Fränkische Straße 2 · 53229 Bonn
Telefon +49 228 98849-0 · Telefax +49 228 98849-99
info@bvse.de · www.bvse.de

Bundesverband Sekundärrohstoffe
und Entsorgung e. V.

Stellungnahme zum Referentenentwurf des BMI zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

I. Vorbemerkung

Der bvse-Bundesverband Sekundärrohstoffe und Entsorgung e.V. vertritt als führender Branchendachverband die Interessen von mehr als 1.000 überwiegend mittelständischen Entsorgungs- und Recyclingunternehmen aus Deutschland und Europa. Die qualifizierten Umweltdienstleister beschäftigen etwa 60.000 Arbeitnehmer. Im bvse sind alle Fachsparten der Recycling-, Sekundärrohstoff- und Entsorgungsbranche vertreten.

II. Allgemein

Wir begrüßen grundsätzlich das Ziel des Gesetzes, die Cybersicherheit von Staat und Wirtschaft durch das NIS2UmsuCG zu stärken.

Wir sind aber der Auffassung, dass die in dem Gesetz enthaltenden Anforderungen und der damit verbundene Kosten- und Personalaufwand gerade im Hinblick auf mittelständische Unternehmen der privaten Entsorgungswirtschaft unverhältnismäßig sind.

III. Im Einzelnen

1. Anwendungsbereich gem. § 28 Abs. 2 Ziffer 3

Gem. § 28 Abs. 2 Ziffer 3 liegt eine „wichtige Einrichtung“ vor, wenn Dienstleistungen angeboten werden, die einer der in Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen ist und

a) mindestens 50 Mitarbeiter beschäftigt oder
b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweist.

Zur der in Anlage 1 aufgeführten Einrichtungsarten gehört auch die „Abfallbewirtschaftung“ i.S. d. § 3 Nr. 14 KrWG. Damit fällt ein erheblicher Teil der privaten mittelständischen Entsorgungsunternehmen in den Anwendungsbereich.

Dies halten wir für völlig überzogen und keineswegs gerechtfertigt. Sowohl beim Kritis-DachG als auch bei dem bisherigen BSIG beschränkte sich der Anwendungsbereich im Bereich der Abfallbewirtschaftung auf die Siedlungsabfallentsorgung.

Diese Regelung war sinnvoll und nachvollziehbar. Die Siedlungsabfallentsorgung ist Teil der Daseinsvorsorge und wird daher ab gewissen Schwellenwerten zu Recht als kritische Infrastruktur angesehen. Ihr Ausfall würde bei Anlagen ab dem festgelegten Schwellenwert zu einer Beeinträchtigung der Bevölkerung führen. Anders sieht dies aber in anderen Bereichen der Abfallbewirtschaftung aus. Hier stellt ein vorübergehender Ausfall zwar den unmittelbaren Anlagenbetreiber vor Probleme. Dies führt aber nicht zu einem Ausfall eines Teiles der Infrastruktur, zumal andere Anlagenbetreiber aus der Branche den Ausfall regelmäßig kompensieren können.

Der Anwendungsbereich in Anlage 1 sollte sich daher wie beim Kritis-DachG auf die Siedlungsabfallentsorgung beschränken und nicht auf die gesamte Abfallbewirtschaftung erweitert werden.

2. § 2 Nr. 39 Definition „Sicherheitsvorfall“

§ 2 Nr. 39 definiert den „Sicherheitsvorfall“. Danach liegt ein Sicherheitsvorfall vor, wenn ein Ereignis die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt werden.

Wir halten die Definition für zu weitgehend. Dass ein Ereignis, das die Integrität und Vertraulichkeit personenbezogener Daten i.S.d. DSGVO gefährdet, einen Sicherheitsvorfall darstellt, versteht sich von selbst.

Wir halten es aber für verfehlt, wenn jedes Ereignis, dass zu einer vorübergehenden fehlenden Verfügbarkeit von Daten führt, einen Sicherheitsvorfall darstellen soll. Ursache hierfür könnte ein Stromausfall, ein Wasserrohrbruch oder lediglich ein internes IT-Problem des Unternehmens sein.

Solange die fehlende Verfügbarkeit nicht durch Fremdeinwirkung von außen herbeigeführt wird, macht es u.E. keinen Sinn, hier eine Meldung zu fordern. Dies würde zum einem das Meldeportal überfrachten und wäre zum anderen auch nicht mit einem Mehrwert/Informationsgewinn für andere Unternehmen verbunden.

Die Definition des Sicherheitsvorfall gem. § 2 Nr. 39 sollte sich auf ein auf Fremdeinwirkung beruhenden Cybersicherheitsereignis beschränken.

3. § 30: Risikomanagementmaßnahmen

In § 30 muss dringend eine realistische Umsetzungsfrist für die Unternehmen festgelegt werden. Betroffenen Unternehmen, die erstmalig mit Inkrafttreten dieses Gesetzes in den Anwendungsbereich fallen, ist es nicht möglich, innerhalb kürzester Zeit die geforderten Risikomanagementmaßnahmen zu ergreifen. Für die Erstellung eines Risikomanagements und der Umsetzung der Maßnahmen werden durchschnittlich 12- 18 Monate benötigt. Man kann den betroffenen Unternehmen daher realistisch allenfalls zumuten, zeitnah ab Inkrafttreten des Gesetzes, nachweislich mit den Maßnahmen zu beginnen. Auch wenn seitens des Bundesamtes für Sicherheit in der Informationstechnik zunächst keine Nachweise angefordert werden sollten, stellt sich die Frage, was ist mit Unternehmen, die unmittelbar nach Erlass des Gesetzes einen Cybervorfall melden müssen und dann kein Risikomanagement vorweisen können. Diese dürfen letztendlich nicht anders behandelt werden als Unternehmen, die keinen Vorfall melden mussten, aber ebenfalls noch kein Risikomanagement vorweisen können. Hier bedarf es einer klaren Regelung.

a. § 30 Abs.1 und Abs. 2

Wir begrüßen ausdrücklich, dass § 30 Abs. 1 hervorhebt, dass bei den Maßnahmen für das Risikomanagement der Grundsatz der Verhältnismäßigkeit zu berücksichtigen ist.

Auf Grund der in § 30 Abs. 2 dargelegten Anforderungen wird dieser gute und richtige Ansatz aber wieder verwässert, indem ein Teil der Maßnahmen als zwingend angesehen werden. So heißt es in § 30 Abs. 2 S.2: „Diese Maßnahmen **müssen** zumindest Folgendes umfassen…“

Wenn der Grundsatz der Verhältnismäßigkeit gem. § 30 Abs.1 tatsächlich gewahrt werden soll, dann muss dieser alle Maßnahmen miteinbeziehen.

In § 30 Abs.2 S. 2 sollte daher das Wort „müssen" durch „sollten" ersetzt werden.

b. § 30 Nr. 4

Für problematisch erachten wir auch die Regelung in § 30 Nr. 4. Hiernach sollen die betroffenen Unternehmen Maßnahmen zur Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstanbietern ergreifen.

Das Ergebnis dieser Regelung darf nicht dazu führen, dass Unternehmen, die nicht in den unmittelbaren Anwendungsbereich des NIS2UmsuCG fallen, dann durch Vertragspartner, die in den Anwendungsbereich fallen, gezwungen werden, ebenfalls die Sicherheitsstandards des NIS2UmsuCG zu erfüllen. Hier sollte klarer herausgestellt werden, dass § 30 Abs.2 Nr. 4 keine Verpflichtung der unmittelbaren Vertragspartner beinhaltet, Sicherheitsmaßnahmen nach dem NIS2UmsuCG zu ergreifen.

4. § 38: Billigungs-, Überwachungs- und Schulungspflichten der Geschäftsleitung besonders wichtiger und wichtiger Einrichtungen

Gem. § 38 Abs. 2 ist ein Verzicht der Einrichtung auf Ersatzansprüche gegenüber der Geschäftsleitung sowie ein Vergleich, der ein grobes Missverhältnis zugunsten der Geschäftsleitung darstellt, unwirksam.

Eine solche Regelung findet sich in dieser Form nicht in der NIS-2-Richtlinie und sollte gestrichen werden. Es gibt bereits für jede Geschäftsform ausreichend gesetzliche Haftungsregelungen (z.B. Geschäftsführerhaftung nach dem GmbhG). Es ist kein Grund ersichtlich, warum hier dem Unternehmen verboten werden sollte, eine Einigung nach dem eigenen Ermessen zu treffen.

Nicht jede „Geschäftsleitung" ist ein gut dotierter Manager einer Aktiengesellschaft mit einem zweistelligen jährlichen Millionengehalt. Gerade bei den mittelständischen Unternehmen handelt es sich häufig um Geschäftsführer, die gleichzeitig Mitgesellschafter oder alleinige Gesellschafter der GmbH sind. Hier kann eine sinnvolle Einigung durchaus auch im Interesse des Fortbestandes der GmbH sein.

Bonn, 28. Mai 2024

[redacted]
Hauptgeschäftsführer