Bayerischer Landtag

19. Wahlperiode 11.11.2026 **Drucksache** 19/**14479**

Dringlichkeitsantrag

der Abgeordneten **Holger Grießhammer, Ruth Müller, Florian von Brunn, Volkmar Halbleib, Anna Rasehorn, Doris Rauscher, Arif Taşdelen, Markus Rinderspacher, Horst Arnold, Nicole Bäumler, Martina Fehlner, Christiane Feichtmeier, Sabine Gross, Harry Scheuenstuhl, Dr. Simone Strohmayr, Ruth Waldmann, Katja Weitzel** und **Fraktion (SPD)**

Kühlketten vor Cyberangriffen schützen – Lebensmittelversorgung und medizinische Infrastruktur in Bayern krisenfest machen

Der Landtag wolle beschließen:

Die Staatsregierung wird aufgefordert, angesichts der jüngsten Cyberangriffe auf digital gesteuerte Kühlanlagen im europäischen Lebensmittelhandel und entsprechender Vorfälle in Bayern die Widerstandsfähigkeit der bayerischen Lebensmittelversorgung – von der Landwirtschaft über die Verarbeitung bis zum Handel – sowie der Blutbanken und der Arzneimittelinfrastruktur gegen digitale Angriffe gezielt zu stärken.

Hierzu soll die Staatsregierung insbesondere

– gemeinsam mit den zuständigen Fachbehörden, dem Bundesamt für Sicherheit in der Informationstechnik, dem Cyber-Allianz-Zentrum Bayern, dem Landesamt für Sicherheit in der Informationstechnik sowie den Verbänden der Landwirtschaft, der Lebensmittelwirtschaft, der Gastronomie, des Einzelhandels und des Kälteanlagenbauerhandwerks eine gezielte Informations- und Beratungsoffensive zur Absicherung digital gesteuerter Kühl- und Tiefkühlanlagen auf den Weg bringen, insbesondere für kleine und mittlere Betriebe.

– Cyberangriffe auf Kühl- und Steuerungstechnik als Szenario in die Planungen der staatlichen Ernährungsnotfallvorsorge aufnehmen und Vorkehrungen treffen, um die Grundversorgung der Bevölkerung mit Lebensmitteln auch bei einem großflächigen, gleichzeitigen Ausfall zahlreicher gewerblicher Kühlanlagen aufrechtzuerhalten.

– gemeinsam mit den Branchenverbänden praxisgerechte Handlungsempfehlungen für betriebliche Notfallkonzepte bei Cyberangriffen auf Kühlanlagen erarbeiten, die insbesondere unabhängige Temperaturüberwachung, frühzeitige Störungserkennung, sichere Notbetriebsverfahren, alternative Kühlmöglichkeiten sowie die Vermeidung unnötiger Lebensmittelverluste berücksichtigen.

– die bestehenden Warn-, Informations- und Abstimmungswege zwischen Cybersicherheitsbehörden, Lebensmittelüberwachung und betroffenen Wirtschaftsverbänden daraufhin überprüfen, ob sie eine frühzeitige Warnung sowie eine koordinierte Reaktion bei Cyberangriffen auf die Lebensmittelversorgung gewährleisten, und erkannte Lücken schließen.

– dem Landtag zeitnah über die bisherigen Erkenntnisse aus den aktuellen Cyberangriffen, die bestehenden Schutz- und Unterstützungsmaßnahmen sowie gegebenenfalls erforderliche weitere Schritte zur Verbesserung der Cybersicherheit in der bayerischen Land- und Lebensmittelwirtschaft und in der Kühlung von Blutprodukteinrichtungen und Arzneimitteln berichten.

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de - Dokumente abrufbar. Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de – Aktuelles/Sitzungen zur Verfügung.

Begründung:

Die jüngsten Cyberangriffe auf Kühl- und Tiefkühlanlagen in europäischen Supermärkten und Blutbanken verdeutlichen die Verwundbarkeit digital gesteuerter Infrastruktur. Nachdem bereits Mitte Oktober 2026 die Kühlanlagen Hunderter Supermärkte in Frankreich Ziel von Cyberangriffen geworden waren, kam es Anfang November zu weiteren Vorfällen in mehreren europäischen Ländern. Dabei wurden auch drei Einrichtungen des französischen Blutspendedienstes angegriffen. Dank funktionierender Alarm- und Überwachungssysteme konnten Schäden an Blutprodukten verhindert werden. Auch ein Edeka-Markt in Reisbach im Landkreis Dingolfing-Landau sowie Betreiber in den Landkreisen Roth und Neustadt an der Waldnaab waren betroffen. Nach Angaben des betroffenen Betreibers wurden die Kühlanlagen aus der Ferne auf einen Heizbetrieb mit einer Solltemperatur von 50 Grad Celsius umgestellt. Große Mengen verderblicher Lebensmittel mussten entsorgt werden. Die Polizei untersucht den Vorfall.

Bereits nach den Angriffen in Frankreich hatte das Bundesamt für Sicherheit in der Informationstechnik vor vergleichbaren Vorfällen in Deutschland gewarnt. Besonders problematisch sind unzureichend abgesicherte Fernzugriffe, veraltete Steuerungssysteme und fehlende Sicherheitsupdates. Betroffen sein können neben der Lebensmittel- und Arzneimittelindustrie und dem Einzelhandel auch Blutbanken, Labore, Krankenhäuser oder Gastronomie und Hotellerie.

Die Ereignisse zeigen, dass die Sicherheit der Lebensmittelversorgung zunehmend auch von der Sicherheit digitaler Anlagen abhängt. Fällt die Kühlung aus oder wird sie gezielt manipuliert, können innerhalb kurzer Zeit erhebliche wirtschaftliche Schäden und Lebensmittelverluste entstehen. Das betrifft nicht nur den Handel, sondern ebenso landwirtschaftliche Betriebe, Molkereien und Schlachtbetriebe, die auf eine funktionierende Kühlung angewiesen sind. Der Ausfall der Kühlung bei Blutprodukten oder Arzneimitteln ist ohnehin lebensgefährlich.

Die Verantwortung der Unternehmen für ihre betriebliche Sicherheit bleibt dabei unbestritten. Gerade kleinere Betriebe verfügen jedoch häufig nicht über eigene IT-Sicherheitsabteilungen und sind bei der Absicherung vernetzter technischer Anlagen auf externe Fachkenntnisse angewiesen.

Die landwirtschaftliche Primärproduktion sowie kleinere Lebensmittelverarbeiter und selbstständige Einzelhändler unterliegen in aller Regel nicht den besonderen Cybersicherheitspflichten des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen. Diese erfassen im Lebensmittelbereich insbesondere größere Unternehmen des Großhandels sowie der industriellen Produktion und Verarbeitung. Die Anforderungen des europäischen Cyber Resilience Act an sichere Produkte gelten erst ab Dezember 2027 und nur für neu in Verkehr gebrachte Geräte; die angegriffenen Altanlagen erfassen sie grundsätzlich nicht. Umso wichtiger sind praxisnahe Beratung und betriebliche Notfallvorsorge, die ohne unnötige zusätzliche bürokratische Belastungen auskommen. Zugleich muss die staatliche Ernährungsnotfallvorsorge einplanen, dass Angreifer Kühlanlagen in vielen Betrieben in einer einzigen Nacht manipulieren können – in Frankreich waren es Hunderte Märkte.

In Bayern wurden 2025 mehr als 49 400 Fälle von Cybercrime angezeigt. Die Bedrohungslage ist so vielschichtig wie nie zuvor und die Angriffsszenarien werden immer komplexer. Die Resilienz gegen Cyberangriffe in Staat, Wirtschaft und Gesellschaft muss daher dringend ausgebaut werden.

Ziel muss es sein, Sicherheitslücken frühzeitig zu erkennen, Betriebe bei wirksamen Schutzmaßnahmen zu unterstützen und im Ernstfall Lebensmittelverluste sowie Beeinträchtigungen der Versorgung so weit wie möglich zu verhindern.