

Standpunkt • 17. Oktober 2023, 13:36

Neue Regulierungen für Kritische Infrastruktur: Nachhaltiger Schutz der Grundversorgung sieht anders aus

Von Ferdinand Gehringer



Betreiber Kritischer Infrastrukturanlagen haben derzeit alle Hände voll zu tun, EU-Richtlinien in nationale Gesetze umzusetzen. Es fehlt jedoch eine Priorisierung der Sektoren, schreibt Ferdinand Gehringer, Experte für Innere- und Cybersicherheit bei der Konrad-Adenauer-Stiftung, in seinem Standpunkt.

Mit dem NIS-2-Umsetzungsgesetz (NIS-2-UmsuCG) und dem Kritis-Dachgesetz werden derzeit zwei Richtlinien der Europäischen Union – die NIS-2 Richtlinie und die CER-Richtlinie – in nationales Recht umgesetzt. Als Kritische Infrastrukturen definiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“

Die neuen Gesetze sollen den **digitalen und physischen Schutz** sowie die **Widerstandsfähigkeit der Kritischen Infrastruktur** verbessern und sichern. Mit den neuen Gesetzen soll vor allem die **Funktionsfähigkeit des Binnenmarktes**

aufrechterhalten werden. Um die bloße Versorgungssicherheit geht es dabei nicht mehr.

So werden **Mindestverpflichtungen** für Betreiber Kritischer Infrastrukturen eingeführt oder ausgebaut, um das Risiko des Ausfalles oder der Störung der Einrichtungen zu minimieren. Die **Zahl der Sektoren nimmt stetig zu, ohne eine Priorisierung** zwischen den unterschiedlichen Versorgungsarten. Was **besonders wichtig für die Grundversorgung der Bevölkerung** ist, wird nicht aufgeführt. Vielmehr stehen die Regelungsziele sinnbildlich für einen sich immer weiter vom Grundgedanken der Krisenvorsorge entfernenden Regulierungsansatz.

Weiter Anwendungsbereich führt zur Überbelastung

Der Anwendungsbereich wird stetig erweitert und die **Anzahl der Sektoren im Vergleich zu den Vorgängerregulierungen erhöht**. Mittlerweile sind es 18 Sektoren in der NIS-2 Richtlinie und elf Sektoren in der CER-Richtlinie. Dies führt in der Umsetzung dazu, dass viel mehr Betreiber kritischer Einrichtungen die Anforderungen erfüllen müssen.

Zudem wird es künftig neben dem Anlagenbezug einen Bezug auf die Einrichtung geben, sodass je nach Umsatz und Mitarbeiterzahl **sogar das gesamte Unternehmen von den Verpflichtungen betroffen sein kann**. Der **Beratungsaufwand** vor allem bei den vielen kleinen und mittelständischen Betreibern wächst enorm an.

Aufgrund des **Fachkräftemangels auch im IT-Dienstleistungssektor** dürfte hier ein Kraftakt erforderlich sein, um eine ordnungsgemäße Umsetzung der Mindestverpflichtungen zu gewährleisten. In Deutschland geht man derzeit davon aus, dass künftig rund **29.000 Betriebe und öffentliche Einrichtungen der NIS-2 Richtlinie unterliegen**. Bisher waren es circa 4.500 Betreiber. So mangelt es derzeit an Ressourcen im operativen Bereich.

Richtlinien gefährden nationale und europäische Kohärenz

Zudem sehen beide Richtlinien jeweils die **Benennung einer nationalen Meldebehörde** vor. In Deutschland wird es mit dem **Bundesamt für Sicherheit in der Informationstechnik** und dem **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe** zwei unterschiedliche Bundesoberbehörden als Meldestellen geben. Überlagernde Zuständigkeiten, uneinheitliche Informationsstände und **Schwierigkeiten bei europäischen Kooperationen** sind vorprogrammiert.

Dazu kommt, dass bei der Umsetzung der Richtlinien in nationales Recht lediglich eine **Mindestharmonisierung** vorgesehen ist, können die **Mitgliedstaaten** im Rahmen der Umsetzung des digitalen und physischen Schutzes jeweils

Regelungen **unterschiedlicher Reichweite** erlassen. Es droht ein **uneinheitliches Schutzniveau in der Union**.

Resilienzgesetz zur Sicherung der Grundversorgung

Der Ansatz, einzelne Einrichtungen zu schützen, führt **nicht zu einer nachhaltigen Sicherung der Grundversorgung im Krisen- oder Katastrophenfall**. Vielmehr braucht es künftig eine **Verordnung zur europäischen Resilienz**, um ein einheitliches Schutzniveau zu verwirklichen. Durch die weiter zunehmende Vernetzung der Prozesse und Einrichtungen sowie durch mögliche Spill-Over Effekte könnte der Schutz einzelner Entitäten konterkariert werden, oder gar leerlaufen.

Schließlich kann das am schwächsten geschützte Glied in der Kette Auswirkungen auf das Schutzniveau der anderen haben. Entscheidend ist, **welche Teil- und Kernbereiche der Versorgung besonders geschützt werden** müssen. Diese müssen dann **priorisiert und deren Ausfall kompensiert** werden. Eine solche Priorisierung fehlt bislang ebenso wie grenzüberschreitende Lösungen innerhalb der EU zur Minderung der Auswirkungen bei Ausfällen oder von Störungsschäden und zur schnellen Wiederherstellung der Funktionsfähigkeit der Versorgung.

Europaweites, flächendeckendes Monitoring notwendig

Die Verordnung kann darüber hinaus Verantwortungsbereiche aufeinander abgestimmt regeln. Sie kann nicht nur Rechte und Pflichten von Betreibern der Infrastruktur beinhalten, sondern zugleich auch diese **von staatlichen Akteuren und der Bevölkerung** mit umfassen, um die Resilienz zu steigern und eine Krisenversorgung zu sichern.

Zugleich würde nur **eine Meldebehörde pro Mitgliedstaat**, vor allem die Zusammenarbeit unter den Ländern und mit der EU vereinfachen. Ein **europaweites und flächendeckendes Monitoring der Versorgung** – wie es das bereits in Ansätzen für die Stromversorgung gibt – sollte langfristig das Ziel sein, um Ausfälle oder Störungen frühzeitig zu erfassen und gegebenenfalls regional, aber auch länderübergreifend in der Europäischen Union auffangen zu können.

Schließlich ist die Grundversorgung erst recht im Krisenfall das, was die Kritische Infrastruktur ausmacht. Weshalb sollte sie dann nicht auch europäisch gesichert werden können?

Ferdinand Gehringer ist Referent für Innere Sicherheit und Cybersicherheit bei der Konrad-Adenauer-Stiftung.