VERBAND KOMMUNALER UNTERNEHMEN e.V.

STELLUNGNAHME

zu den Eckpunkten für die Cyber-Sicherheitsstrategie 2021 vom 24.03.2021

Berlin, 14.04.2021

Verband kommunaler Unternehmen e.V. · Invalidenstraße 91 · 10115 Berlin
Fon +49 30 58580-0 · Fax +49 30 58580-100 · info@vku.de · www.vku.de

DIE KOMMUNALEN UNTERNEHMEN

Der Verband kommunaler Unternehmen (VKU) bedankt sich für die Möglichkeit, zu den „Eckpunkten für die Cyber-Sicherheitsstrategie 2021“ Stellung zu nehmen.

Bedeutung des Vorhabens für kommunale Unternehmen

Der VKU vertritt rund 1.500 kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Als Betreiber von Kritischen Infrastrukturen sind sie für Deutschland von überragender Bedeutung. Insbesondere ohne die jederzeitige Strom- und Wasserversorgung sowie die sichere Entsorgung von Abwasser und Abfall würde das wirtschaftliche und gesellschaftliche Leben innerhalb kürzester Zeit zusammenbrechen. Darüber hinaus treiben immer mehr kommunale Unternehmen den Ausbau von Glasfaser- und Breitbandnetzen vor Ort voran und schaffen so die digitale Infrastruktur.

Auch die kommunalen Unternehmen nutzen die Digitalisierung/Möglichkeiten digitaler Transformation, um ihre Leistungen jederzeit erbringen zu können. Hierbei werden immer mehr Anlagen und Maschinen digital vernetzt. Damit steigt zugleich das Risiko: Je mehr Anlagen und Maschinen digital vernetzt sind, desto mehr Angriffspunkte entstehen, desto vulnerabler wird das Gesamtsystem. Die kommunalen Unternehmen arbeiten bei der IT-Sicherheit täglich daran, technologisch gut aufgestellt zu sein, doch kein IT-System ist „unhackbar“.

Sicherheit ist kein Zustand, sondern ein Prozess. Der VKU begrüßt deshalb das Anliegen der Bundesregierung, die Cyber-Sicherheitsstrategie (CSS) 2016 zu überarbeiten und mit den zur Diskussion gestellten Eckpunkten eine Grundlage für die CSS 2021 zu legen. Teilweise sollten die Eckpunkte jedoch nachgeschärft werden.

Positionen des VKU in Kürze

Aus Sicht des VKU sollten die Eckpunkte insbesondere an folgenden Stellen nachgeschärft werden:

- IT-Sicherheit ist mit hohen Kosten verbunden, deren Refinanzierung in den Eckpunkten berücksichtigt werden muss.
- Hersteller von IT-Produkten sollten verstärkt in die Pflicht genommen werden, sichere IT-Produkte zu liefern.
- Das BSI muss alle ihr bekannten Sicherheitslücken unverzüglich in Unternehmen an diese melden. Nur so kann eine vertrauenswürdige Zusammenarbeit von Staat und Wirtschaft gefördert werden.
- Es sollte ein nationales Cyberabwehrzentrum etabliert werden. Vorbild kann das Nationale Lage- und Führungszentrum für Sicherheit im Luftraum sein.

Stellungnahme

Zu Nr. 3.1 (Handlungsfeld 1 – Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung)

Die Eckpunkte definieren zunächst das Ziel, insbesondere die Informations- und Unterstützungsangebote für KMU zu allen Fragen der Informations- und Cyber-Sicherheit für diese Zielgruppe spezifischer auszugestalten und weiter auszubauen (siehe hierzu auch die entsprechende Passage in Handlungsfeld 2). Dieses Ziel begrüßt der VKU ausdrücklich.

Ergänzt werden sollte dieser Ansatz durch eine Unterstützung in der Fachkräftegewinnung und -ausbildung. Qualifizierte Fachkräfte im Bereich der IT-Sicherheit sind rar und gerade für KMU nicht leicht zu gewinnen. Dies stellt die KMU vor große Herausforderungen.

Zudem muss betont werden, dass es IT-Sicherheit nicht zum Nulltarif gibt. Von Audits durch externe Sachverständige, über die Anschaffung von Hardware, bis zur Sensibilisierung ihrer Mitarbeiter: Alle diese Maßnahmen sind mit hohen Kosten verbunden und müssen refinanziert werden. Auch dieser Punkt muss in die Eckpunkte Eingang finden.

Zu Nr. 3.1 (Handlungsfeld 1 – Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung)

Nach dem Entwurf der Eckpunkte soll insbesondere die Sicherheit von Schlüssel- und Zukunftstechnologien i. S. e. „Security by Design“-Ansatzes von vornherein mitgedacht und gestärkt werden. Dies begrüßt der VKU nachdrücklich.

Sicherheitslücken in der Hard- und Software sind auch für kommunale Unternehmen und insbesondere in der Energie- und Trinkwasserversorgung sowie in der Abwasserentsorgung ein erhebliches Risiko. Hersteller von Soft- und Hardware müssen hier deutlich mehr Verantwortung für ihre Produkte übernehmen. Das bedeutet: Sie müssen die gestiegenen Sicherheitsanforderungen bereits in der Entwicklung berücksichtigen und aufgedeckte Sicherheitslücken in ihren Produkten unverzüglich melden und beheben. Insofern ist es kritisch zu beurteilen, dass im Regierungsentwurf zum „Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“ („IT-SiG 2.0-RegE“) die Herstellerpflichten nicht stärker betont werden.

Zu Nr. 3.2 (Handlungsfeld 2 – Gemeinsamer Auftrag von Staat und Wirtschaft)

In Handlungsfeld 2 wird der gemeinsame Auftrag von Staat und Wirtschaft betont. In der CSS 2021 sollen der vertrauensvolle Austausch, das zeitnahe Schließen von Sicherheitslücken und die Abwehr von Cyber-Angriffen als unverzichtbare Bausteine des gemeinsamen Auftrags von Staat und Wirtschaft zur Erhöhung der Cyber-Sicherheit Deutschlands adressiert werden. Es soll hierbei die Interaktion der Unternehmen mit den zuständigen Stellen in den Teilbereichen Prävention, Detektion und Reaktion der Cyber-Sicherheit weiter verstärkt werden – auch, damit Unternehmen mehr zur Detektion und Aufklärung von Cyber-Sicherheitsbedrohungen beitragen können. Dieses Ziel teilt der VKU.

Allerdings wird dieses Ziel durch das IT-SiG 2.0-RegE in Frage gestellt. So erlaubt § 7b IT-SiG 2.0-RegE dem BSI insbesondere die Detektion von Sicherheitslücken in den IT-Systemen von Kritis-Unternehmen durch Portscans. Dabei muss das BSI diese Sicherheitslücken nicht in jedem Fall den Unternehmen mitteilen. Damit Sicherheitslücken zeitnah geschlossen werden ist es jedoch notwendig, dass das BSI den Unternehmen die ihm bekannten Sicherheitslücken unverzüglich mitteilt.

Zu Nr. 3.2 (Handlungsfeld 2 – Gemeinsamer Auftrag von Staat und Wirtschaft)

Laut Entwurf der Eckpunkte sollen zum Schutz Kritischer Infrastrukturen bestehende Anforderungen weiter ausgestaltet und die Umsetzung bei den Kritis-Betreibern verstärkt unterstützt werden. Bestehende Mindestanforderungen an Kritis-Betreiber sollen aufgrund der sich verändernden Bedrohungslage stetig überprüft und bei Bedarf angepasst werden. Der sich somit verändernde Stand der Technik muss durch die Betreiber erfüllt werden.

Der VKU begrüßt die verstärkte Unterstützung der Kritis-Betreiber. Dies ist insbesondere vor dem Hintergrund der zusätzlichen Anforderungen nach dem IT-SiG 2.0-RegE wichtig. Ergänzend sollte die Fachkräftegewinnung unterstützt und die Refinanzierung der Maßnahmen gesichert werden.

Die Entwicklungen zum Stand der Technik im IT-SiG 2.0-RegE sind dagegen kritisch zu beurteilen. Zukünftig soll das BSI den Stand der Technik einseitig durch technische Richtlinien bestimmen können. Dies lehnt der VKU ab. Der Stand der Technik sollte wie bisher auch durch den Markt bestimmt werden. Dies hat sich bewährt und bietet Flexibilität für zukünftige Entwicklungen unter Marktbedingungen. Die technischen Richtlinien würden sonst im Zweifel bereits im Moment der Veröffentlichung überholt sein.

Zu Nr. 3.2 (Handlungsfeld 2 – Gemeinsamer Auftrag von Staat und Wirtschaft)

Das Ziel einer Vermeidung von Doppelregulierungen auf europäischer Ebene begrüßt und unterstützt der VKU ausdrücklich. Europäische Normen und Standards im Bereich der Cyber-Sicherheit müssen jedoch hinreichend differenziert sein, um ein sachgerechtes Sicherheitsniveau und tragbare Kosten zu gewährleisten. Diese Absicht sollte in der Cyber-Sicherheitsstrategie klar festgehalten und auf EU-Ebene konsequent verfolgt werden.

Zu Nr. 3.3 (Handlungsfeld 3 – Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur)

Der Entwurf der Eckpunkte stellt fest, dass es einer zeitgemäßen Cyber-Sicherheitsarchitektur bedarf, die die verschiedenen Akteure auf Bundesebene wirksam verzahnt und daneben Länder, Kommunen und Wirtschaft im Blick behält. Deshalb soll die Cybersicherheitsarchitektur des Bundes strukturell und prozessual einer Bewertung unterzogen werden. Dies begrüßt der VKU nachdrücklich.

Die existierenden föderalen Strukturen führen zu einem Zuständigkeitsdschungel, der im Ernstfall schnelle Maßnahmen erschwert. Bedrohungslagen müssen jedoch frühzeitig erkannt und Abwehrstrategien entwickelt werden, bevor es zu Angriffen kommt. Es sollte der große Wurf gewagt und ein nationales Cyberabwehrzentrum etabliert werden. Hier sollten die zuständigen Sicherheits- und Aufsichtsbehörden, die IT-Branche und die Unternehmen eng und koordiniert zusammenarbeiten. Denn nur ein frühzeitiger und umfassender Informationsaustausch zwischen allen Akteuren gewährleistet eine maximale Vorbeugung gegen Cyberattacken. Das Nationale Lage- und Führungszentrum für Sicherheit im Luftraum kann hier ein Vorbild sein.

Zu Nr. 3.4 (Handlungsfeld 4 – Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

Laut dem Entwurf der Eckpunkte soll die CSS 2021 die EU-Cyber-Sicherheitsstrategie und die NIS 2-Richtlinie mit aufnehmen und einarbeiten. Dies wird vom VKU begrüßt. Nur in Zusammenschau mit den europäischen Vorgaben macht eine nationale Cybersicherheitsstrategie Sinn.

VERBAND KOMMUNALER UNTERNEHMEN e.V.

Bei Rückfragen oder Anmerkungen stehen Ihnen zur Verfügung:

Andreas Seifert
Stv. Leiter Abteilung Recht, Finanzen und Steuern | Bereichsleiter Recht
Telefon: +49 30 58580-132
E-Mail: seifert@vku.de

Wolf Buchholz
Referent Recht der Digitalisierung
Telefon: +49 30 58580-317
E-Mail: buchholz@vku.de