Erste Analyse des neuen Entwurfs zum IT-SiG 2.0 aus dem Mai 2020: Wenig Neues, wenig Überraschendes

von Dr. Dennis-Kenji Kipker

Nach den politischen Kontroversen aus dem vergangenen Jahr, die sich in erheblichem Maße auch um den chinesischen Mobilfunkausrüster Huawei und das Thema 5G drehten, wurde der neue Entwurf für das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) mit Spannung erwartet. Der aktuelle Referentenentwurf aus dem BMI datiert auf den 07.05.2020 und ist mit 73 Seiten inklusive der Entwurfsbegründung etwas kürzer als die ursprüngliche Version mit 90 Seiten. Geändert werden die folgenden Vorschriften:

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG, Regelungsschwerpunkt)
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Außenwirtschaftsverordnung (AWV)

Inhaltlich ist Vieles beim Alten geblieben, mit einem Unterschied: der Erfüllungsaufwand in Form der Planstellen wird deutlich konkreter gefasst. Daraus wird schnell ersichtlich, dass das BSI mehr und mehr zu einer zentralen Behörde in der deutschen Verwaltungsinfrastruktur heranwächst. Dies dürfte sicher erneut die politischen Diskussionen um seine Selbstständigkeit beflügeln. Laut dem Entwurf zum IT-SiG 2.0 sind zur Umsetzung der einzelnen Neuregelungen insgesamt 583 Planstellen notwendig, unter anderem aus den folgenden Gründen:

- Neue Aufgaben zur Förderung des Verbraucherschutzes und der Verbraucherinformation in der Informationssicherheit
- Erweiterte Informationsaufgabe und Warnbefugnis im Hinblick auf Produkte
- Pflege und Weiterentwicklung sicherer (digitaler) Identitäten
- Kontrolle der Kommunikationstechnik des Bundes
- Erfüllung der Aufgabe der Meldestelle zur Sammlung von Informationen über Sicherheitslücken, Schadprogramme und IT-Sicherheitsvorfälle, um ein Gesamtlagebild zu erstellen
- Durchführung von Detektionsmaßnahmen in der Informationstechnik des Bundes, für die Netz- und Informationssicherheit und zum besonderen Schutz von Mitgliedern der Verfassungsorgane
- Auswertung behördeninterner Protokollierungsdaten

- Erweiterung des Adressatenkreises der schon bestehenden Mobile Incident Response Teams (MIRTs)
- Etablierung der Kommunikationsstruktur und Krisensteuerung für KRITIS
- Durchführung von Bestandsdatenabfragen für die Identifikation von Opfern eines Cyberangriffs
- Durchführung technischer Untersuchungen im Hinblick auf die IT-Sicherheit
- Unterstützung der Digitalisierungsvorhaben der Bundesregierung insbesondere in der Konzeptions- und Planungsphase
- Aufnahme weiterer Branchen in den Regelungsbereich des Gesetzes
- Vergabe der Vertrauenswürdigkeitserklärung
- Konzeption und Vergabe des IT-Sicherheitskennzeichens
- Erweiterung der Bußgeldvorschriften

Außerdem enthält die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) neue Aufgaben und damit ebenfalls weitere Planstellen.

Grundlegende Anforderungen sind gleich oder ähnlich

Grundlegende Anforderungen im neuen Entwurf sind, verglichen mit dem ersten Referentenentwurf aus dem Frühjahr 2019, gleich oder ähnlich geblieben, sodass das Gesetz seinen ursprünglichen Charakter grundsätzlich behält. Änderungen und oder Ergänzungen finden sich zuvorderst bei den Begriffsdefinitionen: So wird die Begriffsbestimmung für die Kommunikationstechnik des Bundes angepasst, und eine neue Definition für Protokollierungsdaten bestimmt. Ergänzt werden die Begriffsbestimmungen in § 2 BSIG durch zusätzliche Definitionen für IT-Produkte (Software sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte) und für Systeme zur Angriffserkennung. Zusätzliche Begriffsbestimmungen sollen außerdem für Kritische Komponenten im Sinne des BSIG und Unternehmen im besonderen öffentlichen Interesse eingeführt werden. Unter ersterem zu verstehen sind insbesondere solche IT-Produkte, die in KRITIS eingesetzt werden und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind – für TK-Netzbetreiber oder TK-Diensteerbringer werden diese Komponenten durch den Katalog nach § 109 Abs. 6 TKG näher bestimmt, alle anderen werden durch einen entsprechenden BSI-Katalog konkretisiert. Interessant sind überdies die Änderungen für die Unternehmen im besonderen öffentlichen Interesse, die durch den Entwurf vorgeschlagen werden. In der Entwurfsbegründung genannt werden u.a. Rüstungshersteller und Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen und Unternehmen, die einer Regulierung durch die Verordnung zum Schutz von Gefahrstoffen unterliegen. Die Unternehmen, die allgemein aufgrund ihrer

volkswirtschaftlichen und Bedeutung und insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichen Interesse sind, werden durch eine Rechtsverordnung näher bestimmt. Hier bleibt es also spannend.

Mehr Aufgaben und Befugnisse für das BSI

Der Entwurf sieht des Weiteren eine Ausdehnung der Aufgaben des BSI vor, zur Erteilung von Befugnissen, als Konformitätsbewertungsstelle im Bereich der IT-Sicherheit tätig zu sein, zur Wahrnehmung der Aufgaben als nationale Behörde für die Cybersicherheitszertifizierung gem. EU Cybersecurity Act (CSA), zur Beratung, Information und Warnung von staatlichen und privaten Stellen in Fragen der Informationssicherheit, zur Förderung der Verbraucherinformation und des Verbraucherschutzes, zur Wahrnehmung der Aufgaben als zentrale Stelle für die IT-Sicherheit, zur Vergabe vom Empfehlungen für Identifizierungs- und Authentisierungsverfahren und zur Bewertung solcher Verfahren sowie für die Entwicklung und Veröffentlichung eines Standes der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte. Insbesondere letztgenannte Aufgabenerweiterung dürfte interessant sein, da sie zukünftig entscheidend zur Ausfüllung dieses unbestimmten Rechtsbegriffs beitragen kann.

Absicherung der Kommunikationstechnik des Bundes

Im Hinblick auf die Unterstützung des BSI zur Sicherstellung der IT-Sicherheit in der Kommunikationstechnik des Bundes soll das BSI wohl seine umfassenden Befugnisse, die schon 2019 vorgeschlagen wurden, behalten. Dazu gehören Überprüfungs- und Kontrollbefugnisse, die Wahrnehmung der Aufgabe als allgemeine Meldestelle, oder die Auswertung und Speicherung von (behördeninternen) Protokolldaten. Ebenfalls geblieben, aber im Detail geändert wurde der § 5c BSIG-E, der die Sicherheit und Funktionsfähigkeit informationstechnischer Systeme im Falle erheblicher Störungen betrifft – hier ist nunmehr von einem „Gesamtplan für die Reaktionsmaßnahmen des Bundes“ die Rede. Selbiges gilt für die Befugnis zur Einholung einer Bestandsdatenauskunft nach § 5d BSIG-E, die zur Kontaktaufnahme zu Zwecken der IT-Sicherheit erforderlich ist. Die in § 7 BSIG-E angeordneten Warnpflichten für die Öffentlichkeit bestehen ebenfalls in nahezu unveränderter Form fort, und umfassen Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten, Warnungen vor Schadprogrammen, Warnungen im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten und Informationen über sicherheitsrelevante IT-Eigenschaften der Produkte. Auch geblieben ist die Vorschrift des § 7a BSIG „Untersuchung der Sicherheit in der Informationstechnik“, die es dem BSI zukünftig gestatten soll, auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt

vorgesehene IT-Produkte und Systeme zu untersuchen. Ein neu vorgeschlagener Abs. 3 ermöglicht es der Behörde, die Untersuchungsergebnisse unverzüglich an die zuständigen Aufsichtsbehörden des Bundes oder an das zuständige Ressort weiterzuleiten, falls diese die Informationen zur Aufgabenerfüllung benötigen. Ebenfalls keine nennenswerten inhaltlichen Änderungen ergeben sich für § 7b BSIG-E (Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit von Angriffsmethoden) und für § 7c BSIG-E (Detektion zum Schutz der Mitglieder der Verfassungsorgane). Ebenso entspricht § 8 BSIG-E (Vorgaben des Bundesamts) nahezu vollständig der ersten Entwurfsfassung.

Änderungen bei den KRITIS-Regelungen

Änderungen hingegen ergeben sich für § 8a BSIG-E, so wird u.a. der bisherige Abs. 1a aufgeteilt und ergänzt. So können KRITIS-Betreiber Prozesse vorsehen, um die Vertrauenswürdigkeit der Beschäftigten zu überprüfen, die in zentralen Bereichen tätig sind. Außerdem wird neuerdings eine Regelung vorgeschlagen, dass solche Daten, die im Rahmen des Einsatzes von Systemen zur Angriffserkennung erhoben wurden, von den Betreibern an die dafür zuständigen Behörden zu übermitteln sind. Ebenso wird eine vom ursprünglichen Entwurf abweichende Änderung von § 8a Abs. 3 BSIG aufgegriffen: So sollen KRITIS-Betreiber dem BSI zusätzlich eine Liste aller IT-Produkte übermitteln, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen von Bedeutung sind. Die Regelung zu KRITIS-Kernkomponenten, die noch in der ersten Entwurfsfassung vorlag, findet sich im aktuellen Entwurf aus Mai 2020 hingegen in dieser Form nicht wieder – dazu aber noch im Folgenden. Der Regelungsvorschlag aus 2019 sah an dieser Stelle des Gesetzes vor, dass derlei Komponenten nur von solchen Herstellern bezogen werden dürfen, die eine Vertrauenswürdigkeitserklärung abgegeben haben.

Für die Regelung der KRITIS-Meldepflicht soll § 8b BSIG nunmehr nicht nur ein neuer Abs. 3a angehängt werden, sondern eine ganze Reihe neuer Absätze, bis 3d. Der ursprüngliche Abs. 3a, der die Ersatzvornahme regeln soll, bleibt dabei bestehen. Abs. 3b und Abs. 3c regelt für Unternehmen im besonderen öffentlichen Interesse die Benennung einer Stelle, die zu den üblichen Geschäftszeiten erreichbar ist – je nach Unternehmenskategorie verpflichtend oder freiwillig. § 3d bestimmt, dass die Überprüfung von Beschäftigten, die in (sicherheits-) sensiblen Bereichen tätig sind, auch für die Unternehmen im öffentlichen Interesse gilt. Überdies werden über den ersten Entwurf aus 2019 hinausgehend zwei neue Absätze 4a und 4b vorgeschlagen, die die Meldepflicht von IT-Störungen der Unternehmen im besonderen öffentlichen Interesse betreffen. Eine Änderung des bisherigen § 8e BSIG (Auskunftsverlangen) sieht Einschränkungen des Informationsinteresses vor, soweit schutzwürdige Belange bzw. Betriebsinteressen dem entgegenstehen.

Die Entwurfsfassung aus Frühjahr 2019 sah im Folgenden die Einfügung der neuen §§ 8f bis 8h BSIG vor. Diese sollten die Anforderungen für Betreiber von Infrastrukturen im besonderen öffentlichen Interesse, die seinerzeit heftig diskutierte „Cyberkritikalität“ und die erweiterten Pflichten der Hersteller von IT-Produkten regeln. Der aktuelle Entwurf schlägt demgegenüber nur die Einfügung eines § 8f BSIG vor, der die Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse regelt und das Vorliegen eines IT-Sicherheitskonzepts bestimmt.

IT-Sicherheitskennzeichen bleibt vorerst

Im neuen Entwurf erhalten geblieben ist auch das IT-Sicherheitskennzeichen (in Abgrenzung zur Zertifizierung gem. EU CSA), das nach wie vor freiwillig ist und sich aus zwei Komponenten zusammensetzt, der Herstellererklärung und der BSI-Sicherheitsinformation (§ 9a BSIG-E).

Kein Einsatz von Kernkomponenten nicht vertrauenswürdiger Hersteller

Hingegen neu hinzu tritt der § 9b BSIG (Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller). Dieser kann so gesehen auch als Auffangtatbestand zur ursprünglich vorgesehenen Regelung zur Vertrauenswürdigkeitserklärung für KRITIS-Kernkomponenten gesehen werden. Bestimmt wird Folgendes:

- Der Einsatz einer kritischen Komponente gemäß der neuen Begriffsdefinition ist dem BMI vor Einbau anzuzeigen.
- Kritische Komponenten dürfen nur von solchen Herstellern eingesetzt werden, die eine Erklärung über die Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur abgegeben haben (sog. „Garantieerklärung“). Diese Garantieerklärung muss sich auch wie bisher auf die gesamte Lieferkette des Herstellers erstrecken. Einzelheiten werden wie bisher auch durch eine Allgemeinverfügung geregelt.
- Ein Hersteller einer kritischen Komponente ist unter anderem dann nicht vertrauenswürdig, wenn er unwahre Tatsachen behauptet hat, Sicherheitsüberprüfungen und Pen-Testing nicht angemessen unterstützt, bekannte Schwachstellen nicht unverzüglich beseitigt oder die kritische Komponente über Eigenschaften verfügt, die die IT-Sicherheit negativ beeinträchtigen können.

Die Untersagung des Einsatzes von kritischen Komponenten kann sich auch auf weitere Komponenten desselben Typs und Herstellers erstrecken.

Die Änderungen in § 10 BSIG betreffen nach wie vor Verordnungsermächtigungen des BMI.

Erweiterter Bußgeldrahmen in Anlehnung an die EU DS-GVO

Bei den Bußgeldvorschriften hält man auch beim neuen Entwurf nach wie vor an dem Rahmen für Bußgeldvorschriften fest, der durch den ersten Entwurf zum IT-SiG 2.0 an die EU DS-GVO angeglichen wurde: bis maximal 20.000.000 EUR oder bis zu 4% des gesamten weltweit erzielten Unternehmensumsatzes des vorangegangenen Geschäftsjahrs. Fraglich ist, inwieweit dieser nationale Vorstoß auch die weitergehende europäische Gesetzgebung zur IT-Sicherheit beeinträchtigen wird.

Kein neuer Straftatbestand der unbefugten Nutzung von IT-Systemen

Ebenfalls anzumerken ist, dass im Referentenentwurf aus Mai 2020 die ursprünglich vorgesehenen Änderungen im Strafgesetzbuch entfallen sind. Dies betrifft insbesondere die Schaffung des neuen Straftatbestands des § 200e StGB-E (unbefugte Nutzung informationstechnischer Systeme), der allein den Zugriff auf die Ressourcen eines IT-Systems unter Strafe stellte, ohne dass dieses notwendigerweise einen Schaden erleiden muss.