Eckpunkte zum Referentenentwurf des "Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-SiG 2.0)

Berlin, 26. Juni 2019

Das Bundesministerium des Innern, für Bau und Heimat (BMI) diskutiert derzeit eine Novellierung des IT-Sicherheitsgesetzes. Ein noch nicht offizieller Referentenentwurf (hier als IT-SiG 2.0i bezeichnet) hierzu gelangte Anfang April in die Öffentlichkeit. Gleichzeitig kamen Fragen zum Vorgehen des BMI im weiteren Gesetzgebungsverfahren auf. Um die Debatte um das IT-Sicherheitsgesetz weiter zu begleiten, hat eco die folgenden Eckpunkte zu dem bekannt gewordenen Referentenentwurf erarbeitet und möchte diese in die weitere Debatte einbringen. Aus Sicht der Internetwirtschaft enthält der Entwurf mehrere Aspekte, die noch einmal einer dringenden Überprüfung sowohl unter dem Aspekt der Rechtsstaatlichkeit, als auch unter dem Gesichtspunkt der Zumutbarkeit für Wirtschaft aber auch für Internetnutzer darstellt.

Maßgeblich gestützt werden diese Überlegungen von den Diskussionen, die in der Branche bereits geführt werden, und als deren Zwischenergebnis festgehalten werden kann, dass eine maßgebliche Verbesserung der Sicherheit vor allem dann erreicht werden kann, wenn alle Akteure, die an der Gestaltung von Diensten, Produkten und Infrastrukturen beteiligt sind, im Rahmen ihrer Gestaltungs- und Handlungsmöglichkeiten Verantwortung übernehmen. Dies umfasst nicht nur Betreiber kritischer Infrastrukturen, sondern insbesondere auch Hersteller von Geräten und Komponenten.

Die Punkte, die eco vor dem Hintergrund dieser Erkenntnisse in Bezug auf den bekannt gewordenen Referentenentwurf IT-SiG 2.0i diskutieren möchte, sind im Folgenden:

- **Begriffsbestimmungen / Anwendungsbereich / KRITIS-Regelungen**

Die Europäische Kommission, das Parlament und der Rat haben sich gemeinsam auf Maßgaben für Kritische Infrastrukturen (KRITIS) verständigt und diese in der NIS-Richtlinie dargelegt. Für die NIS-Richtlinie wurde in Deutschland im Jahr 2017 eine nationale Umsetzung in Form des NIS-Richtlinien Umsetzungsgesetzes geschaffen. Gleichzeitig wurde auf europäischer Ebene die Regulierung von IT-Sicherheit mit dem EU-Cybersecurity Act vorangetrieben. Der nunmehr veröffentlichte Entwurf für das IT-SiG 2.0i stellt diese Strukturen und Regeln vor grundlegende Veränderungen. Der Bereich der KRITIS wird ausgeweitet und es werden neue Bereiche und Sektoren mit einbezogen und Querschnittsanforderungen aufgesetzt, die bislang nicht unter die KRITIS-Regelungen fallen. Durch diese Form der Regulierung können Unklarheiten dahingehend entstehen, wie Verantwortung sowohl in einzelnen Sektoren als auch in der horizontalen Regulierung zugeschrieben werden kann.
Zusammenfassend kann festgehalten werden, dass die insbesondere in Artikel 1

des IT-SiG 2.0i niedergelegten Definitionen für die Anwendungsbereiche des IT-SiG in Bezug auf KRITIS unpräzise und daher problematisch sind. Zwar ist der Wunsch, Hersteller von Endgeräten und Entwickler von Software stärker zu verpflichten nachvollziehbar, die hier raufgeworfenen Regulierungsmaßgaben hingegen lösen die zuvor beschriebenen Unsicherheiten nicht für alle Beteiligten zufriedenstellend auf. Die aus den Maßgaben abgeleiteten Rechtsfolgen von den Auflagen für IT-Sicherheit, die zu erfüllen sind, bis hin zu zuständigen Aufsichtsbehörden sorgen bei Unternehmen für Rechts- und Planungsunsicherheit. Die Kohärenz mit europäischen Maßgaben ist nicht klar.

- **Infrastrukturen von besonderem öffentlichen Interesse**

Neben KRITIS werden außerdem Regelungen aufgeworfen, die auf Infrastrukturen bezogen werden, bei denen ein „besonderes öffentliches Interesse“ unterstellt wird. Dies ist nicht nur problematisch, wenn man die Kohärenz der IT-Sicherheitspolitik im europäischen digitalen Binnenmarkt beleuchtet, es wirft zudem die Frage auf, inwieweit sich durch die hier getroffenen Regelungen Auswirkungen auf das Regulierungsgefüge in der IT-Sicherheit (sektorale und horizontale Regelungen) ergibt. Darüber hinaus ist fraglich, inwieweit die hier vorgesehenen Regelungen für Presseverlage und andere Akteure in die Regelungssystematik passen und sich hier ein vergleichbares „besonderes öffentliches Interesse“ ergibt. Zusätzliche Unschärfe erhalten diese Begriffsbestimmungen dadurch, dass das BSI einzelne Akteure als relevant für die Regeln der IT-Sicherheitsregulierung einstufen kann, so dass das bisherige Prinzip der Schwellenwerte und Selbsteinschätzung aufgeweicht wird und falsche Akzente im Bereich der IT-Sicherheit gesetzt werden.

- **Ausrichtung der IT-Sicherheitspolitik / Aufstellung von IT-Sicherheitsbehörden**

Ein weiterer zentraler Aspekt ist die Frage, wie IT-Sicherheitsbehörden in Deutschland zukünftig aufgestellt sein sollen. Das IT-SiG 2.0i liefert hier Ansatzpunkte dafür, dass das BSI zukünftig zahlreiche neue Kompetenzen bekommen soll. Neben zusätzlicher Verantwortung im Bereich der staatlichen IT-Infrastrukturen soll das BSI insbesondere auch die Kontrolle der KRITIS-Sektoren bekommen. Hier kann das BSI zukünftig auch Ermittlungen auf Anwender- und Nutzerebene durchführen, die bis auf einzelne individuelle Nutzer heruntergebrochen werden können und Informationen über diese sammeln und verarbeiten. Inwieweit diese vorgesehene Bestandsdatenauskunft bei der Beseitigung von Störungen in Netzen hilfreich ist, ist unklar. Darüber hinaus darf das BSI in Zukunft auch direkt Anschlüsse und Endgeräte überprüfen, was zusätzliche Fragen nach der Art und Weise der Prüfung und dem Sinn einer solchen Maßnahme aufwirft.

- **Aufsicht über KRITIS oder Verwaltung des Betriebs von KRITIS**

Die Möglichkeit, für das BSI, Vertrauenswürdigkeitserklärungen von KRITIS-Betreibern einzufordern, ermöglicht zudem eine nachgelagerte Regulierung der eingesetzten Technologie. Die Rechtsfolgen für die

Vertrauenswürdigkeitserklärungen sind derzeit noch klärungsbedürftig. Ähnlich wie die unpräzisen Begriffsbestimmungen kann dies dazu führen, dass der Anwendungsbereich des Gesetzes unpräzise wird. Auch ist derzeit nicht klar, wie genau das BSI zukünftig mit Betreibern von KRITIS interagiert, wenn es ihnen die Ausgestaltung von Systemen zur Angriffserkennung vorgibt. Hier wird erkennbar, dass das BSI weniger die Aufsicht über den Einsatz von IT in KRITIS ausübt, sondern dazu befähigt wird, den Einsatz von Technologie in Unternehmen selbst zu beeinflussen und vorzugeben. Noch schwerwiegender ist die Anordnungsbefugnis, die dem BSI gegenüber Anbietern von Telekommunikationsdiensten eingeräumt wird. Die Regelung ist zu unbestimmt und weitgehend, sie betrifft sensible Maßnahmen im Bereich des Fernmeldegeheimnisses, des Datenschutzes und somit des Bereichs der persönlichen Lebensführung. Einer marktgetriebenen IT-Sicherheitswirtschaft, die sich dynamisch entwickeln soll, ist dies abträglich. Das Vertrauen in digitale Dienste, die auf KRITIS aufsetzen, kann so maßgeblich geschädigt werden. Zudem stellt die Anordnungsbefugnis einen Eingriff in die Freiheit der Anbieter von Telekommunikationsdiensten dar, in eigener Verantwortung Störungssituationen zu regeln. Ein störungsfreier Betrieb der eigenen Netze und Vertragstreue gegenüber Kunden ist in ihrem Interesse. Sie verfügen über bessere Kenntnisse ihrer Anlagen und Netze und sind daher auch eher imstande selbst angemessen auf Störungssituationen zu reagieren. Einer interventionistischen Regulierung, die diese Aspekte außer Acht lässt, bedarf es nicht.

- **Verhältnis zu anderen Sicherheitsfragen und Thematiken**

Besonders problematisch, da nicht im Gesetzesentwurf adressiert, ist das Verhältnis von BSI und der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), die im Auftrag weiterer Sicherheitsbehörden in IT-Systeme eindringen soll. Das Verhältnis der beiden Behörden zueinander sollte geklärt werden. Die bestehende Situation erzeugt Unsicherheit bei IT-Anbietern, die nicht wissen, ob die von ihnen gemeldeten Schwachstellen dann von Sicherheitsbehörden für Angriffe verwendet werden könnten und, wesentlich schwerwiegender, an wen solche Erkenntnisse und Informationen unter Umständen weitergegeben und gelangen könnten. Darüber hinaus ist bei den gewählten Maßnahmen auch nicht eindeutig klar, inwieweit sie reaktiv zur Beseitigung einer Störung eingesetzt / angeordnet werden können bzw. inwieweit damit auch Telekommunikationsdiensteanbieter dazu verpflichtet werden können im Auftrag des BSI angeschlossene bzw. erreichbare Teilnehmer aus dem Netz zu entfernen (Hackback). Bei all diesen Punkten bleibt allerdings offen, inwieweit das BSI für die in seiner Verantwortung bzw. auf seine Veranlassung hin durchgeführte Maßnahmen Verantwortung übernimmt. Eine Regelung zur Haftungsfreistellung für die verpflichteten Unternehmen ist in dem Entwurf nicht enthalten. Unklar ist in diesem Kontext auch, wie die verschiedentlich niedergelegten Meldepflichten für Datenabflüsse sich hier mit weiteren Forderungen an Diensteanbieter verhalten und ob aus diesen Meldungen weitergehende Forderungen abgeleitet werden können.

- **IT-Sicherheitskennzeichen und Kohärenz mit europäischer Gesetzgebung**

Mit den Plänen für ein IT-Sicherheitskennzeichen geht der Referentenentwurf für das IT-SiG 2.0i gegenüber der europäischen Regulierung in Vorleistung. Dort soll ein Rahmen für die Zertifizierung von IT-Produkten auf europäischer Ebene geschaffen werden. Das freiwillige IT-Sicherheitskennzeichen ist dementsprechend ein nationaler Alleingang. Positiv bleibt zu konstatieren, dass das Zeichen freiwillig ist. Gleichzeitig bleibt die Frage, inwieweit dieses Sicherheitskennzeichen am Ende im Gefüge des europäischen IT-Sicherheits-Zertifizierungsrahmens verortet werden kann. Zudem zeigt sich, dass der Begriff des Herstellers eines Produkts genauer betrachtet werden muss, da Informationstechnologie auf offenen Plattformen aufsetzt, so dass sich teilweise Wechselwirkungen ergeben, die nicht ohne weiteres nachvollzogen werden können. Es wäre daher sinnvoll, klarzustellen, dass das geplante IT-Sicherheitskennzeichen im Einklang mit dem durch den EU-Cybersecurity Act gesetzten Zertifizierungsrahmen entwickelt und umgesetzt wird.

- **Strafrechtliche Regelungen für Dienstebetreiber**

Mit dem IT-SiG 2.0i werden auch strafrechtliche Regelungen in die Debatte um IT-Sicherheit mit einbezogen. Ähnliche Diskussionen wurden bereits Anfang des Jahres im Bundesrat von verschiedenen Ländern initiiert. Vor diesem Hintergrund sind insbesondere die Regelungen problematisch, die Anbieter von neutralen und rechtlich nicht zu beanstandenden IT- und Telekommunikationsdienstleistungen kriminalisieren, die von Nutzern missbräuchlich zur Begehung von Straftaten verwendet werden. Anonymisierungs- und Verschlüsselungsdienstleistungen können teilweise dazu genutzt werden, ohne dass die Betreiber dies tatsächlich kontrollieren oder proaktiv eindämmen könnten. Die vom Innenministerium gewählte Formulierung ist dementsprechend nicht hinreichend präzise, um zu gewährleisten, dass auch bislang legale Dienste, die über ein hohes Maß an Sicherheit durch Verschlüsselung verfügen oder bestimmte Formen von Anonymisierungsdiensten wie VPN-Anbieter von dieser Regelung ausgenommen sind. Eine Schwächung von IT-Sicherheit und die Eingrenzung der anonymen Nutzung des Internets sind nicht hinnehmbar. Die Maßgaben der e-Commerce Richtlinie und die Vertraulichkeit elektronischer Kommunikation müssen hier zwingend berücksichtigt werden. Eine pauschale Kriminalisierung digitaler Dienstleistungen ist nicht akzeptabel. Die zusätzliche Anforderung aus Artikel 7 an Diensteanbieter und –betreiber, zukünftig auch bereits auf Anforderung von Behörden Daten bereits vor Zugriff ausländischer Behörden zu speichern und für die Beweissicherung bis zu 180 Tage bereitzuhalten, ist in diesem Sinne ebenfalls kritisch zu sehen.

- **Strafprozessuale Regelungen für Passwortbesitzer**

Der Entwurf des IT-SiG 2.0i sieht auch vor, dass zukünftig Personen, die über Passwörter oder andere Zugänge zu Diensten oder Profilen von Personen verfügen, strafrechtlich belangt werden können, wenn sie diese Ermittlungsbehörden nicht zur Verfügung stellen. Ein Zwang zur Preisgabe von Passwörtern oder Passphrases ist nicht akzeptabel. Damit werden das Vertrauen und die Sicherheit in die Nutzung von Diensten unterminiert. Weitergehenden Implikationen (Presserecht, anwaltlicher

oder seelsorgerischer Geheimschutz) trägt ein solcher Vorstoß nicht Rechnung und ist daher abzulehnen.

Über eco: Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.