DIE KOMMUNALEN UNTERNEHMEN

VERBAND KOMMUNALER UNTERNEHMEN e.V.

Cybersicherheit

Sicherheit erhöhen, Strukturen verschlanken

Unsere Ziele:

- Unternehmen bei IT-Sicherheitsmaßnahmen unterstützen.
- Hersteller von IT-Produkten verstärkt in die Pflicht nehmen.
- Nationales Cyberabwehrzentrum schaffen.

Als Betreiber kritischer Infrastrukturen müssen kommunale Unternehmen besonders hohen Anforderungen an die IT-Sicherheit genügen, um eine reibungslose Versorgung sicherzustellen. Sie versorgen Deutschland rund um die Uhr mit Energie, Wärme, Wasser und schnellem Internet und kümmern sich um die Entsorgung von Abwasser und Abfall. Ohne diese zuverlässige Ver- und Entsorgung würde das wirtschaftliche und gesellschaftliche Leben innerhalb kürzester Zeit zusammenbrechen.

Zunehmende digitalisierte Prozesse, dezentrale Anlagen und Vernetzung von Anlagen und Maschinen führen zu mehr Effizienz und Sicherheit in den Abläufen, zugleich steigt aber auch das Risiko: Je mehr Anlagen und Maschinen digital vernetzt sind, desto mehr Angriffspunkte entstehen. Hinzu kommt: IT-Sicherheit kann nie statisch gedacht werden, sondern erfordert dynamisches Know-how, und zeichnet sich durch kurze Innovationszyklen aus. Deshalb arbeiten die kommunalen Unternehmen tagtäglich daran, technologisch in der IT-Sicherheit bestmöglich aufgestellt zu sein. Doch kein IT-System ist „unhackbar“.

Tatsächlich nehmen Cyberattacken auf die Strom-, Wasser- und Internetversorgung weltweit erheblich zu. Das sind Angriffe auf unser infrastrukturelles Herz. Ohne Strom steht das Land still: vom Kühlschrank bis zum Geldautomat, vom (Mobil-)Telefon bis zur Tankstelle. Ohne Wasser gibt es keine Toilettenspülung und kein Händewaschen. Ohne Internet kommt unsere (digitale) Wirtschaft zum Erliegen.

Unternehmen bei IT-Sicherheitsmaßnahmen unterstützen

Die Bundesregierung hat jüngst die „Cybersicherheitsstrategie für Deutschland 2021“ (09/2021) beschlossen. Darin wird festgestellt, dass insbesondere kleine und mittlere Unternehmen (KMU) den Herausforderungen aufgrund von Mängeln an Ressourcen und Wissen nicht ausreichend gewachsen sind. Sie benötigen daher besondere Förderung für einen ausreichenden Schutz vor Cyberangriffen.

KMU sollten deshalb bei ihren IT-Sicherheitsmaßnahmen unterstützt werden.

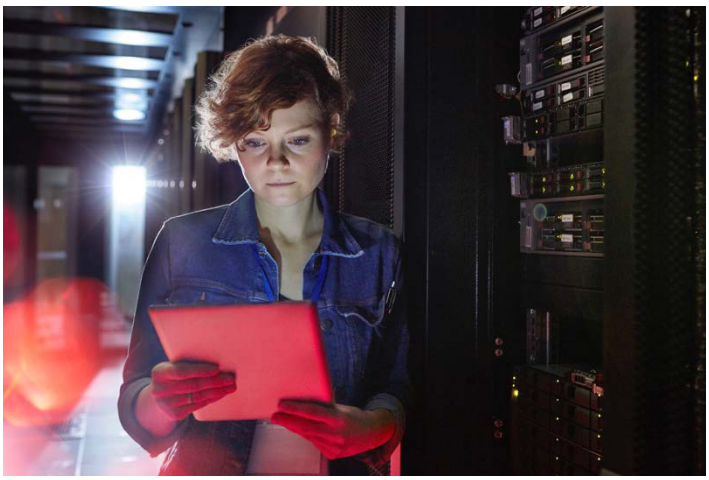
Kommunale Unternehmen halten Deutschland am Laufen

Die kommunalen Unternehmen sorgen maßgeblich dafür, dass in Deutschland der Strom zuverlässig aus der Steckdose und das Wasser aus dem Hahn kommt. Unsere Mitgliedsunternehmen tragen zu 62 Prozent zur Stromversorgung und zu 91 Prozent zur Versorgung mit Wasser in Deutschland bei. Dabei setzen sie zunehmend digitale Anwendungen ein, um ihre Prozesse zu optimieren und Herausforderungen wie dem Klimawandel und der Energiewende zu begegnen. Sie müssen bestmöglich vor Cyberattacken geschützt werden. Nur so kann die hohe Versorgungssicherheit in Deutschland heute und in Zukunft gewährleistet werden.

IT-Sicherheit gibt es nicht zum Nulltarif. Von Audits durch externe Sachverständige über die Anschaffung von Hardware bis zur Sensibilisierung der Mitarbeiter: Alle diese Maßnahmen sind mit hohen Kosten verbunden und müssen refinanziert werden. Die bestehenden Förderprogramme müssen deshalb (finanziell) ausgeweitet und möglichst unbürokratisch gestaltet werden.

Ergänzt werden muss 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, vor allem dann, wenn diese abseits attraktiver Metropolen ansässig sind. Neben attraktiven Angeboten für neue Mitarbeiterinnen und Mitarbeiter geht es für die meisten Unternehmen darum, ihre bestehenden Teams zu qualifizieren.

Hersteller von IT-Produkten verstärkt in die Pflicht nehmen
Nach der Cybersicherheitsstrategie sollte daher insbesondere die Sicherheit von Schlüssel- und Zukunftstechnologien im Sinne eines „Security by Design"-Ansatzes von vornherein mitgedacht und gestärkt werden.



Sicherheitslücken in der Hard- und Software sind auch für kommunale Unternehmen ein erhebliches Risiko, insbesondere in der Energie- und Trinkwasserversorgung sowie in der Abwasserentsorgung. 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 gerade neu geregelten IT-Sicherheitsgesetz 2.0 die Herstellerpflichten nicht stärker betont werden. Hier muss aus Sicht des VKU deutlich nachgebessert werden. Hersteller müssen Verantwortung für ihre Produkte übernehmen.

Nationales Cyberabwehrzentrum schaffen
Die Cybersicherheitsstrategie 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.

In einem nationalen Cyberabwehrzentrum können diese Anforderungen gebündelt, zentrale Maßnahmen geplant und umgesetzt 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.

Ihre Ansprechpartner im VKU

Andreas Seifert
Bereichsleiter Recht
Telefon 030 58580-132
E-Mail: seifert@vku.de

Wolf Buchholz
Referent Recht der Digitalisierung
Telefon: 030 58580-317
E-Mail: buchholz@vku.de

Jonas Wiggers
Referent Grundsatz
Telefon: 030 58580-174
E-Mail: wiggers@vku.de

Bildnachweis: DEEPOL by plainpicture/Agnieszka Olek (S. 2)