Das IT-Sicherheitsgesetz – mehr IT-Sicherheit für kritische Infrastrukturen?

Gastautor 2014-10-21T09:50:51

von JAKOB TISCHER und SÖNKE E. SCHULZ

dem Nationalen IT-Gipfel befassen sich heute hochrangige Vertreter aus Politik, Wirtschaft und Wissenschaft unter dem Motto „Arbeiten und Leben im digitalen Wandel – gemeinsam.innovativ.selbstbestimmt“ unter anderem mit der Sicherheit von Informations- und Kommunikationstechnik und der zugrunde liegenden Infrastruktur. Aber was bedeutet IT-Sicherheit eigentlich konkret? Was wäre etwa, wenn das Internet flächendeckend ausfiele, stunden- oder möglicherweise tagelang? Die vielfältigen Abhängigkeiten und Verflechtungen lassen besorgniserregende Konsequenzen in den Bereich des Vorstellbaren rücken. Wer „Blackout“ von Marc Elsberg gelesen hat, dürfte sich Szenarien des Ausfalls kritischer Infrastrukturen ausmalen können. Kritische Infrastrukturen, bei deren Beeinträchtigung es zu dramatischen Folgen für das Gemeinwohl kommen kann, unterliegen einer staatlichen Schutzgewähr. Auch informationstechnische Systeme gehören dazu – es ist also konsequent, dass sich die Bundesregierung des Themas annimmt.

Am 19.8.2014 legte das Bundesministerium des Innern den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG-E) vor. Das Gesetz soll die IT-Sicherheit insbesondere bei kritischen Infrastrukturen verbessern, dem Schutz der Bürger in einem sicheren Netz und dem Schutz der IT des Bundes dienen. Hinzu kommen eine Stärkung des BSI sowie die Erweiterung der Ermittlungszuständigkeiten des BKA im Bereich Cybercrime. Der Entwurf enthält im Wesentlichen Änderungen des Telekommunikations-, Telemedien- und BSI-Gesetzes.

IT und Internet als kritische Infrastrukturen

Sind Internet und informationstechnische Systeme kritische Infrastrukturen?
Während für den Bürger der Ausfall seiner IT bzw. des Internets für wenige Stunden (wenn auch schwer, so dennoch) verkraftbar ist, sieht dies bei Unternehmen und staatlichen Akteuren anders aus. Eine funktionsfähige Infrastruktur ist nicht ausschließlich für den Freiheitsgebrauch der Bürger erforderlich, sondern der Staat hat selbst ein originäres Interesse daran. Staatliche Aufgabenerfüllung und wirtschaftliche Prozesse sind ohne IuK-Technologien undenkbar. Insofern ist man schnell veranlasst, „dem Internet“ den Stempel einer kritischen Infrastruktur aufzudrücken. Es bedarf aber einer Einschränkung: Wie § 12g EnWG exemplarisch für den Energiesektor zeigt, ist nicht die gesamte „Energieversorgung“ als solche kritisch, sondern nur – im europäischen Kontext – diejenigen Anlagen, deren Störung erhebliche Auswirkungen in mindestens zwei EU-Mitgliedstaaten haben kann.

Die TK-Infrastruktur als Rückgrat

Die Funktionsweise des Internets verdeutlicht, dass wesentliche Elemente der Infrastruktur, die als kritisch eingestuft werden könnten, Telekommunikationsinfrastrukturen sind, die seit jeher den kritischen Infrastrukturen zugeordnet werden. Insofern können rechtliche Handlungsinstrumente ggf. hier – d. h. im TKG – ansetzen. Hinzu kommt, dass nicht jeder „Netzteil“, jedes „Teilnetz“ und jede Einrichtung, die zur flächendeckenden Funktionsfähigkeit des Internets beiträgt, zugleich kritisch ist. Ein Router bzw. Switch, der eine Kleinstadt versorgt, mag die Systemrelevanz nicht erfüllen, der DE-CIX in Frankfurt vielleicht schon eher. Es ist daher konsequent, die TK-Anbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, stärker in die Verantwortung zu nehmen.

Die vom IT-SiG-E vorgesehenen Änderungen konkretisieren u. a. den Störungsbegriff i. S. v. § 100 TKG: Künftig sollen die von § 100 Abs. 1 TKG erlaubte Erhebung und Verwendung von Bestands- und Verkehrsdaten auch zur Prävention und Beseitigung von Störungen, die zu einer Einschränkung der Verfügbarkeit von IuK-Diensten oder zu einem unerlaubten Zugriff auf Nutzersysteme führen können (und nicht nur bei Störungen der physischen Beschaffenheit), gerechtfertigt sein. Die geplante Neufassung von § 109 Abs. 5 TKG soll die den Anbietern bereits auferlegte Meldepflicht bei Sicherheitsverletzungen und Störungen auf das Vorfeld erweitern.

Rechtfertigung erhöhter Verantwortlichkeiten von TK-Anbietern

Indem der Staat durch den Abbau des Monopols im Telekommunikationsbereich seinen unmittelbaren Einfluss aufgegeben hat, ist er zu dessen Schutz im Sinne einer Verantwortungsteilung auf die Betreiber angewiesen. Der Schutz kritischer Infrastrukturen ist gemeinsame Aufgabe, bei deren Erfüllung der Ausgleich zwischen Wirtschafts- und übergeordneten Allgemeininteressen herzustellen ist. Eine etwaige Übergewichtung des wirtschaftlichen Interesses seitens der über mehr Einfluss verfügenden Betreiber könnte allerdings den fragilen Ausgleich stören und zu Unzulänglichkeiten beim Schutzniveau führen. Deshalb ist zur

Sicherstellung des Gemeinwohls die Auferlegung besonderer Pflichten denkbar. Die Rechtfertigungsgründe für eine solche Inhalts- und Schrankenbestimmung zu Lasten des Eigentums der Betreiber sind im Kontext der Sozialbindung des Eigentums (Art. 14 Abs. 2 GG) sowie den Anforderungen, die eine Enteignung rechtfertigen würden, zu sehen. Für kritische Infrastrukturen ist nur an deren Definition zu erinnern, die vergleichbare Merkmale aufweist: Es handelt sich um Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Beeinträchtigung erhebliche Versorgungsengpässe bis hin zu Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können.

IT-Sicherheit der (sonstigen) kritischen Infrastrukturen

Weiterhin ist das Verhältnis von Internet und IT zu anderen kritischen Infrastrukturen zu betrachten: IT als solche ist keine kritische Infrastruktur – sie ist Mittel zum Zweck, niemals Selbstzweck. Nur diejenige IT ist daher kritisch, die für eine andere kritische Infrastruktur zwingend erforderlich ist. Dies gilt bspw. für Steuerungseinrichtungen von Verkehrs-, Energie-, Entsorgungs- und Gesundheitsinfrastrukturen. Im rechtlichen Sinn ist eine dreifache Relevanzprüfung angelegt: in einem ersten Schritt ist ein bestimmter Infrastrukturbereich als „kritisch“ zu klassifizieren, wobei sich diese Einstufung – in Stufe zwei – nur auf die systemrelevanten Teile bezieht. In einem dritten Schritt strahlt diese besondere Bedeutung auf die für den maßgeblichen Teil der Infrastruktur maßgeblichen IT-Systeme aus.

Meldepflichten als Handlungsinstrument

Insofern ist es sachgerecht, die informationstechnischen Systeme der Unternehmen in den Blick zu nehmen, die (andere) kritische Infrastrukturen betreiben. Zentraler Ansatzpunkt können Meldepflichten für die Betreiber sein, wie sie im Rahmen des IT-SiG-E vorgesehen sind. Der Entwurf wirft allerdings noch (Rechts-)Fragen auf. Zum einen erscheint der Auslöser der Meldepflicht, eine *Beeinträchtigung von informationstechnischen Systemen, Komponenten oder Prozessen, die zu einem Ausfall oder einer Beeinträchtigung der betriebenen Kritischen Infrastruktur führen kann,* einen breiten Interpretationsspielraum zu lassen. Eine Präzisierung soll auf Ebene eines von BSI und Betreibern entwickelten Kriterienkatalogs für meldungsrelevante Sicherheitsvorfälle erfolgen. Ob dies die Bestimmtheitsanforderungen erfüllt, an denen die Verpflichtung zu einer – im Fall der tatsächlichen Beeinträchtigung der kritischen Infrastruktur – nicht mehr anonymisierten Meldung zu messen ist, erscheint zweifelhaft. Konkretisierungsbedürftig sind auch die kritischen Infrastrukturen selbst, die künftig durch Rechtsverordnung festgelegt werden sollen. Trotz der Vorzüge des Instruments der Rechtsverordnung (bessere Reaktionsfähigkeit bei dynamischen Materien, größere Sachnähe des Verordnungsgebers, keine Überfrachtung des Parlamentsgesetzes) stellt sich die Frage, ob die mit weitreichenden Konsequenzen (im Sinne eines Anknüpfungspunkts für staatliche Eingriffe) verbundene Festlegung kritischer Infrastrukturen nicht aufgrund ihrer Wesentlichkeit eine Befassung des Parlaments erfordert. Gleichwohl dürften sich Meldepflichten – wie auch Seitenblicke

ins Lebensmittel- und Infektionsschutzrecht zeigen – als angemessenes und geeignetes Mittel der Abwehr von Gefahren für die IT-Sicherheit darstellen.

Das BSI als Mammutbehörde

Mit dem IT-SiG-E wird ein sektorenübergreifender Ansatz gewählt – mit Ausnahme besonderer Regelungen im TKG und (im Interesse des Schutzes der Bürger) im TMG. Ein Blick ins geltende Recht zeigt aber, dass auch sektorspezifisches Vorgehen denkbar wäre: So ist als Bestandteil des institutsinternen Risikomanagements bei Kredit- und Finanzdienstleistungsinstituten von § 25a Abs. 1 Satz 3 Nr. 3 KWG die Festlegung eines angemessenen Notfallkonzepts, insbesondere für IT-Systeme, verpflichtend. Auch der IT-SiG-E versucht der Verschiedenheit der Branchen Rechnung zu tragen, indem die Einbeziehung branchenspezifischer Sicherheitsstandards ermöglicht wird. Der Vorteil eines sektorspezifischen Ansatzes wäre allerdings, dass sachnähere Aufsichts- und Verantwortungsstrukturen existieren. Aufsichtsbehörden könnten über fachspezifische Expertise verfügen und um die Funktionslogiken des jeweiligen Sektors wissen. So ist für das TKG, einschließlich der IT-sicherheitsrelevanten Normen, die BNetzA und nicht das BSI zuständig. Durch den gewählten Ansatz droht das BSI zur „Mammutbehörde“ mit Zuständigkeiten für weite Teile des Wirtschaftslebens zu werden.

Regelungslücken in vernetzten Gesamtsystemen

Dennoch bleibt zu berücksichtigen, dass sich „das Internet“ und seine Funktionsfähigkeit nicht in Telekommunikationsinfrastrukturen erschöpfen. Es bleibt eine Lücke, die nicht vom TKG, aber auch nicht von anderen Regulierungen erfasst wird. Dazu dürften bspw. die DNS-Server zählen, deren Aufgabe die Auflösung von Internet- in IP-Adressen ist, ohne die die Kommunikation im Netz nicht möglich ist und die überwiegend in der Hand nicht-staatlicher, nicht-regulierter Organisationen (in Deutschland: denic eG) liegen. Die Besonderheit des Internets besteht gerade darin, dass nicht eine Entität Gesamtverantwortung für das Gesamtsystem trägt, sondern die Verantwortlichkeit, die durch Regulierung explizit zugewiesen und ausgeformt werden kann, auf viele Akteure verteilt ist. Insofern ist anzuerkennen, dass sich kaum alle Teilbereiche und -aspekte werden regulieren lassen, sodass ggf. andere Maßnahmen ergänzend hinzutreten müssen (bspw. resiliente Systeme durch Entnetzung).
