FACHBEREICH
SICHERHEIT – SCHUTZ
UND ZUVERLÄSSIGKEIT

Berlin, 9. Dezember 2020

Stellungnahme

des Fachbereichs Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V.

zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

des Bundesministeriums des Innern, für Bau und Heimat (BMI)

Ansprechpartner und Autor:
Bernhard C. Witt, Sprecher des GI-Fachbereichs „SICHERHEIT“, bcwitt@it-sec.de

Einleitung

Durch Veröffentlichung des Entwurfs eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) zum 02.12.2020 auf https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html wurde seitens des Bundesministeriums des Inneren, für Bau und Heimat dazu aufgerufen, Stellungnahmen bis zum 09.12.2020 per Mail an CI1@bmi.bund.de einzureichen.
Der Fachbereich Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V. nimmt diese Gelegenheit gerne wahr und nimmt zu dem Gesetzesentwurf vor allem zu Artikel 1, der die Änderung des bestehenden BSIG umfasst (im Folgenden daher als BSIG-E referenziert), Stellung. Die Stellungnahme erfolgt unter Berücksichtigung vorausgehender Beiträge folgender GI-Gremien:

- Präsidiumsarbeitskreis Datenschutz und IT-Sicherheit der GI, dieser Stellungnahme als Anlage beigefügt (https://gi.de/fileadmin/GI/Allgemein/PDF/2020-12-02_GI_PAK_IT-SiG_20_FINAL.pdf)
- GI-Fachgruppe Ada – Zuverlässige Software-Systeme, dieser Stellungnahme als Anlage beigefügt (https://gi.de/fileadmin/GI/Allgemein/PDF/2019-05-22_Stellungnahme_IT_Sicherheitsgesetz.pdf)
- GI-Fachgruppe Datenschutzfördernde Technik

Zu § 2 Abs. 14 BSIG-E: Unternehmen im besonderen öffentlichen Interesse

Insgesamt wird die Erweiterung der KRITIS-Verpflichteten begrüßt. Die Einbeziehung der größten Unternehmen gemäß ihres Wertschöpfungsbeitrags erscheint dagegen recht unspezifisch zu sein, im Hinblick darauf, dass es um den Schutz kritischer Infrastrukturen geht. Zielführender wäre es aus Sicht des GI-Fachbereichs Sicherheit, Zulieferer und Hersteller darunter einzuordnen, die innerhalb eines Sektors eine maßgebliche Bedeutung haben, d.h. mind. 50 % der im Sektor gelisteten kritischen Infrastrukturen mit Schlüsseltechnik bedienen. Das ist z.B. bei der Leittechnik so für Energie & Wasser - diese fallen aber nicht notwendigerweise unter die Wertschöpfungsdefinition. Dies könnte zugleich ein wertvoller Beitrag zur digitalen Souveränität darstellen.

Zu § 3 Abs. 1 Nr. 20 BSIG-E: Aufgabe des BSI im Kontext Stand der Technik

Gemäß Gesetzentwurf soll das Bundesamt für Sicherheit in der Informationstechnik die Aufgabe zugewiesen bekommen, einen Stand der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte zu entwickeln und zu veröffentlichen. Diese Aufgabe ist aus mehreren Gründen missverständlich:

1. Stand der Technik ist laut Gesetzesbegründung des bestehenden Gesetzes wie folgt definiert worden (siehe Drucksache 18/4096, S. 26): „Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen

lässt." Damit ist bereits festgelegt, was als Stand der Technik zu verstehen ist. Aus Sicht des GI-Fachbereichs Sicherheit zeigt jedoch der vorliegende Gesetzesentwurf, dass es zweckmäßig wäre, diese Definition als Legaldefinition in das BSIG ausdrücklich in § 2 als neuer Abs. 15 aufzunehmen.

2. Das BSI kann in diesem Sinne folglich keinen Entwicklungsstand entwickeln, denn dieser resultiert aus unternehmerischer und wissenschaftlicher Forschung und Entwicklung und hängt insbesondere im Einklang mit den weiteren Ausführungen aus der damaligen Gesetzesbegründung davon ab, was einschlägige internationale, europäische und nationale Normen und Standards ausweisen und welche Verfahren, Einrichtungen und Betriebsweisen mit Erfolg in der Praxis erprobt wurden. Insoweit kann es aus Sicht des GI-Fachbereichs Sicherheit allenfalls Aufgabe des BSI sein, diesen Stand der Technik zu beschreiben, nicht aber diesen zu entwickeln.

Zu § 7b, 8f, 9a und 9c BSIG-E: Neue Befugnisse des BSI

Im Zuge des Gesetzesentwurfs soll das Bundesamt für Sicherheit in der Informationstechnik weitreichende, neue Befugnisse erhalten: Es soll demnach

- Sicherheitsrisiken detektieren dürfen nach § 7b BSIG-E,
- in begrenztem Umfang Aufsichtsfunktionen übernehmen über Unternehmen im besonderen öffentlichen Interesse nach § 8f BSIG-E, die zumindest nach aktuellem Stand des Gesetzesentwurfs Unternehmen in Abhängigkeit ihres Wertschöpfungsbeitrags umfassen,
- die Cybersicherheitszertifizierung durchführen nach § 9a BSIG-E und
- Aufgaben zum digitalen Verbraucherschutz im Kontext des freiwilligen IT-Sicherheitskennzeichens erhalten.

Aus Sicht des GI-Fachbereichs Sicherheit sind das allesamt Aufgaben, die einer Beibehaltung der Zuordnung des BSI an das BMI entgegenstehen und es erfordern, dass das BSI als eigenständige oberste Bundesbehörde, vergleichbar zum Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, konstitutionell neu aufgestellt wird. Insoweit wird durch den GI-Fachbereich Sicherheit nachdrücklich eine entsprechende Änderung des § 1 BSIG empfohlen.

Zu § 7b BSIG-E: Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit

Oberstes Schutzziel im Rahmen von KRITIS ist bereits nach bestehendem § 8a BSIG die Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind. Aus Sicht des GI-Fachbereichs Sicherheit ist es daher zwingend erforderlich, dass durch die vom BSI selbst oder im Auftrag durchgeführten Portscans und vergleichbaren Tests die Funktionstüchtigkeit der kritischen Dienstleistung nicht gefährdet werden darf, was damit als ergänzendes Kriterium in § 7b BSIG-E aufzunehmen ist. Weitere Ausführungen hierzu, auch zur Notwendigkeit der Veröffentlichung von entsprechenden Erkenntnissen, sind in der beigefügten

Stellungnahme des GI-Präsidiumsarbeitskreises Datenschutz und IT-Sicherheit ausgeführt.

Zu § 8a Abs. 1b BSIG-E: Aufbewahrungspflicht von Daten zur Angriffserkennung und -nachverfolgung

Betreiber einer kritischen Infrastruktur sollen gemäß dem Gesetzentwurf 4 Jahre lang Daten zur Angriffserkennung und -nachverfolgung vorhalten. Das BSI selbst, welches entsprechende Daten auswertet, ist jedoch angehalten, diese nach § 5 Abs. 2 BSIG-E nur 1 Jahr lang zu speichern. Aus Sicht des GI-Fachbereichs Sicherheit ist die Frist für die Betreiber einer kritischen Infrastruktur damit ebenfalls auf 1 Jahr zu begrenzen, da längere Speicherfristen offensichtlich unnötig und damit unverhältnismäßig sind.

Zu § 9b BSIG-E: Untersagung des Einsatzes kritischer Komponenten

Neu aufgenommen werden soll eine an sich durchaus effektive Befugnis, den Einsatz kritischer Komponenten zu untersagen. Aus Sicht des GI-Fachbereichs Sicherheit fehlt es hier bisher angesichts des damit verbundenen sehr weitgehenden Eingriffes in Eigentumsrechte der Betreiber einer kritischen Infrastruktur einer präzisen rechtswirksamen Festlegung und einer ausreichend langen Übergangsfrist, zumal es sich im Kontext von kritischen Infrastrukturen hierbei überwiegend um solche Komponenten handeln dürfte, die über einen längerfristigen LifeCycle verfügen und die gesamte Zertifizierungslandschaft überhaupt erst noch aufgebaut werden muss. Eine derart weitreichende Kompetenz setzt zudem aus Sicht des GI-Fachbereichs Sicherheit voraus, dass damit eine ausreichende Gewaltenteilung sichergestellt ist, die zulassende und prüfende Kompetenzen differenziert, wie in der beigefügten Stellungnahme der GI-Fachgruppe Ada näher ausgeführt. Andernfalls zweifelt der GI-Fachbereich Sicherheit an der Verfassungsmäßigkeit einer solchen Regelung.

Ergänzende Empfehlungen:

Aus Sicht des GI-Fachbereichs Sicherheit wären neben den oben bereits aufgeführten Anpassungen in den §§ 1 und 2 BSIG folgende Regelungen mitaufzunehmen:

- Kritische Infrastrukturen sollten ausdrücklich gesetzlich dazu verpflichtet werden, einen ausreichend unabhängigen Informationssicherheitsbeauftragten (analog zur Funktion eines Datenschutzbeauftragten) zu benennen
- Die Bundesländer sollten dazu verpflichtet werden, näher zu verfolgen, welche kritischen Infrastrukturen auf ihrem Landesgebiet angesiedelt sind, weshalb das BSI zugleich über eine entsprechende Übermittlungsbefugnis von entsprechenden Registrierungsdaten verfügen sollte

Anlagen:

- Stellungnahme des Präsidiums-Arbeitskreises „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik e.V. (GI) zum dritten Referentenentwurf eines

Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 –IT-SiG 2.0) des Bundesministeriums des Innern, für Bau und Heimat (BMI) vom 02.12.2020

- Stellungnahme der Fachgruppe ADA – Zuverlässige Software-Systeme der Gesellschaft für Informatik e.V. zum Entwurf des Bundesministeriums des Innern, für Bau und Heimat für ein „IT-Sicherheitsgesetz 2.0“ vom 21.05.2019

Über den Fachbereich Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V.

Der GI-Fachbereich "Sicherheit -Schutz und Zuverlässigkeit" wurde im Februar 2002 gegründet und vernetzt zwei "Communities" miteinander: Während die „Safety-Community“ vor allem den Schutz der Umwelt vor IT-Systemen (beispielsweise Sicherheit des Menschen vor schwerwiegenden Systemfehlern in Flugzeugen, Kernreaktoren und Kraftwerken) sowie Fehlertoleranzmaßnahmen (z.B. Systemausfälle als Folge von Ermüdungserscheinungen, Softwarefehlern und Naturereignissen) im Blick hat, beschäftigt sich die „Security-Community“ hauptsächlich mit dem Schutz der IT-Systeme und ihrer Umgebung vor Bedrohungen von außen, insbesondere vor Gefahren, die von bösartigen Angriffen (durch Menschen) ausgehen. Der Fachbereich bietet ein Forum, in dem alle auf dem Gebiet der Sicherheit informationstechnischer Systeme arbeitenden Menschen ihr Fachthema, organisiert in Fachgruppen, wiederfinden. Neben der rein wissenschaftlichen Arbeit ermöglicht der Fachbereich einen fachlichen Austausch zwischen Wissenschaft und Praxis. Mehr Information über den Fachbereich Sicherheit der GI kann der Webseite https://fb-sicherheit.gi.de/ entnommen werden.

Über die Gesellschaft für Informatik e.V.

Die Gesellschaft für Informatik e.V. (GI) ist mit rund 20.000 persönlichen und 250 korporativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum und vertritt seit 1969 die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Gesellschaft und Politik. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.

Die GI-Mitglieder binden sich an die Ethischen Leitlinien für Informatikerinnen und Informatiker der Gesellschaft für Informatik e.V.: https://gi.de/ethische-leitlinien