Partnerschaftlich agieren

Schutz kritischer Infrastrukturen

Der Begriff „kritische Infrastrukturen“ (im folgenden: kI) war bis Ende des vorigen Jahrhunderts nicht gebräuchlich. Heute wird er geradezu inflationär verwendet. Dabei ist der Schutz von kI eine der zentralen Aufgaben von Staat und Wirtschaft.

Kritische Infrastrukturen – dazu gehören unter anderem Energie, Informationstechnik, Transport und Verkehr. Bild: Peter Freitag/Pixelio

Der Begriff Infrastruktur meint die innere Struktur eines Organismus, sowohl auf der mikroökonomischen Ebene eines Unternehmens wie auf der makroökonomischen Ebene einer Branche, einer Volkswirtschaft oder einer internationalen Wirtschaftsgemeinschaft.

Nach der allgemein anerkannten Definition des Bundesministerium des Innern (BMI) sind kI 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.

Je gravierender die Schadensauswirkungen sind, umso kritischer ist die Infrastruktur. Vor einer inflationären Nutzung des Begriffs muss jedoch gewarnt werden. Hierzu einige Grundgedanken:

Unterschiedlichkeit der einzelnen kI

So unterschiedlich die Versorgungsbedürfnisse von Staat, Bevölkerung und Wirtschaft sind, so verschieden sind die dafür erforderlichen Infrastrukturen. Sie finden sich vor allem in den Sektoren Gesundheit, Wasser und Ernährung, Energie, Informationstechnik, Telekommunikation und Medien, Transport und Verkehr, Finanz- und Versicherungswesen, Verwaltung, öffentliche Sicherheit und Verteidigungswesen. Der Verschiedenheit dieser Versorgungsbereiche entsprechend sind auch Schutzziele, Bedrohungsphänomene und Mittel zu deren Abwehr höchst unterschiedlich.

Schutzziele und Bedrohungsphänomene

Die wichtigsten Schutzziele, die anzustreben sind, damit die kI ihren Zweck optimal erfüllen können, sind ihre zweckentsprechende Verfügbarkeit, ihre Sicherung vor Angriffen und Zerstörungen der verschiedensten Art, der Know-how-Schutz gegenüber Ausspähung und illegalem Technologietransfer sowie der Schutz der Vertraulichkeit von Kommunikation, von gespeicherten und transferierten Daten und vertraulich zu behandelnder Informationen.

Diese Schutzziele werden durch menschliches und technisches Versagen (technische Störungen, Bedienungsfehler, Nachlässigkeit im Umgang mit kI), durch Kriminalität (vor allem durch Sabotage, terroristische Anschläge, Diebstahl und Spionage) und Naturkatastrophen beeinträchtigt.

Verantwortlichkeit des Betreibers

Unbeschadet einer überlagernden Verantwortlichkeit des Staates zur Daseinsvorsorge und zur Gewährleistung der für die Daseinsvorsorge notwendigen Infrastrukturen obliegt die Primärverantwortung für den Schutz kI dem Betreiber. Insgesamt sind etwa 80 Prozent aller kI in privater Hand. Die Verantwortung des Betreibers kI für ihren Schutz ergibt sich unabhängig von normativen Regelungen aus dem Verursacherprinzip ebenso wie aus der

→ AUTOR

***Manfred Buhl** ist Vizepräsident des BDSW, Bad Homburg.*
Tel.: +49 6172 948050
E-Mail: info@bdsw.de
www.bdsw.de

Sozialpflichtigkeit des Eigentums gemäß Art. 14 Abs.2 GG. Teilweise ist diese Verantwortung auch in Einzelgesetzen festgeschrieben, so zum Beispiel

→ für Luftfahrtunternehmen und Flughafenbetreiber im Luftverkehrsgesetz und im Luftsicherheitsgesetz
→ für die Betreiber von Eisenbahnen und Schienenwegen im Eisenbahngesetz
→ für die Betreiber von Anlagen, in den gefährliche Stoffe gelagert oder verarbeitet werden in der Störfallverordnung
→ für die Errichter und Betreiber von Anlagen mit Kernbrennstoffen im Atomgesetz.

Der Beitrag des Sicherheitsgewerbes

Vielfach beauftragt der Betreiber ein Sicherheitsunternehmen mit einzelnen Schutzaufgaben oder dem gesamten Schutz einer kI. Der großen Bedeutung kI entsprechend muss die Sicherheitsdienstleistung zuverlässig, sorgfältig, fachgerecht und effizient sein. Der Betreiber sollte sich daher schon vor der Beauftragung von der Zuverlässigkeit und Leistungsfähigkeit des Sicherheitsunternehmens und der einzusetzenden Dienstkräfte überzeugen:

→ Zertifizierung: Eine Möglichkeit dazu bietet der Nachweis einer Zertifizierung. Mindestens sollte das zu beauftragende Sicherheitsunternehmen nach den allgemeinen Qualitätsnormen der ISO 9001 ff. zertifiziert sein. Mit der Fortschreibung des Programms Innere Sicherheit im Jahr 2009 hat die Innenministerkonferenz (IMK) zur Erreichung und Optimierung einheitlicher Standards die Zertifizierung privater Sicherheitsdienste – vor allem für die Zusammenarbeit mit der Polizei – gefordert. Eine von der IMK eingesetzte Projektgruppe hat dazu einen Kriterienkatalog mit besonderen Anforderungen für Einsätze zum Schutz von Veranstaltungen, Verkehrsflughäfen, ÖPV und sonstiger kI entwickelt und Vorschläge für das weitere Vorgehen erarbeitet. Entsprechend der EU-Direktive 2008/114/EC hat der europäische Dachverband des Sicherheitsgewerbes (CoESS) als Voraussetzung für die Beauftragung von Sicherheitsunternehmen mit dem Schutz von Anlagen kI mit „transnationaler“ Dimension einen eigenen Kriterienkatalog mit anspruchsvollen Qualitätskriterien erarbeitet, die aber noch der Konkretisierung und Detaillierung bedürfen.
→ Zuverlässigkeit: Zum Schutz kI sollten ausnahmslos nur zuverlässige Unternehmer und Mitarbeiter eingesetzt werden. Zur Bestätigung der Zuverlässigkeit ist die unbeschränkte Auskunft aus dem Bundeszentralregister erforderlich. Darüber hinaus ist jeder, der mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll, vorher einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz zu unterziehen.
→ Qualifikation der Manager und ihrer Mitarbeiter: Die notwendige Qualifikation des Managements eines Sicherheitsunternehmens und der einzusetzenden Mitarbeiter richtet sich nach den wahrzunehmenden Sicherheitsfunktionen. Je komplexer der Auftrag ist, umso höher und umfassender muss die Qualifikation sein. Übernimmt ein Dienstleister die gesamte Unternehmenssicherheit, so muss das Management die Betriebsabläufe und Geschäftsprozesse kennen lernen.
Nur so kann es alle sicherheitsrelevanten Prozesse feststellen und eine Sicherheitskonzeption erarbeiten, die alle Schwachstellen umfasst.
→ Brand- und Explosionsschutz, Umgang mit gefährlichen Stoffen und Gefahrgut: Wegen der oft verheerenden Folgen eines Brandes, die zum völligen Ausfall einer kI im örtlichen Bereich führen kann, bildet der Brandschutz die zumeist wichtigste Schutzvorkehrung. Dazu gehört der bauliche ebenso wie der technische und organisatorische Brandschutz einschließlich sicherer Flucht- und Rettungswege sowie Evakuierungsübungen. Soweit in kI gefährliche Stoffe im Sinne des Chemiegesetzes und des Sprengstoffgesetzes gelagert oder verarbeitet werden, muss ein mit der Unternehmenssicherheit beauftragtes Unternehmen die Gefährlichkeit der Stoffe und die beim Umgang und der Lagerung zu beachtenden Vorschriften kennen.
→ Verantwortlichkeit des Staates für den Schutz kritischer Infrastrukturen: Die Verantwortlichkeit des Staates für den Schutz kI ist mehrschichtig angelegt: Sie kann in einer Gewährleistungsverantwortung (zum Beispiel für Post und Telekommunikation) oder auch in einer Erfüllungsverantwortung bestehen (so in der Wahrnehmung der Polizei- und Verteidigungsfunktionen). Sie kann sich auf die Gesetzgebung beschränken oder auch die Verwaltung umfassen. Und sie kann zwischen Bund und Ländern geteilt sein. Dem Staat stehen vielfältige Einflussmöglichkeiten und Einwirkungsmaßnahmen zur Verfügung.

Ziele definiert

Das BMI hat sich in seiner nationalen Strategie zum Schutz kI auf drei strategische Ziele konzentriert:

→ Prävention durch die Analyse aller zu erwartenden Risiken und der dadurch veranlassten Schutzvorkehrungen
→ Minimierung der Folgen von Störungen und Ausfällen durch effektives Notfall- und Krisenmanagement sowie Selbsthilfekapazität der unmittelbar Betroffenen
→ Gefährdungs- und Störfallanalysen zur nachhaltigen Verbesserung des Schutz von kI und Entwicklung von Schutzstandards gemeinsam mit Betreibern.

In allen drei Funktionsbereichen sind Sicherheitspartnerschaften zwischen Staat und Wirtschaft und die Verhältnismäßigkeit von Ressourcen maßgebliche Leitprinzipien. In Umsetzung dieser Leitprinzipien sind „Gesprächskreise Kritis“ zwischen Bund, Ländern und Kommunen gebildet worden. Zu den Handlungsempfehlungen gehört der erstmals 2008 veröffentlichte Leitfaden für Unternehmen und Behörden zum Risiko- und Krisenmanagement für kI. Er bietet das Handwerkszeug, um ein Risiko- und Krisenmanagement in Einrichtungen und Unternehmen aufzubauen und bestehende Systeme zu ergänzen. □