# Im Fadenkreuz

**RESILIENZ:** Angriffe auf kritische Infrastrukturen nehmen zu. Abwehrmechanismen aber fehlen weitestgehend. Relevante Akteure sprechen von Zuständigkeitswirrwarr.

VON KATHLEEN SPILOK

Dass kritische Infrastrukturen angegriffen oder zumindest empfindlich gestört werden können, zeigte sich zuletzt bei den Sprengungen an den beiden Nord-Stream-Pipelines. Die Bilder der sprudelnden Ostsee gingen um die Welt. Doch die unterseeischen Gasleitungen sind nicht die einzigen anfälligen Infrastrukturen. Kurz danach, im Oktober 2022, fielen die Kommunikationskabel der Deutschen Bahn einem Sabotageakt zum Opfer: In Norddeutschland brach der Zugverkehr zusammen. Niemand wurde verletzt. Trotzdem zeigt dies: Deutschland ist verwundbar. Fällt zum Beispiel der Strom großflächig aus, sind Rechenzentren, Versorger und Krankenhäuser kaum noch handlungsfähig. Selbst wenn sie Notstromaggregate haben, mit denen sich kürzere Zeiträume überbrücken lassen. Flugzeuge bleiben am Boden, Bahnnetz und Straßenverkehr kommen zum Erliegen.

**Kritische Infrastruktur kann nur gemeinsam vor Sabotage geschützt werden:** Der Schutz kritischer Infrastrukturen ist eine gemeinsame Aufgabe von Bund, Ländern und den Kommunen. Gerade jetzt in unruhigen Zeiten. „Wir haben seit Beginn des verbrecherischen russischen Angriffskriegs gegen die Ukraine auch eine veränderte Sicherheitslage in Deutschland", äußerte sich Bundesinnenministerin Nancy Faeser Anfang Dezember 2022, als sie die Eckpunkte für das sogenannte Kritis-Dachgesetz vorstellte, das bis zum Sommer fertig sein soll. Kritis steht für kritische Infrastrukturen. Sieben Sektoren zählen in Deutschland dazu: Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit, IT und Telekommunikation, Transport und Verkehr, Wasser. Wer aber ist bei Kritis für den Schutz vor was in Deutschland eigentlich verantwortlich?

In Bezug auf die Kritis-Infrastrukturen nimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Rolle als Cybersicherheitsbehörde ein, die die digitale Infrastruktur auf Bundesebene schützen soll. Mit der Novelle des BSI-Gesetzes vom Juni 2021 wurden die Sektoren um die Siedlungsabfallentsorgung erweitert. Die Gefahr, dass sich Seuchen verbreiten, war der ausschlaggebende Punkt. Für die Änderungsverordnung wird der Referentenentwurf im ersten Halbjahr 2023 erwartet. Außerdem gelten die Bereiche Staat und Verwaltung sowie Medien und Kultur als sicherheitsrelevant und damit zählen sie zu den kritischen Infrastrukturen.

**Kritis-Betreibern kommen besondere Aufgaben zu:** Für alle Betreiber von Anlagen, die die Versorgungssicherheit gewährleisten, sogenannte Kritis-Betreiber, formuliert das BSI Anforderungen und fordert Audits ein. Schwellenwerte beschreiben, ob es sich um Kritis-relevante Anlagen handelt. Ganz grob fallen Anlagenbetreiber darunter, die mehr als 500 000 Personen versorgen. Das unabhängige Online-Nachschlagewerk „OpenKRITIS" zählte im Jahr 2021 rund 1600 registrierte Betreiber.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sieht kritische Infrastrukturen aus dem Blickwinkel des Zivil- bzw. Katastrophenschutzes. Es wurde 2004 eingerichtet als Antwort auf die Ereignisse des 11. September 2001 und auf das Elbhochwasser in Hamburg. Generell ist das BBK keine operative Behörde, sondern sieht sich mehr als Thinktank. Aus dem BBK kommen die Informationen, das Wissen über kritische Infrastrukturen, es werden Empfehlungen gegeben. Allerdings sieht das Kritis-Dachgesetz nun vor, das BBK in Zukunft als zuständige Behörde für den Schutz kritischer Infrastrukturen zu installieren. Welche Befugnisse das BBK damit neuerdings erhält, ist noch offen.

**Zu viele Akteure behindern den wirksamen Schutz der kritischen Infrastruktur:** Relevante Akteure etwa auf Bundesebene sind aber nicht nur BSI, BMI (Bundesinnenministerium) und BBK. Die AG Kritis, ein Zusammenschluss von Fachleuten, die allesamt in Kritis-Berufen tätig sind, spricht gar von einem Zuständigkeitswirrwarr. Der Versuch, die Aufgabenverteilung in einem Schaubild deutlich zu machen, endete in einem unübersichtlichen Wimmelbild. Die Experten stellten fest, dass zu viele Behörden in diesem Zusammenhang tätig sind. „Jeder ist ein bisschen zuständig, aber keiner kann im Prinzip allein handeln", meint Johannes Rundfeldt, einer der Sprecher der AG.

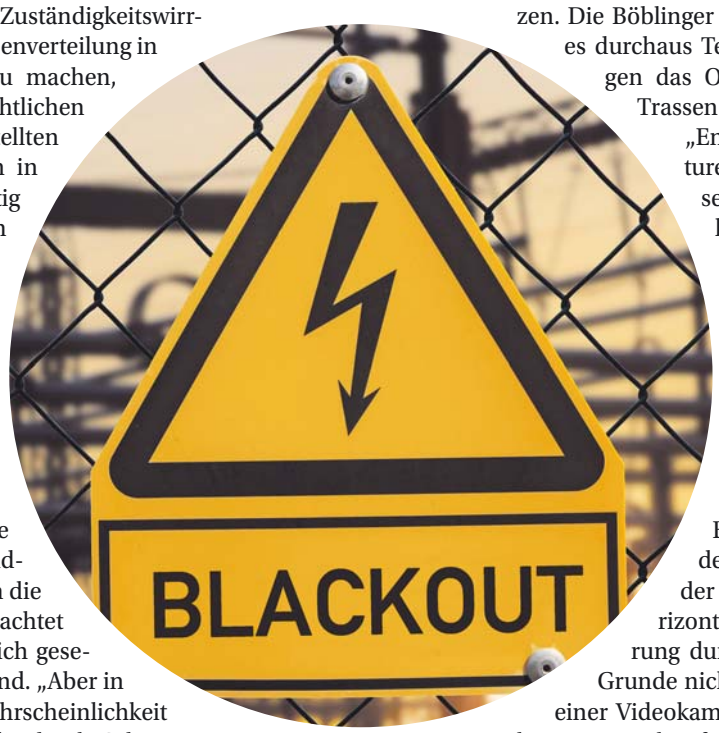
Die AG Kritis ist eine ehrenamtliche Organisation, die es sich zur Aufgabe gemacht hat, zuständige Stellen zu beraten und öfter mal auf missliche Umstände aufmerksam zu machen. Rundfeldt macht sich Sorgen, denn die Arbeitsgemeinschaft beobachtet eine Menge Effekte, die für sich gesehen noch nicht dramatisch sind. „Aber in der Summe die Eintrittswahrscheinlichkeit für eine Großschadenslage, die durch Cybervorfälle hervorgerufen wird, doch stark steigen lässt", macht er klar.

**Krisenmanagement für eine gestörte kritische Infrastruktur:** Auf Orts-, Kreis- und Länderebene gibt es zusätzlich zahlreiche Aktivitäten, die die Sicherheit der Bevölkerung adressieren. Zum Beispiel die Enquetekommission des Landtags von Baden-Württemberg „Krisenfeste Gesellschaft". Sie arbeitet seit April 2022 an der Frage, wie das Gemeinwesen widerstandsfähig wird. Hilfsdienste wurden gehört, Mitarbeiter von Vodafone und der Deutschen Bahn, der Stand von Wissenschaft und Technik vorgestellt. Bürgerinnen, Bürger, Jugendliche kamen in einem Extraformat zu Wort.

Die schwierigste Aufgabe wird sein, die schiere Menge an Informationen so abzuschichten, dass am Ende konkrete Maßnahmen stehen. Andererseits: Es gibt natürlich Routinen, die immer greifen, egal welche Art von Krise stattfindet. „Wie verallgemeinern wir das so, dass wir trotzdem nicht in solche Bredouillen und Bedrängnisse hineinkommen – wie bei Corona", formuliert Alexander Salomon, der die Enquetekommission leitet, sein Ziel. „Aber so richtig endgültig krisensicher werden wir vielleicht nicht werden. Weil wir Krisen nicht vorhersagen können", resümiert er.

**So wird kritische Infrastruktur widerstandsfähiger – ein Beispiel.** Esslingen beispielsweise reagierte auf eine Empfehlung der Landesregierung, sich auf Notsituationen vorzubereiten. In der Stadt am Neckar stellte der Erste Bürgermeister vor einigen Wochen an 19 Stellen in der Stadt Schilder auf, die Notfalltreffpunkte markieren. Für den Fall, dass es längere Stromausfälle gibt oder andere kritische Situationen eintreten, sollen sich die Bewohner dort treffen. Länger als 15 min zu Fuß sollte keiner unterwegs sein.

Einen Krisenstab der Stadtverwaltung Esslingen gibt es bereits seit sieben Jahren. Der entscheidet, welche Angebote es dort geben wird, wie im Krisenfall kommuniziert wird. Ob etwa die Feuerwehr Lautsprecherdurchsagen macht. „Wenn die Bevölkerung gut vorbereitet ist, verschafft uns das in einer Schadenslage etwas mehr Luft", sagt Andreas Gundl von der Feuerwehr Esslingen.




**Was tun, wenn der Blackout wirklich eintritt?** Fachleute kritisieren, dass die Zuständigkeiten zum Schutz kritischer Infrastrukturen sehr vielschichtig organisiert sind.

Foto: imago images/U. J. Alexander

„Jeder ist ein bisschen zuständig, aber keiner kann im Prinzip allein handeln."

**Johannes Rundfeldt,** Sprecher der AG Kritis, zur Notfallverantwortung für kritische Infrastrukturen in Deutschland

**Wie aber erkennt man, wenn sich jemand an der Infrastruktur zu schaffen macht?** Mit Zäunen oder anderen physikalischen Maßnahmen lassen sich die Hunderte Kilometer langen Pipelines, Stromtrassen, Schienennetze kaum schützen. Die Böblinger Firma AP Sensing zeigt, dass es durchaus Technologien gibt, die sozusagen das Ohr direkt an den kritischen Trassen und Strecken haben.

„Entlang den meisten Infrastrukturen liegen Glasfaserkabel. Diese nutzen wir als Sensor und können hierüber an jedem einzelnen Meter einer Strecke Vibrationen in Echtzeit aufnehmen", beschreibt Clemens Pohl, CEO von AP Sensing, das Prinzip. Die Kombination mit künstlicher Intelligenz (KI) lässt die Böblinger erkennen, welche Art Vibration es ist. Ein Bagger etwa hat eine andere Signatur, als wenn man mit der Schaufel gräbt oder eine Horizontalbohrmaschine eine Bohrung durchführt. Damit lässt sich im Grunde nichts verhindern: „Aber wie bei einer Videokamera oder einem Radarsystem kann man sich sofort darum kümmern, Saboteure können ergriffen werden", sagt Pohl. Netzbetreiber zum Beispiel könnten entscheiden, ob jemand rausgeschickt wird, der nachschaut, was den Alarm ausgelöst hat. „Unsere Systeme sind in die Leitwarten der Übertragungsnetzbetreiber eingebunden", erläutert Pohl. Der Betreiber erfasst und klassifiziert die Daten für sich.

**Ist Deutschland im Fall einer Krise wirklich handlungsfähig?** Nimmt man die Stromversorgung in den Blick, dann können unterschiedlichste Faktoren dazu führen, dass die Bevölkerung überregional ohne Strom dasteht. Ein solches Blackout-Szenario kann entstehen, wenn in einer sowieso schon angespannten Verbrauchs- oder Erzeugungssituation bei der Erzeugung, der Stromübertragung oder der Verteilung über die Netze etwa Sabotage, Naturkatastrophen, Cyberattacken, Lastabschaltungen oder menschliches Versagen zu einem Ausfall der Systeme führen. Ohne Strom laufen auch die Trinkwasserpumpen nicht. Einem Bericht des rbb vom November 2022 zufolge könnte beispielsweise Berlin für 36 Stunden nach einem Stromausfall mit Trinkwasser versorgt werden. Anschließend müsste Frischwasser aus Notbrunnen gezapft werden.

„Wir sind nicht komplett handlungsunfähig, aber wir müssen Dinge verbessern", betont Johannes Rundfeldt von der AG Kritis. Bisherige Vorfälle seien allesamt zufriedenstellend abgearbeitet worden. Auch bei den verschiedenen großen Ausfällen von Behörden-IT in den vergangenen Jahren hätte der Staat mehr oder weniger funktioniert, meint Rundfeldt. „Nun hatten wir den Blackout, den überregionalen Notfall noch nicht gehabt. Und das ist gut so, aber wir müssen uns auf genau dieses Ereignis besser vorbereiten", drängt er. So fordert die AG Kritis beispielsweise die Gründung eines Cyberhilfswerks (CHW). Es soll ähnlich wie das THW in Großschadenslagen zum Einsatz kommen. Das CHW könnte bei einem massenhaften Befall von Schadsoftware in der Verwaltung helfen oder die zivile Internetversorgung wiederherstellen.