VERBAND KOMMUNALER UNTERNEHMEN e.V.

STELLUNGNAHME

zum Gesetzesentwurf der Bundesregierung - Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungsgesetz)

Berlin, 21.08.2025

Der Verband kommunaler Unternehmen e. V. (VKU) vertritt 1.592 Stadtwerke und kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Mit rund 309.000 Beschäftigten wurden 2022 Umsatzerlöse von 194 Milliarden Euro erwirtschaftet und mehr als 17 Milliarden Euro investiert. Im Endkundensegment haben die VKU-Mitgliedsunternehmen signifikante Marktanteile in zentralen Ver- und Entsorgungsbereichen: Strom 66 Prozent, Gas 65 Prozent, Wärme 91 Prozent, Trinkwasser 88 Prozent, Abwasser 40 Prozent. Die kommunale Abfallwirtschaft entsorgt jeden Tag 31.500 Tonnen Abfall und hat seit 1990 rund 78 Prozent ihrer CO2-Emissionen eingespart – damit ist sie der Hidden Champion des Klimaschutzes. Immer mehr Mitgliedsunternehmen engagieren sich im Breitbandausbau: 220 Unternehmen investieren pro Jahr über 912 Millionen Euro. Künftig wollen 90 Prozent der kommunalen Unternehmen den Mobilfunkunternehmen Anschlüsse für Antennen an ihr Glasfasernetz anbieten.
Zahlen Daten Fakten 2024
Wir halten Deutschland am Laufen – denn nichts geschieht, wenn es nicht vor Ort passiert: Unser Beitrag für heute und morgen: #Daseinsvorsorge. Unsere Positionen: https://www.vku.de/vku-positionen/

Verband kommunaler Unternehmen e.V. · Invalidenstraße 91 · 10115 Berlin
Fon +49 30 58580-0 · info@vku.de · www.vku.de

DIE KOMMUNALEN UNTERNEHMEN

Der VKU nimmt im Folgenden zu dem Gesetzesentwurf der Bundesregierung „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (im Folgenden NIS-2-Umsetzungsgesetz) Stellung.

Allgemeines

Das NIS-2-Umsetzungsgesetz soll die IT-Sicherheitsverpflichtungen für Unternehmen, die in den vom Gesetz betroffenen Sektoren – darunter die für die kommunalen Unternehmen relevanten Bereiche Energieversorgung, Wasserversorgung, Abwasserentsorgung, Siedlungsabfallentsorgung und Telekommunikation – tätig sind, regeln. Voraussetzung soll sein, dass mindestens 50 Mitarbeiter beschäftigt werden oder ein Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro ausgewiesen wird. Das Gesetz wird seit über zwei Jahren diskutiert und hat die Umsetzungsfrist der europäischen NIS-2-Richtlinie bereits deutlich überschritten.

Das NIS-2-Umsetzungsgesetz ist zu einem guten Teil eine Ergänzung zu den bisherigen Regelungen, die ganz überwiegend nur die Betreiber von kritischen Infrastrukturen nach der BSI-Kritisverordnung betroffen haben. Diese sind zur Einhaltung von IT-Sicherheit auf höchstem Niveau verpflichtet.

Der VKU unterstützt im Einklang mit der Philosophie der NIS-2-Richtlinie den Gedanken, dass auch Unternehmen, die nicht als Betreiber kritischer Infrastruktur anzusehen sind, konkreten IT-Sicherheitspflichten unterliegen sollen. Von der neuen Regulierung sind allerdings auch die bisherigen Betreiber der kritischen Infrastrukturen insoweit betroffen, als auch die Bereiche außerhalb ihrer kritischen Anlagen reguliert werden (etwa die allgemeine Verwaltung, Buchhaltung, Werkstätten, etc.).

Allerdings beinhaltet das vorliegende Gesetz Regelungen, die klar als **nicht sicherheitsrelevante Überregulierung/Bürokratisierung** anzusehen sind und die aus Sicht des VKU dringend geändert werden müssen. Andernfalls drohen große Probleme in der Umsetzung des Gesetzes und es besteht die Gefahr, dass das wichtige Thema der IT-Sicherheit durch unverhältnismäßige und unlesbare Vorschriften in Misskredit gebracht wird.

§ 28 BSIG

Der VKU konzentriert sich in der Stellungnahme vor allem auf die als überkomplex eingestuften Regelungen zu **Mehrspartenunternehmen**, d.h. zum Beispiel Wasser- oder abfallwirtschaftliche Unternehmen, die neben der Wasserversorgung bzw. Abfallentsorgung in ihren Anlagen auch Energie erzeugen.

Hintergrund ist, dass es unterschiedliche Standards zur Sicherung der IT-Systeme gibt, je nachdem welcher Branche ein Unternehmen angehört. Energieunternehmen sind nach den Standards im **EnWG**[1] reguliert (**Aufsichtsbehörde Bundesnetzagentur**), Abfall- und Wasserunternehmen nach den Standards des **BSIG**[2] (**Aufsichtsbehörde BSI**). Die Regelungen nach dem EnWG sind hierbei detaillierter und strenger als die Regelungen nach dem BSIG. Ferner wird die Regulierung des EnWG genauer in einem IT-Sicherheitskatalog festgelegt, der verbindlich einzuhalten ist.

Der VKU hat stets darauf hingewiesen, dass eine **Doppelregulierung** von Unternehmen nach zwei Standards mit zwei unterschiedlichen Aufsichtsbehörden, an die zu berichten wäre, **dringend zu vermeiden** ist. Über lange Zeit der politischen Diskussionen zum NIS-2-Umsetzungsgesetz war der sehr praktikable Ansatz im Gespräch, dass Unternehmen, die ihr Haupttätigkeitsfeld im Bereich eines nach BSIG regulierten Sektors haben, und nur in untergeordnetem Maße Energie erzeugen und weitergeben, ausschließlich nach dem BSIG reguliert bleiben sollten.

Der von der Bundesregierung vorgelegte Gesetzesentwurf weicht hiervon völlig ab und leistet einer Doppelregulierung/Bürokratisierung Vorschub. § 28 Abs. 5 BSIG legt fest, dass jedes Mehrspartenunternehmen, **das in nicht vernachlässigbarer** Weise Energie erzeugt (Energieanlage), **nach dem EnWG** unter Aufsicht der Bundesnetzagentur zu regulieren ist. Sofern dieses Unternehmen jedoch weitere kritische Anlagen betreibt oder weitere Tätigkeiten entfaltet, die nach dem BSIG geregelt sind, so sind die Unternehmen in Bezug auf diese Kritische Anlage(n) oder die Tätigkeiten **zusätzlich nach dem BSIG (Aufsicht BSI) reguliert**. Die gesamte Office-IT, die nicht der nach dem BSIG unterfallenden Anlage zuzuordnen ist, wäre wiederum nach dem EnWG zu regulieren.

Das hätte folgendes Ergebnis: Ein Abfallunternehmen, das einen Fuhrpark unterhält, die Abfallsammlung und die Straßenreinigung organisiert, Wertstoffhöfe betreibt und, eine **Müllverbrennungsanlage** hat, die Restmüll verwertet und Energie erzeugt, wäre mit Blick auf ihre allgemeine IT als nach dem EnWG, also insgesamt als Energieunternehmen, reguliert einzustufen mit Berichtspflichten an die Bundesnetzagentur. Das nur, weil das Unternehmen unter anderem eine Müllverbrennungsanlage betreibt, die lediglich als Nebenzweck Energie erzeugt. Die Müllverbrennungsanlage selbst wäre, da sie der Siedlungsabfallentsorgung zuzuweisen ist, zwar nach dem BSIG reguliert. Lediglich der Teil der Anlage, der Energie erzeugt, wäre wiederum nach EnWG reguliert. Hier ist es in der Praxis auch völlig unklar, wo hier innerhalb der Anlage die Grenze zwischen dem abfallbewirtschaftenden und dem energieerzeugenden Teil verläuft.

Ähnliche Probleme ergeben sich in der **Wasserwirtschaft** etwa bei **untergeordneten energiewirtschaftlichen Tätigkeiten bei Klärwerken**.

[1] Energiewirtschaftsgesetz
[2] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik

Eine solche Doppelregulierung schafft aus Sicht des VKU **keinerlei sicherheitsrelevanten Mehrwert**, sondern schafft **große Probleme bei der Umsetzung**, da durch die Anwendung zweier Rechtsregime eine Vielzahl von Abgrenzungsfragen mit Blick auf den Inhalt und Bezug der Sicherheitspflichten, die Form und Routine der Berichtspflichten, der Behördenzuständigkeit u.v.m. entstehen. Dies ist bereits bei der Interpretation des Gesetzesentwurfs deutlich geworden.

Mit dem grundsätzlich sehr wichtigen Thema des IT-Schutzes würde mit dem Gesetzentwurf ein derartig großer Aufwand geschaffen, dass dem Anliegen des IT-Schutzes nicht mehr gedient wäre und der auch konträr ist zu den Bekundungen nach schlanker Bürokratie.

Der VKU plädiert damit für eine Regelung, die eine **Doppelregulierung vermeidet** und insb. bei Anlagen, die lediglich als Nebenzweck die Erzeugung von Energie haben, wie etwa bei Müllverbrennungsanlagen, Bioabfallvergärungsanlagen, Klärwerken mit PV-Anlagen u.a., eine Regulierung nach dem EnWG entfällt und diese Anlagen und Unternehmen ausschließlich nach dem BSIG reguliert werden. Dies hätte auch den Vorteil, dass die für IT-Schutz originär geschaffene Fachbehörde, nämlich das BSI, für diese Unternehmen inklusive der Office-IT zuständig bleibt. Zudem wäre die Bundesnetzagentur sicherlich personell überfordert, mit der Beaufsichtigung hunderter (wenn nicht tausender) zusätzlicher Unternehmen.

Die Ausnahme für lediglich „vernachlässigbaren" Geschäftsbereichen durch § 28 Abs. 3, Abs. 5 S. 4 BSIG ist dagegen zusammen mit der Gesetzesbegründung (die u.a. auf den Satzungszweck abstellt) zu eng formuliert und würde die oben beschriebenen Energieanlagen der Mehrspartenunternehmen nicht von der Regulierung nach dem EnWG ausnehmen. § 28 Abs. 5 S. 4 wäre damit wie folgt zu ändern:

> „Im Fall, dass der Betrieb einer Energieanlage nach Satz 1 Nummer 2 einer in Satz 1 aufgeführten besonders wichtigen und wichtigen Einrichtung im Hinblick auf die gesamte Geschäftstätigkeit dieser Einrichtung **eine Nebentätigkeit darstellt** ~~**ver-nachlässigbar ist**~~, findet Absatz 5 keine Anwendung."

Als Begründung kann Folgendes angeführt werden:

> „Mit Satz 4 wird klargestellt, dass im Fall, dass der Betrieb einer Energieanlage als Geschäftstätigkeit nach Satz 1 Nummer 2 im Hinblick auf die gesamte Geschäftstätigkeit eine Nebentätigkeit darstellt, eine Regulierung nach dem EnWG entfällt und weiterhin das BSIG anwendbar bleibt. Eine Nebentätigkeit ist dabei weiter zu verstehen, als eine vernachlässigbare Geschäftstätigkeit nach § 28 Abs. 3. Beispielhaft dafür sind dafür im Regelfall die Energieanlagen der thermische Abfallbehandlungsanlagen und Biovergärungsanlagen. Auch Klärwerke mit kleinen, aber nicht vernachlässigbaren PV-Anlagen würden darunterfallen."

§ 30 BSIG

Die Überbürokratisierung betrifft in ganz ähnlicher Form auch Konzerne, die eine Service-Gesellschaft für zentrale Services (Buchhaltung, rechtliche Dienstleistungen, Personalwirtschaft, IT, etc.) gegründet haben. Dies ist in der Praxis bei Konzernen wahrscheinlich der Standardfall. Wird in dieser Service-Gesellschaft auch der zentrale IT-Betrieb des Konzerns übernommen, so würde es sich um einen „Managed Service Provider" (§ 2 Nr. 26 BSIG) oder um einen „Managed Security Service Provider" (§ 2 Nr. 25 BSIG) handeln, für den auf Grund des Verweises in § 30 Abs. 3 BSIG die besonders strengen Regeln der Durchführungsverordnung (EU) 2024/2690[3] gelten. Diese strengen Regeln würde für die gesamte Service-Gesellschaft gelten, auch wenn der zentrale IT-Betrieb nur einen kleinen Anteil ausmacht (also eher eine Nebentätigkeit ist), aber nicht „vernachlässigbar" ist.

§ 30 Abs. 3 wäre damit wie folgt zu ändern:

> (3) Der von der Europäischen Kommission gemäß Artikel 21 Absatz 5 Unterabsatz 1 der NIS-2-Richtlinie erlassene Durchführungsrechtsakt zur Festlegung der technischen und methodischen Anforderungen an die in Absatz 1 genannten Maßnahmen in Bezug auf […] Managed Service Provider, Managed Security Service Provider, […] hat für die vorgenannten Einrichtungsarten Vorrang. **Dies gilt nicht für Managed Service Provider und Managed Security Service Provider, wenn diese Tätigkeit im Hinblick auf die gesamte Geschäftstätigkeit dieser Einrichtung eine Nebentätigkeit darstellt.**

Auch hier geht es, wie bei den Ausführungen zu § 28 BSIG, nicht darum einer Regulierung vollkommen zu entgehen. Es geht darum einer angemessenen Regulierung zu unterliegen, was in diesem Fall die einfache Regulierung nach dem BSIG ist.

§ 5c EnWG

Die **Gefahr der Überbürokratisierung betrifft auch die Regelungen des EnWG an sich** und zwar unabhängig von der zu § 28 BSIG ausgeführten Problematik. Die dort festgelegten Regelungen werden in noch zu erlassenden IT-Sicherheitskatalogen deutlich detaillierter verbindlich festgelegt (5c Abs. 2 – 4 EnWG). Wie genau die Regeln der IT-

[3] Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt.

Sicherheitskataloge aussehen werden, ist unbekannt, was ein Problem bei der Beurteilung des Gesetzes darstellt, da nicht alle Auswirkungen bekannt sind.

Damit hier Klarheit herrscht und eine mögliche Überbürokratisierung über die IT-Sicherheitskataloge verhindert wird, muss es **klare gesetzliche Vorgaben** geben. Grundlegende Entscheidungen dürfen nicht auf die behördliche Ebene verschoben werden. Dies betrifft insbesondere die sogenannte dreistufige Abstufung innerhalb der Pflichten der Unternehmen.

Im Bereich des BSIG ist klar festgelegt, dass alle drei Stufen der von der NIS2-Regulierung betroffenen Unternehmen (Betreiber kritischer Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen) unterschiedlich und damit risikoangemessen reguliert werden. Auch **im EnWG muss klar geregelt werden**, dass dieser **dreistufige Ansatz auch in den IT-Sicherheitskatalogen nachvollzogen** wird. Bisher gibt es dazu im Gesetz und in der Gesetzesbegründung lediglich Andeutungen in diese Richtung, die allerdings nicht eindeutig genug sind.

§ 5c Abs. 3 S. 3 EnWG wäre damit wie folgt zu ändern:

> „[…] Zur Wahrung der Angemessenheit der Anforderungen des jeweiligen IT-Sicherheitskatalogs sind bei der Erstellung folgende Faktoren zu berücksichtigen:
>
> 1. Ausmaß der Risikoexposition,
>
> 2. die Größe des Betreibers,
>
> 3. **die Eigenschaft als eine wichtige Einrichtung, eine besonders wichtige Einrichtung oder als Betreiber einer kritischen Anlage,**
>
> […]“

VERBAND KOMMUNALER UNTERNEHMEN e.V.

Bei Rückfragen oder Anmerkungen steht Ihnen zur Verfügung:

Wolf Buchholz
Senior-Fachgebietsleiter Kritische Infrastruktur und Cybersicherheit
Abteilung Recht, Finanzen und Steuern

Telefon: +49 30 58580-317
E-Mail: buchholz@vku.de