Stellungnahme des Milchindustrie-Verbandes e.V. (MIV) zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

(Stand: 7. Dezember 2020)

Die Digitalisierung und das Internet verändern die Produktionsprozesse und Lieferketten in der gesamten Wirtschaft, so auch in der Lebensmittelindustrie. Eines der größten Herausforderungen der Zukunft ist dabei die IT-Sicherheit. Der Milchindustrie-Verband e.V. (MIV) begrüßt das Vorhaben der Bundesregierung, die IT-Sicherheit in Deutschland zu stärken. Die größten milchverarbeitenden Unternehmen fallen unter die BSI-KritisV und haben in den letzten Jahren bzw. Monaten IT-Sicherheitsmanagementsysteme eingeführt. Es ist zu erwarten, dass die Anzahl der betroffenen Unternehmen in der Milchindustrie mittelfristig steigen wird.

Der MIV möchte an dieser Stelle ausdrücklich die Vereinheitlichung der Vorschriften auf EU-Ebene betonen (NIS-Richtlinie). Die Aufnahme des Sektors Ernährung in die BSI-KritisV führt nach unserer Auffassung im internationalen- bzw. im EU-Vergleich zu einer Wettbewerbsverzerrung, da Deutschland strengere Vorgaben verlangt, als das EU-Recht. In anderen europäischen Ländern sind die Unternehmen der Lebensmittelindustrie z. B. bisher nicht zur Einführung eines IT-Sicherheitsmanagementsystems verpflichtet.

Darüber hinaus sollen aus Sicht des MIV in dem Entwurf die Hersteller und Lieferanten in Bezug auf die KRITIS-Anforderungen stärker berücksichtigt werden.

Im Folgenden übermitteln wir Ihnen unsere Anmerkungen zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) und bitten, diese im Gesetzgebungsprozess zu berücksichtigen.

Systeme zur Angriffserkennung (§8a)

Die geplanten Änderungen im § 8a des IT-SiG 2.0 verpflichten die Betreiber der kritischen Infrastrukturen zum Einsatz der Systeme zur Angriffserkennung und zwar spätestens ein Jahr nach dem Inkrafttreten des Gesetzes. Darüber hinaus müssen Betreiber Kritischer Infrastrukturen die für die Angriffserkennung und -nachverfolgung

Milchindustrie-Verband e.V. | Jägerstraße 51 | 10117 Berlin | Telefon +49 30 4030445-0 | Telefax +49 30 4030445-55 | E-Mail info@milchindustrie.de

relevante nicht personenbezogenen Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens vier Jahre speichern.

Aus Sicht des MIV ist der Einsatz solcher Systeme sinnvoll, die vorgegebenen Fristen sind allerdings nicht praktikabel und müssen dringend angepasst werden.

Bisher ist der Einsatz der Systeme zur Angriffserkennung in der Milchindustrie nicht verbreitet. Die Einführung beinhaltet in der Praxis oft eine sorgfältige Auswahl eines Dienstleisters und muss im Budget der Firmen berücksichtigt werden. **Der MIV schlägt vor, die Frist zum Einsatz der Systeme auf drei Jahre nach dem Inkrafttreten des Gesetzes zu verlängern.**

Darüber hinaus sollen für die Angriffserkennung und -nachverfolgung relevante nichtpersonenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens vier Jahre gespeichert werden. Der MIV lehnt diese Anforderung als praxisfern und nicht umsetzbar ab. Die notwendigen Speicherkapazitäten wären enorm. Kritisch zu sehen ist außerdem die Trennung personenbezogener Daten von nicht personenbezogenen Daten, da dies technisch nicht im angemessenen Verhältnis leistbar ist. Darüber hinaus würde die Forderung einer Vorhaltung von Protokollierungsdaten über vier Jahre den Aufbau eines technisch komplexen Archivierungssystems erfordern. Die zu erwartenden Mengen an anfallenden Protokollierungsdaten können in den Angriffserkennungssystemen selbst technisch nicht vorgehalten werden. **Die Daten sollen nach Auffassung des MIV drei bzw. bei Verdacht auf einen Angriff bis höchstens zwölf Monate gespeichert werden.**

Registrierung der Betreiber einer Kritischen Infrastruktur durch BSI (§ 8b)

Nach dem § 8b Absatz 3 IT-SiG 2.0 erhält das BSI die Befugnis zur Abfrage von schwellwertrelevanten Kennzahlen der Betreiber. Die Betreiber werden verpflichtet, dem Auskunftsersuchen unverzüglich nachzukommen. Darüber hinaus kann das BSI die Registrierung eines Betreibers einer Kritischen Infrastruktur auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt.

Der MIV stellt den Mehrwert dieser Regelung gegenüber dem bisherigen Registrierungsprozess in Frage. Durch § 8b entsteht Unsicherheit, weil grundsächlich jedes Unternehmen „benannt“ werden kann. Die Unsicherheit betrifft z. B. Unternehmen, die bisher knapp unter die Schwellen der BSI-KritisV fallen. *Kommt ein Betreiber einer kritischen Infrastruktur seiner Pflicht zur Registrierung nicht nach, kann das BSI den Betreiber auf seine Pflicht hinweisen und eine entsprechende Frist setzen.*

Untersagung des Einsatzes kritischer Komponenten (§ 9b)

Laut § 9b kann die Nutzung bereits im Einsatz befindlicher kritischer Komponenten untersagt werden. Das kann zu erheblichen Kosten führen (bspw. der Austausch aller aktiven Komponenten eines Netzwerkes), ohne dass hier der Komponentenhersteller in Haftung genommen wird. **Bei der Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller sind im IT-SiG 2.0 dringend weitere Maßnahmen vorzusehen, die für die Aufrechterhaltung der kritischen**

Geschäftsprozesse (trotz Untersagung) sorgen, realistische Übergangsfristen geben und die Pflicht zur Nennung von verfügbaren Austauschprodukten enthalten.

Betreiber werden an Stelle des Gesetzgebers in die Pflicht genommen, beim Hersteller eine Garantieerklärung einzuholen, welche an das BMI gesendet werden soll. Die Verwaltung und Übermittlung von Garantieerklärungen stellen einen erheblichen Aufwand dar. Daraus ergibt sich kein Mehrwert für den effektiven Schutz Kritischer Infrastrukturen.

Darüber hinaus müssen die Kriterien zur Auswahl von einsetzbaren „kritischen Komponenten“ zwingend festgelegt werden, um auf Betreiberseite Beschaffungsprozesse und die notwendige kurzfristige Reaktionsfähigkeit zur Aufrechterhaltung der Informationssicherheit auch im Gefahrenfall zu ermöglichen.

Detektion von Sicherheitsrisiken und Angriffsmethoden (§ 7b)

Angriffssimulationen vom BSI auf Betreiber Kritischer Infrastrukturen können zu Systemabstürzen führen. Sie müssen auf Schwachstellendetektion eingeschränkt werden. Zudem muss die Haftung, für die durch Schwachstellenanalysen ggf. hervorgerufenen Schäden, geklärt werden. **Vor der Detektion von Sicherheitsrisiken für die Netz- und Informationssicherheit eines Betreibers Kritischer Infrastrukturen durch das Bundesamt nach § 7 b sollte der betroffene Betreiber unverzüglich und ohne Ausnahmen informiert werden.**

Der Gesetzestext schränkt den Umfang der Angriffssimulation leider nicht ein. Es muss daher klar dargelegt werden: unter keinen Umständen darf es in diesem Zusammenhang zu unabgestimmten weiterführenden Tests (z. B. sog. Penetrationstests/ Red-Teaming-Tests) kommen. Das sind Tests, die weiter gehende Angriffe simulieren und üblicherweise durch explizit beauftragte IT-Sicherheitsexperten durchgeführt werden. In diesem Fall sogar mit Insiderwissen, auf Grund von Informationen, welche Betreiber gesetzlich verpflichtet an die Behörde übermitteln müssen (Liste kritischer Komponenten sowie Daten aus Systemen zur Angriffserkennung). Solche Tests stellen eine große Gefahr dar, da oft die Verfügbarkeit der angegriffenen Systeme beeinträchtigt sind oder sogar von außen in interne Netze eingedrungen wird und vertrauliche Daten offengelegt werden. Durch bewusste Gegenmaßnahmen des Betreibers können (kritische) Geschäftsprozesse unterbrochen werden und es drohen Schäden an kritischen Systemen (inkl. Haftungsfrage) durch unzureichendes branchenspezifisches Wissen der behördlichen IT-Sicherheitsexperten. Des Weiteren ist die Übermittlung von Daten aus Systemen zur Angriffserkennung zu unbestimmt und kann einen hohen Verwaltungsaufwand bedeuten.

Bei dem Einsatz von Systemen und Verfahren des BSI, welche einem Angreifer einen erfolgreichen Angriff vortäuschen (Honeypot, Artikel 1 § 7b (4) BSI-G), muss im Gesetz geregelt sein, dass der Einsatz von branchenspezifischen Lösungen (z. B. Produktionsanlagen, Industrielle Kontrollsysteme) mit den Betreibern abgestimmt sein muss, um hier keine „Lernplattform“ für Angreifer zu schaffen.

Bußgelder (§ 14)

Der vorliegende Entwurf sieht eine deutliche Erhöhung der Bußgelder vor. Bisher sah das Gesetz einen kooperativen Ansatz zwischen Behörden und KRITIS-Betreibern vor. Dieser Weg wird jetzt ohne Grund verlassen.

Der in den Bußgeldvorschriften neu eingeführte Verweis auf das Ordnungswidrigkeitengesetz, der zu einer Erhöhung um das 200-Fache des jetzigen Sanktionsmaßes führen kann, muss aus Sicht des MIV gestrichen werden, da ein derart enormes Sanktionsmaß wiederum zu einer extremen Unverhältnismäßigkeit führt.

Es ist ferner sicher zu stellen, dass es nicht zu einer Doppelregulierung/ -bestrafung durch DSGVO und IT-SIG 2.0 kommen kann (sobald personenbezogene Daten betroffen sind).

Bei Rückfragen stehen wir Ihnen gerne zur Verfügung.

Vielen Dank.

i. V. Marcin Preidl
Referent