19.03.2021

An
Frau Dr. Papenkort
Referat CI 1
Grundsatz; Cyber- und Informationssicherheit
Bundesministerium des Innern, für Bau und Heimat
Alt Moabit 140, 10557 Berlin

Bearbeitet von

Tim Bagner (DST)
Telefon: +49 30 37711-610
E-Mail: tim.bagner@staedtetag.de
Aktenzeichen: 70.28.05 D

Michael Schmitz (DLT)
Telefon: +49 30 590097-361
E-Mail: michael.schmitz@landkreistag.de

Dr. Klaus Nutzenberger (DStGB)
Telefon: +32 (0)2 740 16 40
E-Mail: klaus.nutzenberger@eurocommunal.eu

Simon Kessel (VKU)
Telefon: +49 170 8580 125
E-Mail: kessel@vku.de

Stellungnahme zum Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS 2) vom 16.12.2020

Sehr geehrte Frau Dr. Papenkort,

die Bundesvereinigung der kommunalen Spitzenverbände (BV) und der Verband kommunaler Unternehmen e.V. (VKU) begrüßen, dass die NIS 2-Richtlinie die Cybersicherheitsstandards in der gesamten Europäischen Union erhöhen soll. **Die Sicherheit und Integrität der Systeme sowie die Gewährleistung der Ver- und Entsorgungssicherheit haben für die Kommunalwirtschaft und die Kommunen oberste Priorität, und der Vorschlag der Kommission kann hierzu einen wesentlichen Beitrag leisten.** Allerdings sollte hier mit Augenmaß vorgegangen werden. Eine unverhältnismäßige, wirtschaftlich schädliche Mehrbelastung darf nicht das Resultat der Harmonisierungsbestrebungen werden. Der aktuell vorliegende Richtlinienvorschlag wäre für eine Vielzahl kommunaler Unternehmen der Versorgungs- und Entsorgungswirtschaft mit erheblichem Erfüllungsaufwand verbunden, weshalb an einigen Stellen nachgebessert werden sollte. Insgesamt sollte aus Sicht der BV und des VKU stärker auf das Verhältnis zwischen angestrebtem Sicherheitsniveau und damit verbundener Mehrbelastung geschaut werden. Mehr Spielraum zur Differenzierung der Sicherheitspflichten kann es den Mitgliedsstaaten erlauben, eine zweckmäßige und passgenaue Balance von sinnvollen Sicherheitsmaßnahmen und einer verträglichen Mehrbelastung der Betreiber zu finden.

Zusammenfassung der Kernpunkte

Artikel 18: Risikomanagementmaßnahmen im Bereich der Cybersicherheit

- **Abs. 2**: Eine pauschale Verpflichtung aller Betreiber zur Umsetzung des gesamten Maßnahmenkatalogs ist aus unserer Sicht nicht zielführend, da keine Differenzierung nach sektoral sinnvollen Sicherheitsmaßnahmen möglich wäre. Wir empfehlen daher, nationalen Gesetzgebern die Möglichkeit zur sektoralen Differenzierung der Sicherheitsmaßnahmen einzuräumen, um eine Abwägung zwischen Sicherheitsniveau und Erfüllungsaufwand der Betreiber zu ermöglichen.
- **Abs. 6**: Die Kommission sollte in Art. 18 Abs. 6 zu Durchführungsrechtsakten und nicht zu delegierten Rechtsakten ermächtigt werden, um die formale Einbindung der Mitgliedsstaaten bei der Erweiterung des Maßnahmenkatalogs aus Art. 18 Abs. 2 zu gewährleisten.
- **Abs. 2 Buchst. d**: Bei der Gewährleistung der „Sicherheit der Lieferkette“ wäre eine faire Verteilung der Haftung zwischen Betreiber und Zulieferer angemessen. Bei kritischen Komponenten sollten nationale Behörden bei der Risikobewertung eingebunden werden, insbesondere um kleine Betreiber zu entlasten.

Artikel 2: Anwendungsbereich

Um die vorgesehene Ausnahme für kleine- und Kleinstunternehmen aus dem Anwendungsbereich der Richtlinie auch für kommunale Unternehmen einschlägig zu machen, empfehlen wir Art. 3 Abs. 4 des Anhangs der Empfehlung 2003/361/EG der Kommission von der Anwendung auszuschließen.

Artikel 21: Cybersicherheitszertifizierung

Abs. 2: Eine Pflicht zur Nutzung eines europäischen Systems zur Cybersicherheitszertifizierung sollte nur dann greifen, wenn es keine geeigneten nationalen Zertifizierungsschemata und Branchenstandards gibt. Die Kommission sollte zu Durchführungsrechtsakten und nicht zu delegierten Rechtsakten ermächtigt werden, um eine bessere Abstimmung mit existierenden nationalen Standards zu gewährleisten. Zudem muss der Anwendungsbereich bei der Zertifizierung von Komponenten klar definiert und beschränkt werden.

I. Einschränkung des Gestaltungsspielraums bei der nationalen Umsetzung

Die Wahl des Instruments einer Richtlinie ist zu begrüßen, da es den EU-Mitgliedsstaaten Gestaltungsspielraum bei der Umsetzung bietet, um nationalen Gegebenheiten Rechnung zu tragen. **Allerdings muss in diesem Zusammenhang angemerkt werden, dass aus Sicht der kommunalen Unternehmen und Kommunen der Gestaltungsspielraum für die nationalen Gesetzgeber im vorliegenden Entwurf zu stark eingeschränkt ist.** Dies ist insbesondere mit Blick auf die sektorale und vertikale Ausweitung des Anwendungsbereichs des Richtlinienentwurfs problematisch, da eine große Zahl an Einrichtungen pauschal in den Anwendungsbereich der Richtlinie aufgenommen wird. Dabei wird nicht unterschieden, welche Tätigkeiten oder Anlagentypen mit Blick auf das Ausfallrisiko als wichtig oder wesentlich im Sinne der Richtlinie einzustufen sind. Dies könnte der Abstimmung der NIS 2 mit bestehenden nationalen Regeln im Bereich Cybersicherheit bei der Umsetzung im Weg stehen. Die Möglichkeit zur Abstimmung mit nationaler Gesetzgebung ist auch dahingehend wichtig, dass der Anpassungsbedarf möglichst geringgehalten und eine Duplikation von

Verpflichtungen für Einrichtungen minimiert werden sollte. Im Folgenden wird auf einzelne Bestimmungen des Richtlinienentwurfs im Detail eingegangen:

II. Sektor-übergreifender Maßnahmenkatalog - Art. 18

Aus kommunalwirtschaftlicher und kommunaler Perspektive ist die Ausweitung des Anwendungsbereichs der NIS 2 ein zentraler Aspekt des Vorschlags der Kommission. Die vorgesehene Ausweitung des Anwendungsbereichs auf alle Unternehmen mit mehr als 50 Mitarbeitern und einem Jahresumsatz oder einer Bilanzsumme von über 10 Millionen Euro würde insbesondere im Bereich der Daseinsvorsorge den Großteil der Unternehmen unter den Anwendungsbereich der Richtlinie bringen. **Um sinnvolle und zweckmäßige Sicherheitsstandards zu schaffen, sollte eine Abwägung zwischen der resultierenden Mehrbelastung und dem sektoral sinnvollen Sicherheitsniveau getroffen werden können. Hierzu empfehlen wir den EU-Mitgliedsstaaten die Möglichkeit zur sektoralen Differenzierung der verpflichtenden Sicherheitsmaßnahmen aus Art. 18 Abs. 2 einzuräumen.** Nicht alle Sektoren sind im gleichen Maße für die Ver-/Entsorgungssicherheit oder die Bereitstellung von gesellschaftlich kritischen Diensten relevant, womit eine Differenzierung der Sicherheitspflichten angezeigt wäre.

Ein Beispiel: Als wichtige Einrichtung gemäß Annex II und damit der Richtlinie unterfallend wird u.a. definiert: Unternehmen der Abfallbewirtschaftung im Sinne des Artikels 3 Nummer 9 der Richtlinie 2008/98/EG29. “Abfallbewirtschaftung“ umfasst nach der referenzierten Richtlinie die Sammlung, den Transport, die Verwertung (einschließlich der Sortierung) und die Beseitigung von Abfällen, einschließlich der Überwachung dieser Verfahren sowie der Nachsorge von Beseitigungsanlagen und einschließlich der Handlungen, die von Händlern oder Maklern vorgenommen werden. Damit wären jegliche Tätigkeiten der Abfallwirtschaft von der Richtlinie umfasst, ohne dass die Frage gestellt wird, ob bei einem Cyberangriff die grundlegende Dienstleistung nicht durch analoge Techniken einfach aufrechterhalten werden kann – etwa beim Ausfall eines Tourenplanungstools, das dann durch manuelle Eingaben ersetzt werden kann. **Dieses Beispiel macht deutlich, dass der derzeitige Ansatz der Richtlinie nicht im erforderlichen Maße auf ihre Ziele fokussiert ist und dass den Mitgliedstaaten die Möglichkeit zur sektoralen Differenzierung eingeräumt werden sollte.**

III. Ermächtigung der Kommission zur Erweiterung des Maßnahmenkatalogs - Art. 18 Abs. 6

Art. 18 Abs. 6 ermächtigt die Kommission zum Erlass delegierter Rechtsakte zur Erweiterung des Maßnahmenkatalogs aus Art. 18 Abs. 2, um „Cyberbedrohungen, technologischen Entwicklungen oder sektorspezifischen Besonderheiten Rechnung zu tragen“. Aus Sicht der kommunalen Spitzenverbände und des VKU ist die nachträgliche Erweiterung des Maßnahmenkatalogs durch nachgelagerte Rechtsakte eine sinnvolle Reglung, um der sich dynamisch veränderten Bedrohungslandschaft Rechnung zu tragen. Gleichwohl sollte die Passgenauigkeit der europäischen Reglungen mit nationalen Sicherheitsstandards gewährleistet werden. Hier erachten wir eine Einbindung der Mitgliedsstaaten in die Erweiterung des Maßnahmenkatalogs aus Art. 18 Abs. 2 als erforderlich. **Um dies zu gewährleisten, sollte die Kommission in Art. 18 Abs. 6 zu Durchführungsrechtsakten und nicht zu delegierten Rechtsakten ermächtigt werden.**

IV. Sicherheit der Lieferkette und EU-weit koordinierte Risikobewertungen kritischer Lieferketten – Art. 18 Abs. 2 Buchst. d, Abs. 3 und Art. 19

Als Teil der verpflichtenden Risikomanagementmaßnahmen sollen Einrichtungen die „Sicherheit der Lieferkette“ gewährleisten. **Aus Sicht der Unterzeichner kann dies mit erheblichem Erfüllungsaufwand verbunden sein, was insbesondere für kleine Einrichtungen verfügbare Kapazitäten übersteigen kann und mit unverhältnismäßigem Aufwand verbunden wäre.** Die hier vorgesehene Regelung würden die Verantwortung für die Sicherheit den Einrichtungen auflasten. **In diesem Zusammenhang scheint eine faire Verteilung der Haftung zwischen Betreiber und Zulieferer ein gangbarer Weg**, damit die Verantwortung nicht einseitig bei den Betreibern liegt. Die getroffenen Regeln sollten Rechtssicherheit und klare Verantwortlichkeiten gewährleisten. **Bei kritischen Komponenten wäre Unterstützung und Risikobewertung durch einschlägige nationale Behörden empfehlenswert, um der Komplexität der Materie und dem Stellenwert der Sicherheit Rechnung zu tragen.**
In Artikel 19 wird eine EU-weit koordinierte Risikobewertung kritischer Lieferketten angedacht. Es ist unklar, welche Konsequenzen an diese Risikobewertung geknüpft würden: Dürfen die Dienstleistungen oder Produkte von bestimmten Anbietern nach einer negativ ausfallenden Risikobewertung nicht mehr eingesetzt werden. Was bedeutet dies mit Blick auf Bestandsschutz für existierende Anlagen? Wird es eine Phasing-out-Frist geben? **Es sollte in der Richtlinie klar geregelt werden, ob und welche Konsequenzen mit diesen Risikobewertungen verbunden sind. Zudem empfehlen die kommunalen Spitzenverbände und der VKU die Festlegung eines Bestandsschutzes oder von festen Phasing-out-Fristen erwogen werden.**

V. Keine Anwendung der KMU-Definition zur Bestimmung des Anwendungsbereichs - Empfehlung 2003/361/EG der Kommission (EU-KMU-Definition) - Art. 2 Abs. 1

Zur Ermittlung des Anwendungsbereichs über Schwellenwerte in Art. 2 Abs. 1 verweist der Richtlinienvorschlag auf die Empfehlung 2003/361/EG der Kommission (EU-KMU-Definition). In der Folge würden viele Unternehmen der Ver- und Entsorgungswirtschaft in den Bereichen Wasser, Energie und Abfall unabhängig von ihrer Größe in den Anwendungsbereich der NIS 2 aufgenommen werden, da sie mehrheitlich in öffentlicher Hand sind. Dies ergibt sich aufgrund des Artikel 3 Absatz 4 des Anhangs der Empfehlung 2003/361/EG, wonach ein öffentliches Unternehmen kein KMU ist, wenn „25 % oder mehr seines Kapitals oder seiner Stimmrechte direkt oder indirekt von einem oder mehreren öffentlichen Stellen oder Körperschaften des öffentlichen Rechts“ kontrolliert werden.

Eine Bestimmung der Schwellenwerte anhand der KMU-Definiton würde der Logik größenbasierter Schwellenwerte und dem Verhältnismäßigkeitsprinzip widersprechen. Zudem steht das Gefahrenpotenzial eines Ausfalls nicht mit der Eigentumsstruktur im Zusammenhang. Zur Lösung der Problematik sollte deshalb der Verweis auf die Empfehlung 2003/361/EG der Kommission den Art. 3 Abs. 4 des Anhangs von der Anwendung ausschließen, damit die größenabhängige Ausnahme aus dem Anwendungsbereich auch für kommunale Unternehmen einschlägig ist.

VI. Cybersicherheitszertifizierung - Art. 21 Abs. 2

In Art. 21 Abs. 2 würde die Kommission zum Erlass delegierter Rechtsakte ermächtigt, um die Verwendung eines europäischen Systems für die Cybersicherheitszertifizierung für Kategorien

wesentlicher Einrichtungen verpflichtend zu machen. Aus Sicht der Unterzeichner ist ein europäischer Mindeststandard bei der Zertifizierung prinzipiell zu begrüßen, wenn eine Pflicht zur Mehrfachzertifizierung vermieden wird. **Daher empfiehlt es sich, dass eine Pflicht zur Nutzung eines europäischen Systems gemäß dem Prinzip der Subsidiarität nur dann greift, wenn es keine geeigneten nationalen Zertifizierungsschemata und Branchenstandards gibt.** Zudem sollte auch hier die Kommission zu einem Durchführungsrechtsakt und keinem delegierten Rechtsakt ermächtigt werden, um die Einbindung der Mitgliedsstaaten und so die Harmonisierung der Bestimmungen zu gewährleisten. **In diesem Zusammenhang sollte der Anwendungsbereich bei der Zertifizierung von Komponenten klar definiert und beschränkt werden, um eine sachgerechte Zertifizierungspflicht zu gewährleisten.**

Mit freundlichen Grüßen

Detlef Raphael
Beigeordneter
des Deutschen Städtetages

Dr. Kay Ruge
Stellvertreter des Hauptgeschäftsführers
des Deutschen Landkreistages

Timm Fuchs
Beigeordneter
des Deutschen Städte- und Gemeindebundes

RA Dr. Andreas Zuber
Geschäftsführer
Abteilung Recht, Finanzen und Steuern
Verband kommunaler Unternehmen e.V