DIE KOMMUNALEN UNTERNEHMEN

VKU VERBAND KOMMUNALER UNTERNEHMEN e.V.

CYBER-SICHERHEIT EFFEKTIV GESTALTEN

Sicherheit ist kein Zustand, sondern ein Prozess

- **Ein nationales Lage- und Führungszentrum für Cyber-Sicherheit schaffen**
- **Security-by-design-Ansatz im IT-Sicherheitsgesetz 2.0 festschreiben**
- **Teilhabe der Stadtwerke an der krisenfesten 450 MHz-Frequenz gewährleisten**

Die Stromversorgung ist der Herzschlag der digitalen Gesellschaft. Ohne Strom steht unser Alltag still. Der Schutz einer jederzeit ungestörten, sicheren Stromversorgung durch die deutschen Stadtwerke, insbesondere vor Cyberangriffen aller Art, ist daher eine Aufgabe der nationalen Sicherheit. Sicherheit ist aber kein Zustand, sondern ein Prozess. Deswegen müssen wir unsere Cyber-Sicherheitsarchitektur renovieren.

Ohne Strom nichts los

In unserer zunehmend digitalisierten Welt sind nahezu alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens auf die stets zuverlässige Funktion der notwendigen Informations- und Kommunikationstechnik angewiesen. Deren Ausfall oder Beeinträchtigung kann zu erheblichen Störungen oder im schlimmsten Fall sogar zum völligen Ausfall der wirtschaftlichen und administrativen Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen führen.

Grundlage der ungestörten Funktion der Informations- und Kommunikationstechnik ist eine jederzeit sichere Stromversorgung ihrer Betriebssysteme. Hierfür sorgen die deutschen Stadtwerke und ihre Verteilnetzbetreiber rund um die Uhr.

Sie nutzen die Digitalisierung aber auch für die Energiewende. Damit steigt zugleich das Risiko: Je mehr Anlagen und Maschinen digital vernetzt sind, desto mehr Angriffspunkte entstehen.

Wie alle Unternehmen in Deutschland arbeiten auch die Stadtwerke und ihre Verteilnetzbetreiber bei der IT-Sicherheit täglich daran, technologisch gut aufgestellt zu sein, doch kein IT-System ist „unhackbar“.

Tatsächlich sind Cyberattacken auf das Stromnetz an der Tagesordnung. Das sind Angriffe auf unser infrastrukturelles Herz. Ohne Strom steht das Land still: vom Kühlschrank bis zum Geldautomat, vom (Mobil-)Telefon bis zur Tankstelle.

Bei der Abwehr von Cyber-Angriffen auf das Stromnetz geht es um die nationale Sicherheit – bei jedem, vor Ort! Die Stromversorgung muss Teil der deutschen Cyber-Sicherheitsarchitektur werden.

Angesichts der zunehmenden Skrupellosigkeit der Angreifer stellt sich jedoch die Frage: Ist unsere föderale Sicherheitsarchitektur mit derzeit 23 zuständigen Ministerien und Behörden auf Bundes- und Landesebene die richtige Antwort für die Zukunft?

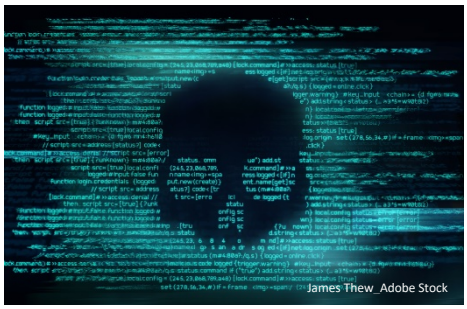
Effektive Cyber-Sicherheit

Wenn die Angreifer schneller und aggressiver werden, müssen wir eine adäquate Verteidigung aufstellen, die flexibel reagiert und antizipiert, wenn sich Angriffstaktiken verändern. Die existierenden föderalen Strukturen führen aber vorab schon zu einem Zuständigkeitsdschungel, der im Ernstfall schnelle Maßnahmen erschwert. Bedrohungslagen müssen jedoch frühzeitig erkannt und Abwehrstrategien entwickelt werden, bevor es zu Angriffen kommt.

Dem ständigen Wettlauf gegen die Zeit sollten wir mit schlanken Strukturen und kurzen Entscheidungswegen begegnen: einem Cyber-Abwehrzentrum auf Bundesebene. Hier müssen alle sicherheitsrelevanten Akteure – von Behörden über die IT-Branche bis zu Energieversorgungsunternehmen – zusammenarbeiten. Dort könnten alle Informationen frühzeitig zusammenlaufen, Angriffe abgewehrt und Gegenmaßnahmen durchgeführt werden. Beim Schutz der nationalen Sicherheit muss schnell und beherzt eingegriffen werden können. Kurzum: Lassen Sie uns mehr Mut zur Zusammenarbeit und Koordination wagen!

Ein nationales Cyberabwehrzentrum, in dem die zuständigen Sicherheits- und Aufsichtsbehörden, die IT-Branche und die Energieversorger eng und koordiniert zusammenarbeiten, wäre eine gute Lösung. Denn nur ein frühzeitiger und umfassender Informationsaustausch zwischen allen Akteuren gewährleistet eine maximale Vorbeugung gegen Cyberattacken und Blackout-Risiken sowie ein konsequentes und wirksames Vorgehen ohne Zeitverzug im Schadensfall.

Das Nationale Lage- und Führungszentrum für Sicherheit im Luftraum zeigt, dass es geht. Nur sollten wir – anders als bei der Luftraumsicherheit – die notwendige Sicherheitsarchitektur aufbauen, bevor es einen gravierenden Vorfall gibt.


James Thew_Adobe Stock

Security-by-design

Sicherheitslücken in der Hard- und Software sind auch für die Energie- und Trinkwasserversorgung sowie Abwasserentsorgung ein erhebliches Risiko.

Die Bundesregierung muss beim geplanten IT-Sicherheitsgesetz 2.0 und seiner praktischen Umsetzung die Voraussetzungen für ein einheitliches IT-Sicherheitskennzeichen schaffen und den security-by-design-Ansatz einführen.

Hersteller von Soft- und Hardware müssen deutlich mehr Verantwortung für ihre Produkte übernehmen. Das bedeutet: Sie müssten die gestiegenen Sicherheitsanforderungen bereits in der Entwicklung berücksichtigen und aufgedeckte Sicherheitslücken in ihren Produkten unverzüglich melden und beheben.

Was die Digitalisierung von den vorangegangenen technologischen Revolutionen unterscheidet, ist ihr Innovationstempo. Neue Technologien, neue Methoden: Die Zyklen werden kürzer. Entsprechend schneller müssen Organisationen reagieren. Das setzt Lern- und Anpassungsfähigkeit voraus. Kurzum: Veränderungsbereitschaft ist entscheidend.

450 MHz-Frequenz

Stromversorger und ihre kritischen Infrastrukturen brauchen eine sichere Lösung, um auch im Notfall schnell und direkt kommunizieren zu können. Das öffentliche Mobilfunknetz ist dafür nicht geeignet: Fällt der Strom aus, funktioniert der Mobilfunk nicht. Das gilt für alle Frequenzen – mit Ausnahme der 450 MHz-Frequenz. Sie ist sicher und ermöglicht Kommunikation, die elementar ist, um Katastrophen oder Schadensereignisse schneller zu bewältigen. Deswegen müssen Stadtwerke und ihre Verteilnetzbetreiber zwingend an den 450 MHz Frequenzen teilhaben.

Sicherheit hat ihren Preis

Sicherheit ist kein Zustand, sondern ein Prozess. Stadtwerke und ihre Verteilnetzbetreiber entwickeln ihre IT-Sicherheitsmaßnahmen ständig weiter: von Audits durch externe Sachverständige bis zur Sensibilisierung ihrer Mitarbeiter. Ihre Investitionen in Sicherheit, IT und Fachleute müssen sie auch in der Netzregulierung refinanziert bekommen. Auch dazu muss die Bundesregierung adäquate Antworten finden.

Denn: Sicherheit ist vielleicht nicht alles, aber ohne Sicherheit ist alles nichts.