DIE KOMMUNALEN UNTERNEHMEN

VERBAND KOMMUNALER UNTERNEHMEN e.V.

Kritische Infrastrukturen

Sicherheit erhöhen, Strukturen verschlanken

Unsere Ziele:

- Zügige Umsetzung der europäischen NIS2-Richtlinie und CER-Richtlinie
- Engere Zusammenarbeit von Bund, Ländern und Betreibern von kritischen Infrastrukturen
- Unnötigen Bürokratismus verhindern

Nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die **Gefährdungslage im Cyberraum so hoch wie nie**. Deutlich wird dies zum einen, wenn man sich die finanzielle Dimension der Schäden vergegenwärtigt. So wird der jährliche **Schaden** für deutsche Unternehmen auf **über 200 Milliarden Euro** geschätzt mit einer stark steigenden Tendenz. Insbesondere vor dem Hintergrund des russischen Angriffs auf die Ukraine bleibt die IT-Sicherheitslage zudem weiterhin dynamisch und kann sich jederzeit ändern. Das BSI geht davon aus, dass grundsätzlich alle Anlagen der **kritischen Infrastruktur potenzielles Ziel von Angriffen** sein können.

Kommunale Unternehmen sind für große Teile der Daseinsvorsorge in Deutschland verantwortlich und sind sehr häufig **Betreiber von kritischen Infrastrukturen**. Die im VKU vertretenen kommunalen Unternehmen versorgen die Bevölkerung mit Energie, Wasser, Telekommunikation und entsorgen Abwasser und Abfall. Dementsprechend stehen häufig auch kommunale Unternehmen im Focus der Angreifer. Macht man sich bewusst, dass die kritischen Infrastrukturen nicht nur digital, sondern **auch physisch angegriffen** werden (man denke z.B. an die Anschläge auf die Nordstream Pipelines oder auf eine LNG-Pipeline in Schleswig-Holstein), so ergibt sich das Bild einer insgesamt hohen abstrakten Gefährdungslage die aber auch bereits ins Konkrete durchschlägt.

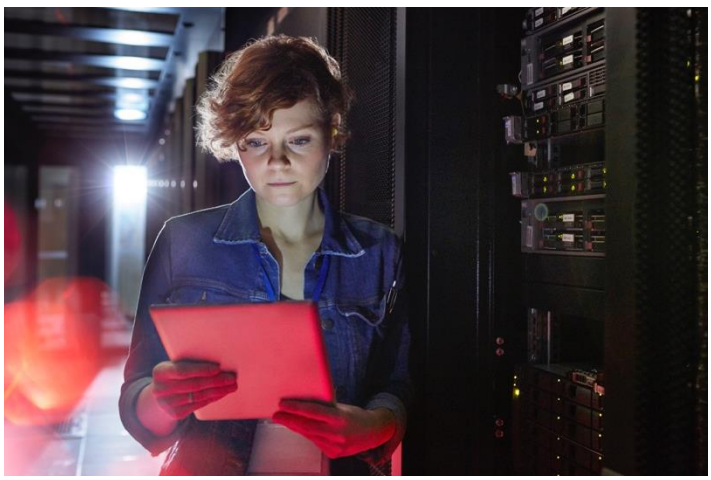
Da niemand exakt vorhersagen kann, wie sich zukünftig die Lage entwickelt, muss die **Gesellschaft insgesamt** und die **Betreiber von kritischen Infrastrukturen** im Besonderen **resilienter** werden. Dies bedeutet, dass die Widerstandsfähigkeit gegen Schocks erhöht und gleichzeitig die Regenerationsfähigkeit nach einem Schock gefördert werden muss. Exakt diesem Ziel dienen zwei europäischen Richtlinien, die bereits im Jahr 2022 in Kraft getreten sind: die **NIS2-Richtlinie** und **die CER-Richtlinie**. Während die NIS2-Richtlinie die Cybersicherheit adressiert, soll die CER-Richtlinie den physischen Schutz von kritischen Infrastrukturen steigern. Die Umsetzung dieser Richtlinien in deutsches Recht hätte bis Oktober 2024 geschehen müssen. Auf Grund des vorzeitigen Bruchs der Ampel-Koalition konnte die entsprechenden deutschen Gesetze (**NIS2-Umsetzungsgesetz** und das **Kritis-Dachgesetz**) jedoch nicht mehr verabschiedet 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.

Zügige Umsetzung der NIS2-Richtlinie und der CER-Richtlinie
Die **Umsetzung der NIS2-Richtlinie** und der **CER-Richtlinie** ist **überfällig** und hätte eigentlich bereits bis Oktober 2024 stattfinden müssen. Die fehlende Umsetzung führt dazu, dass die Unternehmen keine ausreichende Rechtssicherheit haben und sich deshalb teilweise mit ihren Investitionen zurückhalten. Außerdem droht Deutschland ein Vertragsverletzungsverfahren und hohe Bußgeldzahlungen auf Grund der fehlenden Umsetzung der Richtlinien. Bei der zügigen Umsetzung der Richtlinien muss jedoch darauf geachtet werden, dass nicht über die europäischen Vorgaben hinausgegangen wird, also kein „**Goldplating**“ betrieben wird.

Engere Zusammenarbeit von Staat und Betreibern
Wir benötigen eine noch **engere Zusammenarbeit zwischen Staat und Betreibern**, denn weder der Staat noch die Betreiber allein können die Sicherheit, der im Eigentum der Betreiber stehenden kritischen Infrastrukturen gewährleisten. Die Betreiber kennen ihre zu schützenden Anlagen selbst deutlich besser als es der Staat jemals könnte. Deshalb muss der Staat mögliche **weitere Regulierungen** in diesem Bereich **eng mit den Betreibern abstimmen**. Nur so können sinnvolle und erfüllbare Anforderungen an die Betreiber formuliert werden. Auch muss der Staat ein einheitliches deutschlandweites Lagebild aufbauen und die **Informationen mit den Betreibern teilen**. Für die Betreiber muss bei einem Vorfall klar sein, ob es sich um ein nur sie betreffendes Problem handelt oder ob es sich um einen deutschlandweiten Angriff auf die kritischen Infrastrukturen handelt. Das Bundesamt für Sicherheit in der Informationstechnik (**BSI**) sollte für diesen Zweck zu einer **Zentralstelle** im Bereich der Cybersicherheit ausgebaut werden. Die **Zusammenarbeit** zwischen **Bund** und **Ländern** sollte zudem besser verzahnt werden, um die Cyberabwehr des Bundes zu stärken.



Unnötigen Bürokratismus verhindern
Insbesondere im Rahmen der Umsetzung der europäischen Richtlinien muss dringend darauf geachtet werden, dass die Unternehmen nicht mit einem unnötigen Bürokratismus belastet werden. Jeder Euro, der in **Dokumentations- und Berichtspflichten** fließt, kann nicht in die tatsächliche Steigerung der Sicherheit gesteckt werden. Jede Minute der Abstimmung mit einer **weiteren Behörde** ist eine Minute, die nicht für die Umsetzung von Sicherheitsmaßnahmen zur Verfügung steht.

Förderung von KMUs
Kleine und mittlere Unternehmen (KMU) stehen vor besonderen Herausforderungen, denn sie haben nur eine eingeschränkte Finanz- und Personalkraft. **IT-Sicherheit und physische Schutzmaßnahmen** sind **teuer** und müssen refinanziert werden. Die bestehenden **Förderprogramme** müssen deshalb (finanziell) ausgeweitet und möglichst unbürokratisch gestaltet werden. Zudem sollten entsprechende Investitionen besonders **steuerlich gefördert** 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.

Grundsätzliche Diskussion über den Stellenwert der kritischen Infrastrukturen führen
Angriffe auf kritischen Infrastrukturen sind immer auch **Angriffe auf die gesamtdeutsche Sicherheit**. Vor diesem Hintergrund müssen die **Transparenzpflichten**, denen die Betreiber unterliegen **kritisch hinterfragt** werden. Im Moment müssen die Betreiber eine Vielzahl von Informationen über ihre kritischen Infrastrukturen offenlegen, die dann offen im Internet abgerufen werden können. Dies ist auf Grund der neuen Bedrohungslage nicht mehr zeitgemäß. Auch muss allgemein eine **Diskussion über die Kosten der Resilienzmaßnahmen** geführt werden. Resilienzmaßnahmen sind teuer und irgendjemand muss die Rechnung bezahlen. Es muss aber z.B. verhindert werden, dass diese **Kosten den Strompreis** weiter in die Höhe treiben. Der Schutz der kritischen Anlagen sollte als **überragendes öffentliches Interesse** anerkannt werden, und diese Wertung dann in jeder Abwägungsentscheidung auf gesetzlicher Ebene und auf Ebene der Verwaltung berücksichtigt werden. Die Gesetzgebung muss zudem **klarstellen**, **wo die Verantwortung des Staates für die Sicherheit der Bevölkerung endet** und **wo die Verantwortung der Betreiber** der kritischen Anlagen **beginnt**. Der Staat muss eine **vereinfachte Sicherheitsüberprüfung** der Mitarbeiter der Betreiber ermöglichen.