Experte beschwert sich über die komplexe EU-Vorgabe, im Gegenteil. „Wenn eine Festung fällt, fallen auch ganz viele Dörfer", erläutert es Richter. „Das war im Mittelalter so, und es ist auch heute so mit Blick auf Netzwerke von Unternehmen."

Schon mal gut da stehen Fleischereiunternehmen, die vielleicht bereits den BSI-Grundschutz installiert haben oder besser noch nach ISO 27001 zertifiziert sind. DIN EN ISO beziehungsweise IEC 27001 für Informationssicherheit gibt vor, wie Unternehmen Informations- und Cybersicherheit planen, umsetzen, überwachen und optimieren können. Unternehmen, die das alle drei Jahre zu erneuernde Audit durchlaufen, fehlt nicht viel zu den NIS2-Anforderungen. „Rund 80 Prozent der Vorgaben erfüllen nach ISO 27001 zertifizierte Unternehmen bereits", schätzt Glenzer.

NIS-2 wie auch ISO 27001 machen Vorgaben für einen IT-Grundschutz, die Netzwerksicherheit, regelmäßige Backups sowie Zugangskontrollen, NIS-2 fordert darüber hinaus auch, dass Unternehmen dies alles dokumentieren – und zwar so, dass es auch Unbeteiligte nachvollziehen können.

Schulung der Mitarbeiter

Fleischereiunternehmer müssen sich schon aus Datenschutzgründen mit der Sicherheit ihrer Server befassen – und wo diese stehen. Wichtig wird mit Blick auf das Cyberrisiko nun ein ausgefeilteres Berechtigungsmanagement für den physischen wie auch elektronischen Zugriff. Weil Cybersicherheit nicht nur eine Frage der Technik ist, sondern auch eine der Prozesse und der Menschen, ist die gründliche Schulung der Beschäftigten wichtig – der verantwortlichen Mitarbeiter sowieso fachlich-technisch, aber auch aller anderen Kollegen mit Blick auf Sensibilisierung. Wie bei ISO 27001 ist auch mit NIS-2 nun Schulung der Mitarbeiter Pflicht.

Bedenken sollten Fleischereiunternehmer: Die Backups müssen nicht nur im Fall eines Cybervorfalls parat stehen, sondern auch im Fall physischer Zerstörung der Systeme oder des Ausfalls der Elektrizität. Auch für die Sicherheit in der Lieferkette müssen sie gemäß der NIS-2-Richtlinie sorgen. Das ist auch der Grund, warum über kurz oder lang auch kleinere Fleischereibetriebe unterhalb der festgesetzten Größenordnungen in die Pflicht geraten dürften, die EU-Vorgaben beachten und dies auch nachweisen zu müssen – wenn Kunden oder Partnerbetriebe dies verlangen.

Wichtig auch: „Unternehmen müssen ihr Risikomanagement und die ganzen Sicherheitsmaßnahmen nicht nur implementieren und aufrechterhalten, sondern auch mal in einer Notfallübung die Krise durchspielen", sagt IT-Sicherheitsdienstleister Richter. „Also wenn alles fertig ist, ruhig auch mal testweise das Notfallteam zusammentrommeln und schauen, wie lange es braucht."

Vierstufiges Meldesystem

Selbst für bereits dank ISO 27001 gut aufgestellte Unternehmen kommt mit NIS-2 eine wichtige Anforderung ganz neu hinzu: das vierstufige Meldesystem. Bei einem sicherheitsrelevanten Vorfall müssen Unternehmen nach NIS-2-Vorgabe binnen 24 Stunden eine frühe Erstmeldung an das BSI absetzen und diese binnen 72 Stunden aktualisieren. Auf BSI-Anfrage müssen sie ad-hoc antworten und viertens innerhalb eines Monates eine Abschlussmeldung einreichen.

Ihre Pflichten zu delegieren, das ging nach Auffassung von PwC-Partner Glenzer eigentlich noch nie. „Mit NIS-2 gibt es nun ein gesetzliches Regulativ, das dies auch wirksam unterbindet", sagt er. Insbesondere die persönliche Verantwortung werde bislang noch unterschätzt. „Geschäftsführer haften über die Organhaftung – die Verantwortung für die Informationssicherheit kann deshalb nie, und ich meine wirklich niemals, delegiert werden", hebt er hervor.

Während NIS-2 bei den Anforderungen und Meldepflichten nur unwesentlich über NIS-1 hinausgeht, sind die geplanten Kontrollen und Strafen deutlich härter. Bußgelder für Verstöße gegen die Cybersecurity-Maßnahmen oder Meldepflichten betragen für wesentliche Einrichtungen bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Gesamtumsatzes des vorangegangenen Finanzjahrs und für wichtige Einrichtungen sieben Millionen Euro oder 1,4 Prozent des Vorjahresumsatzes. **Midia Nuri**

> „Rund 80 Prozent der Vorgaben erfüllen nach ISO 27001 zertifizierte Unternehmen bereits."
>
> André Glenzer, Partner bei PwC für Cyber Security & Privacy