DIE KOMMUNALEN UNTERNEHMEN

VERBAND KOMMUNALER UNTERNEHMEN e.V.

Positionspapier

zur Überarbeitung des EU-Rechtsakts zur Cybersicherheit

Sondierung der EU-Kommission

Kernforderungen der Kommunalwirtschaft:

- Bürokratie abbauen;
- Security-by-Design als Grundelement sicherstellen;
- Gänzliche Sicherheit in der IKT-Lieferkette verankern.

Die Sicherheitslandschaft Europas hat sich seit Inkrafttreten des EU-Rechtsakts zur Cybersicherheit (Cybersecurity Act, CSA) 2019 spürbar verändert. Deswegen ist es richtig und wichtig, dass der CSA überarbeitet wird. Als Betreiber kritischer Infrastrukturen ist Cybersicherheit für kommunale Unternehmen ein besonders hohes Gut. Sie sind resilient, lokal und sicher. Vor allem in Krisensituationen tragen sie eine besondere Verantwortung für die Daseinsvorsorge vor Ort.

Aus Sicht des Verbandes kommunaler Unternehmen (VKU) sollten dementsprechend folgende Kernforderungen im weiteren Gesetzgebungsprozess berücksichtigt werden:

1. Konkret Bürokratie abbauen und Cybersicherheitsvorgaben vereinfachen

Der VKU begrüßt das Ziel der Kommission, die Wettbewerbsfähigkeit Europas durch gezielten Bürokratieabbau anzukurbeln. Die Kommission sollte das Regelwerk im Bereich Digitalisierung vereinfachen, ohne zu deregulieren. Kritische Infrastrukturen müssen sicher und geschützt sein. Gleichzeitig belasten auch kommunale Unternehmen erhebliche Dokumentations-, Berichts- und Transparenzpflichten. Das ist eine besonders große Herausforderung angesichts fehlender personeller Ressourcen. Diese Anstrengungen und Ressourcen werden in anderen Arbeitsbereichen dringend benötigt, wenn es darum geht, die Sicherheit kritischer Infrastrukturen zu gewährleisten. Deswegen ist wichtig, dass Vorhaben, die darauf abzielen Bürokratie abzubauen, zügig umgesetzt werden, um Unternehmen für das kommende Jahr Rechts- und Planungssicherheit zu geben. Anknüpfend daran sollte die Kommission berücksichtigen, dass Gesetze in diesem Bereich flexibilisiert werden sollten, um dem technischen Fortschritt und die damit einhergehenden neuen Bedrohungen der Cybersicherheit „schlank“ und schnell berücksichtigen zu können.

Die Überarbeitung des CSA bietet eine Gelegenheit, komplexe Vorschriften zu vereinfachen. Seit 2019 ist das EU-Cybersicherheitsregelwerk deutlich komplexer geworden. Kommunale Unternehmen unterliegen in diesem Bereich einer Vielzahl von Anforderungen, die sich kaum überblicken lassen. Exemplarisch lassen sich folgende EU-Rechtsakte anführen:

- **NIS-2-Richtlinie;**
- **Cyberresilienzgesetz** (Cyber Resilience Act, CRA);
- **Richtlinie über die Resilienz kritischer Einrichtungen** (Critical Entities Resilience Directive, CER-Richtlinie);
- **Netzkodex zur Cybersicherheit** (Network Code on Cybersecurity, NCCS).

Essenziell ist, dass diese mittlerweile zahlreichen Vorgaben zur Cybersicherheit kompatibel sind. Insbesondere bzgl. Berichtspflichten und Cybersicherheitsrisikomanagement besteht Handlungsbedarf. Redundanz oder Widersprüche in europäischen Vorgaben sollten gezielt vermieden werden.

Diese Vielzahl an komplexen und aufwendigen Vorgaben, die sich teilweise überschneiden, führen derzeit zu einem erheblichen Aufwand bei der Umsetzung komplexer und aufwändiger Pflichten. Außerdem stellt der Nachweis der Umsetzung dieser Maßnahmen, gemäß den ebenso komplexen Compliance-Vorgaben, eine hohe Belastung für kommunale Unternehmen dar. Die EU-Kommission sollte zeitnah nach Veröffentlichung des Rechtsakts Leitlinien zur Verfügung stellen, die Klarheit für die Umsetzung bieten. Darüber hinaus kommt es für kommunale Unternehmen darauf an, dass die Meldepflichten im Bereich Cybersicherheit vereinfacht und vor allem verschlankt werden.

Außerdem mangelt es auf nationaler Ebene an digitalen Lösungen, wenn es darum geht, Informationen effizient an die zuständigen Behörden zu übermitteln. Hier könnte die EU-Ebene über die Einführung einfacher Formulare, für zentrale Informationspunkte als „One-Stop-Shop“, unterstützen bieten.

2. Security-by-Design als Grundelement sicherstellen

Sicherheitslücken können ein erhebliches Risiko für die Energie- und Wasserversorgung sowie für die Abwasser- und Abfallentsorgung bergen. Dabei sind kommunale Unternehmen auf sichere IKT-Produkte angewiesen. Deswegen sollten Hersteller von Hard- und Software bereits bei der Entwicklung ihrer Produkte steigende Sicherheitsanforderungen so weit wie möglich berücksichtigen. Im Falle einer Regulierung der Sicherheit digitaler Produkte sollte der CSA hier die Vorgaben des CRA lediglich flankieren.

Wichtig ist allerdings, dass Security-by-Design nicht zu einem Engpass in einem bereits sehr schwierigen Beschaffungsprozess wird oder zu erheblichen Preissteigerungen führt. Mögliche Anforderungen sollten nicht so ausgestaltet sein, dass am Ende nur sehr wenige Anbieter weltweit in der Lage sind, diese zu erfüllen. Die Kommission sollte deswegen Sicherheitsanforderungen an Hersteller in jeglichen zukünftigen industriepolitischen Überlegungen, zur technologischen Souveränität Europas an erster Stelle platzieren.

3. Sicherheit der IKT-Lieferkette gänzlich betrachten

Der Fokus der Überarbeitung des CSA auf die Bewältigung von Sicherheitsherausforderungen in der IKT-Lieferkette ist richtig und wichtig. Das Risiko von Cybersicherheitsvorfällen, die von IKT-Lieferketten, von Unternehmen in kritischen Sektoren ausgehen, ist in den vergangenen fünf Jahren deutlich gestiegen (z. B. durch Ransomware, Social Engineering oder Lieferkettenangriffe). Weder der aktuelle CSA noch der europäische Cybersicherheitszertifizierungsrahmen adressieren diese Risiken ausreichend. Rein technische Maßnahmen (z. B. On-Device-Verarbeitung, Verschlüsselung) bieten keinen ausreichenden Schutz vor diesen Bedrohungen. Deswegen ist es wichtig, dass die Überarbeitung eine sichere Lieferkette in den Blick nimmt. Einheitliche Zertifizierungsschemata für Produktzertifizierungen und vertrauenswürdige Lieferkettennachweise von Herstellern und Lieferanten wären diesbezüglich begrüßenswert.

Ihre Ansprechpartnerin im VKU

Anna Sophie Kirchmayr
Referentin mit Schwerpunkt Digitalisierung und Nachhaltigkeitsberichterstattung
Telefon: +32 2 740 16 55
E-Mail: kirchmayr@vku.de