BVLH
Bundesverband des
Deutschen Lebensmittelhandels

HDE
Handelsverband
Deutschland

Handelsverband Deutschland • 10873 Berlin

An den Bundestagsausschuss für Inneres

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)297

15.04.2015

„Entwurf des IT-Sicherheitsgesetzes“

Sehr geehrte «Anrede» «Name»,

derzeit befindet sich der Entwurf des IT-Sicherheitsgesetzes in der parlamentarischen Abstimmung. Wir möchten hierzu nicht erneut Stellung nehmen und verweisen auf die Positionen des BVLH und des HDE in anliegendem PDF-Dokument.

Eindringlich hinweisen möchten wir Sie allerdings auf eine Unstimmigkeit in der Begründung (B. Besonderer Teil) des Entwurfes. Zu Nummer 8 (§ 10 Ermächtigung zum Erlass von Rechtsverordnungen) zu Buchstabe a (Kriterien zur Bestimmung der Kritischen Infrastrukturen). Dort werden die unterschiedlichen Sektoren aufgeführt, die kritische Dienstleistungen im Sinne des Gesetzes sein können. Unter Nummer 6 wird der Sektor „Ernährung“ genannt. In der Klammer werden dann die Bezeichnungen „Ernährungswirtschaft“ und „Lebensmittelhandel“ ergänzt.

Dies ist u.E. eine nicht richtige Darstellung. Laut allgemein anerkannter Definition umfasst die Lebensmittelwirtschaft bzw. Ernährungswirtschaft als Wirtschaftszweig die Wirtschaftsbereiche, die sich mit Produktion, Verarbeitung und Handel von Lebensmitteln bzw. Nahrungsmitteln befassen. Daher ist die zusätzliche Nennung von Lebensmittelhandel eine Doppelbenennung, die nicht nachvollziehbar ist, gängigen Einteilungen widerspricht und entsprechend zu streichen ist.

Im Vergleich hierzu wird unter Sektor „Energie“ (Nummer 1) bei den Stromversorgern auch nicht unterschieden in Netzbetreiber und Stromerzeuger.

Insofern möchten wir Sie dringend um entsprechende Korrektur des Entwurfes zum IT-Sicherheitsgesetz bitten.

Mit freundlichen Grüßen

Ulrich Binnebößel
Handelsverband Deutschland

Christian Mieles
Bundesverband des Deutschen Lebensmittelhandels

Ulrich Binnebößel
Am Weidendamm 1 A
10117 Berlin
Telefon: (030) 72 62 50-62
Telefax: (030) 72 62 51-88
E-Mail: binneboessel@hde.de
www.einzelhandel.de

Referentenentwurf
für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Stellungnahme des Handels

Einleitung

Das Bundesministerium des Innern (BMI) übermittelte am 4. November 2014 den betroffenen Wirtschaftszweigen einen Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) zur weiteren Abstimmung.

Die Verbände BVLH und HDE nehmen, stellvertretend für die Unternehmen des deutschen Lebensmittel-Einzelhandels, aufgrund der besonderen Betroffenheit der Branche nachfolgend zum Vorschlag Stellung:

Kernelement des Vorschlages/Betroffenheit

Angelehnt an den ersten Vorschlag aus dem Jahre 2013 soll auch mit dem jetzt vorgelegten Entwurf eines IT-Sicherheitsgesetzes eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland erreicht werden, was der Lebensmittelhandel ausdrücklich begrüßt.

Was die wesentlichen Kernelemente des jetzigen Regelungsvorschlages betrifft, gilt für Betreiber Kritischer Infrastrukturen künftig u. a.:

- eine Verpflichtung binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung angemessene Vorkehrungen und Schutzmaßnahmen zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind;
- dass sie oder ihre Verbände branchenspezifische Sicherheitsstandards vorschlagen können;
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mindestens alle zwei Jahre eine Aufstellung der durchgeführten Sicherheitsaudits, Prüfungen oder Zertifizierungen, einschließlich der dabei aufgedeckten Sicherheitsmängeln, zu übermitteln;
- bei Sicherheitsmängel dem BSI auf Verlangen die Unterlagen zur Verfügung zu stellen;

- dem BSI binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung Warn- und Alarmierungskontakte zu benennen, über die er jederzeit erreichbar ist;
- die Beeinträchtigung ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung führen können, unverzüglich an das BSI (ggf. anonym) zu melden;
- führt eine Beeinträchtigung zu einem Ausfall oder zu einer Beeinträchtigung der Kritischen Infrastruktur, dies unverzüglich über seine Warn- und Alarmierungskontakte unter Angabe der Informationen an das BSI zu melden.

In Betrachtung dieser sehr weitreichenden Regelungselemente sollte aus Sicht des Lebensmittelhandels zunächst sehr sorgfältig geprüft werden, welche Branchen und Wirtschaftszweige als unmittelbar gefährdete Kritische Infrastrukturen einzustufen sind. Hier pauschal und ohne nähere Begründung den Sektor Ernährung einzubeziehen, der dann in der Begründung in Richtung der Branchen Ernährungswirtschaft und Lebensmittelhandel konkretisiert wird, halten wir weder für nachvollziehbar noch für zielführend.

Besonderheiten des Lebensmittelhandels

Bereits in der Stellungnahme des Lebensmittelhandels zum ersten Gesetzesvorschlag, die wir Ihnen am 5. April 2013 übermittelt hatten, stellten wir nach eingehender Analyse fest, dass die Gefahr flächendeckender Versorgungsengpässe aufgrund von Cyberattacken als sehr gering eingeschätzt wird. Zwar bestehen durchaus Möglichkeiten, dass es in einzelnen Unternehmen oder Unternehmensteilen zu Störungen des Betriebes kommt, ein flächendeckender Ausfall über längere Zeit wird aber mit Blick auf die Anbieter- und Systemvielfalt im Handel - wie nachfolgend dargestellt - als wenig realistisch eingestuft:

- Der Lebensmittelhandel ist durch eine Vielzahl einzelner Unternehmenseinheiten gekennzeichnet.
- Der Betrieb der Geschäfte und die dazu erforderliche IT-Infrastruktur werden jeweils individuell, also je Vertriebslinie und Region, gesteuert. Es gibt keine unternehmensübergreifenden Netzwerke.
- Der Einsatz der IT-Systeme (Hardware und Software) im Handel ist äußerst heterogen und ist von einer Vielzahl von Anbietern und Eigenentwicklungen geprägt.
- Die Unternehmen haben aus Eigeninteresse umfangreiche Maßnahmen zur Herstellung einer größtmöglichen IT-Sicherheit ergriffen.
- Bei einem IT-Komplettausfall kann über Notfallprozeduren der Betrieb - bis zu zwei Wochen - aufrechterhalten werden. Beispielsweise können Filialen bei Ausfall des Bestellwesens mit „Verdachtsbelieferungen“ versorgt werden.
- Meist unterschiedliche IT-Automatisierungssysteme steuern Lagerung und Filialbetrieb der Unternehmen.
- Trotz großer Umschlagsgeschwindigkeit reichen die Bestände einer Filiale zumindest für mehrere Tage aus.
- Die Bestände auf Großhandelsstufe sind teils durch manuelle Prozesse noch nutzbar.

Im Ergebnis wird deutlich, dass allein die große Vielfalt an Unternehmenseinheiten dazu führt, dass eine flächendeckende Gefährdung aller Unternehmen durch Cyberattacken sehr unwahrscheinlich ist. Hinzu kommen die ganz unterschiedlichen IT-Systeme im Handel. Dies trägt ebenfalls zur Erkenntnis bei, dass ein zentraler Angriff mit Auswirkungen auf alle Unternehmen des Lebensmittelhandels nur schwer möglich ist. Kritische Infrastrukturen, deren Ausfall die Versorgung der Bevölkerung gefährden könnten, sind daher im Lebensmittelhandel nicht auszumachen.

Doppelte Betroffenheit des Lebensmittelhandels

Der Entwurf sieht unter anderem auch den Sektor Transport und Verkehr als kritische Dienstleistungen vor. Hierzu stellen wir fest, dass wesentliche Teile des Handels auf logistischen Prozessen basieren. Die Lagerung von Waren und Bündelung über Zentralläger mit anschließender Belieferung der Filialen ist eine klassische Transportleistung, die bereits im Spiegelstrich „Transport von Gütern“ im genannten Sektor aufgegriffen wird. Große Bereiche bzw. die möglicherweise als kritisch erkannten Prozesse des Handels wären daher ohnehin bereits von der Regulierung betroffen.

Handel bereits heute umfassend in der Pflicht

Aus den Handelshäusern wird zudem deutlich darauf hingewiesen, dass sich aus den im Unternehmensumfeld anwendbaren Gesetzen bereits heute konkrete Verpflichtungen für die Gewährleistung eines angemessenen IT-Sicherheitsniveaus in den Unternehmen ableiten lassen.

Die Unternehmen des Lebensmittelhandels setzen diese gesetzlichen Forderungen - auch im eigenen Interesse - schon heute um. Dies geschieht insbesondere zur Absicherung der Geschäftsprozesse und somit zur Sicherstellung des Fortbestandes des eigenen Unternehmens.

Hingegen wird ein weiteres Gesetz, wie im konkreten Fall das IT-Sicherheitsgesetz, als nicht geeignet eingestuft, das IT-Sicherheitsniveau in den Unternehmen zu erhöhen. Dies wird wie folgt begründet:

- Die bereits heute zur Verfügung stehenden Gesetze, Normen, Standards und Regelwerke sind völlig ausreichend, um ein angemessenes Niveau für Informationssicherheit in allen Unternehmen der Lebensmittelbranche zu etablieren (Beispiele hierfür: BDSG, GmbHG, AktG, HGB, KonTraG, TKG, PCI-DSS etc.). So besteht eine Meldepflicht für Datenschutzvorfälle beispielsweise bereits heute.

- Mit Blick auf und in Anpassung an aktuelle Bedrohungen heben die Handelsunternehmen schon heute ihre jeweiligen IT-Sicherheitsniveaus kontinuierlich an. Dies geschieht in Eigenverantwortung und aus Eigeninteresse eines jeden Unternehmens und ist in der notwendigen Dynamik mit gesetzlichen Regelungen nicht geeignet abbildbar.

- Die Unternehmen können ihre IT jedoch nur gegen elementare, einfache Angriffe absichern (Stichwort: Hackerkids). Dies machen die Handelsunternehmen bereits seit vielen Jahren. Gegen Angriffe staatlicher oder terroristischer/krimineller Organisationen haben die Unternehmen kaum Möglichkeiten.

  Dazu das folgende Zitat von Dr. Sandro Gayken (Institute of Computer Science, AG Secure Identity, Freie Universität Berlin) in einer schriftlichen Stellungnahme vom Mai 2014 für den Deutschen Bundestag:

  Sicherheit ist relativ. Eine sichere Kommunikation gegen schwache Angreifer (Kleinkriminelle, Aktivisten) ist mit bestehenden Techniken unter akzeptablen Kollateralschäden möglich, sofern diese Techniken dem Stand der Technik entsprechen, agil, effektiv und effizient sind und korrekt implementiert und bedient werden.

  Eine sichere Kommunikation gegen starke Angreifer (organisierte Kriminelle, Nachrichtendienste, Militärs) ist gegenwärtig nicht möglich. Das „normale" Modell der Rechnersicherheit ist diesen Angreifern gegenüber konzeptionell überfordert und überholt. Dieses normale Modell hat sich aus Grundannahmen zur Computersicherheit der Sechziger bis Achtziger Jahre herausgebildet. (…)

  Die vollständige Stellungnahme ist als **Anlage** beigefügt.

- Anmerken möchten wir zudem, dass die Handelsunternehmen eine Meldepflicht an das BSI als nicht zielführend einschätzen. Äußerst kritisch vom Handel gesehen bis ablehnend eingeschätzt wird zudem, ihre IT-Sicherheit mit den genannten Einschränkungen von heute von diesbezüglich derzeit nur bedingt kompetenten Stellen und Einrichtungen (BSI, TÜV o. ä.) testieren zu lassen. Derartig vorgesehene Testierungen werden handelsseitig als Fehlleitung von Ressourcen eingestuft, die die IT-Sicherheit nicht erhöhen werden.

- Hingegen würde eine Stärkung des BSI hinsichtlich Personal und Etats handelsseitig ausdrücklich unterstützt. Dies könnte und sollte jedoch ganz unabhängig von einem IT-Sicherheitsgesetz durchgeführt werden. Damit sollte die aktive Information des BSI und ggf. anderer staatlicher Stellen über konkrete, bekannte Bedrohungen gestärkt werden, die dann schneller und umfassender erfolgen könnte, um den Unternehmen verbesserte Möglichkeiten der Reaktion geben zu können.

Unverhältnismäßige Kostenbelastung durch fragwürdige neue Verpflichtungen

Derzeit lässt sich nicht einschätzen, welche konkrete Kostenbelastung auf den Handel zukommen würde. Es ist nicht bekannt, welche Einrichtungen, Betriebe oder Betriebsteile des Lebensmittelhandels in welchen Regionen einbezogen werden sollen. Jedoch wird bereits in diesem Entwurfsstadium deutlich, dass den Betreibern absehbar zusätzliche Kosten entstehen. Dies geht beispielsweise aus § 8a Abs. 3 BSIG-E hervor, der den Betreibern Nachweispflichten mit verpflichtenden

Sicherheitsaudits, Prüfungen oder Zertifizierungen auferlegt. Die im Vorwort des Gesetzentwurfs unter E.II (S. 4) enthaltene Aussage, Mehrkosten würden nur dort verursacht, „wo bislang noch kein hinreichendes Niveau an IT-Sicherheit bzw. keine entsprechenden Meldewege etabliert sind“, ist insoweit nicht plausibel. Es muss davon ausgegangen werden, dass für alle Betreiber Kritischer Infrastrukturen erhebliche Mehrkosten entstehen.

Meldepflichten zu weitreichend

Durch die Ersetzung der Worte „andere Stellen“ durch das Wort „Dritte“ in § 3 Abs. 1 Satz 2 Nr. 2 BSIG-E könnte im Zweifel eine Erweiterung des Kreises derjenigen ergeben, an die Informationen weitergegeben werden: „Andere Stellen“ konnte noch dahingehend einschränkend ausgelegt werden, dass staatliche Stellen Informationen erhalten. Dies erscheint bei dem Begriff „Dritte“ nicht mehr möglich. Die einzig verbleibende Anforderung, dass die Zurverfügungstellung der Information an den Dritten nur dann erfolgen darf, wenn dies zur Erfüllung seiner Aufgaben - welche Aufgaben, wird nicht gesagt - erforderlich ist, ermöglicht eine zu weitgehende Weitergabe von Informationen, die die Betreiber der Kritischen Infrastrukturen betreffen, an beliebige Dritte. Der Entwurf sollte an dieser Stelle konkretisiert und auf die Weitergabe an staatliche Stellen beschränkt werden.

Hiermit zusammenhängend: § 8c BSIG-E stellt für die Auskunft des BSI an Dritte auf die schutzwürdigen Interessen der Betreiber ab, ohne dass erkennbar wäre, wie das BSI diese schutzwürdigen Interessen erkennen soll. Eine Abstimmungspflicht mit den Betreibern erscheint mindestens dann geboten, wenn es sich bei den Dritten nicht um staatliche Stellen handelt.

Dass die Betreiber Kritischer Infrastrukturen gemäß § 8b Abs. 4 Beeinträchtigungen ihrer IT-Systeme, Komponenten oder Prozesse schon dann unverzüglich an das BSI melden müssen, wenn diese zu einem Ausfall oder einer Beeinträchtigung der „Kritischen Infrastrukturen führen können“, führt bereits bei einer sehr geringen Wahrscheinlichkeit der Betroffenheit zu einer Meldepflicht. Beispielsweise wäre bei einem beliebigen Virenbefall, dessen völlige Ungefährlichkeit noch nicht 100%ig abschließend feststeht, die sofortige Meldung erforderlich. Richtiger erscheint, hier erstens eine angemessenere Schwelle für das Maß der Wahrscheinlichkeit einzufügen und zweitens zusätzlich zu verlangen, dass mindestens eine schwerwiegende Beeinträchtigung der Kritischen Infrastruktur drohen muss.

Keine Vorratsdatenspeicherung durch die Hintertür

Der Handel wendet sich gegen eine verpflichtende Ausweitung der Speicherung von Nutzungsdaten. Dies kommt einer Einführung der Vorratsdatenspeicherung durch die Hintertür gleich. Zwar wird in Artikel 2 „Änderung des Telemediengesetzes“ (§ 15 Abs. 9 TMG neu) derzeit lediglich eine Option zur Speicherung von Nutzungsdaten gegeben. In der Auslegung und auch der weiteren Diskussion zum Entwurf besteht jedoch die Gefahr, dass eine „Quasi-Verpflichtung“ des Diensteanbieters zur Erhebung von Nutzerdaten besteht, will er den Anforderungen der Gefahrenabwehr genügen.

Handlungsbedarf: Energie und Telekomunikation

Flächendeckende Störungen der Energieversorgung und der Telekommunikation können hingegen dazu führen, dass auch der Lebensmittelhandel in seiner Versorgungsfunktion deutlich eingeschränkt wird. Insofern ist eine mittelbare Gefährdung des Handels durch die Abhängigkeit von Stromversorgung und Telekommunikation gegeben.

Werden jedoch Maßnahmen zum erweiterten Schutz der Stromversorgung und Telekommunikation ergriffen, ist auch diese mittelbare Gefährdungslage wirksam eingedämmt. Vor diesem Hintergrund begrüßt es der Handel, dass die Sektoren Energie und Telekommunikation im besonderen Fokus des vorgelegten Gesetzentwurfes im Hinblick auf die Prävention gegen Cyberattacken stehen.

Dieser besondere Fokus findet sich zudem im von der EU-Kommission (KOM) vorgelegten Richtlinienvorschlag vom Februar 2013 wieder, der Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union vorsieht. Auch in diesem Vorschlag befinden sich (siehe Anhang II) diverse adressierte Marktteilnehmer, wie Telekommunikationsdienste und Energieversorger. Jedoch ist der Ernährungssektor mit der Branche Lebensmittelhandel dort zu Recht nicht aufgeführt, da wohl auch die KOM erkannt hat, dass hier kein Handlungsbedarf besteht.

Auch im aktuellen Koalitionsvertrag der Bundesregierung „Deutschlands Zukunft gestalten“ ist die notwendige Schaffung eines IT-Sicherheitsgesetzes formuliert, ohne jedoch explizit den Sektor Ernährung mit der Branche Lebensmittelhandel zu adressieren.

Schlussbemerkung

Der Gesetzentwurf sieht zusätzliche IT-Sicherheitsmaßnahmen und Meldepflichten für den Lebensmittelhandel vor, die auf handelsseitige Ablehnung stoßen, da diese im Ergebnis unserer Analyse nicht zielführend und in ihren belastenden Auswirkungen als hochgradig unverhältnismäßig eingestuft werden müssen.

Vor diesem Hintergrund fordern BVLH und HDE mit Nachdruck die Bundesregierung auf, den Lebensmittelhandel vom Anwendungsbereich des Gesetzes vollständig auszunehmen. Zudem sollte zunächst die europäische Richtlinie abgewartet werden. Der deutsche Gesetzgeber sollte im Sinne einheitlicher Regelungen und zur Vermeidung von Wettbewerbsverzerrungen zulasten deutscher Unternehmen nicht über die europäischen Vorgaben hinausgehen.

BVLH/HDE, Berlin, 13. November 2014