GESELLSCHAFT
FÜR INFORMATIK

Berlin, 2. Dezember 2020

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)

Jüngst wurde der dritte Referentenentwurf des IT-SiG 2.0 veröffentlicht, der die deutsche IT-Sicherheitsgesetzgebung in Einklang mit der neuen deutschen Cybersicherheitsstrategie bringen soll, die voraussichtlich zur Jahresmitte 2021 verabschiedet wird. Das Gesetzgebungsverfahren zum IT-SiG 2.0, dessen Erwägungen auf den BSI-Befugniserweiterungen und den Regelungen für Kritische Infrastrukturen des ersten IT-Sicherheitsgesetzes von 2015 fußen, dauert bereits seit über eineinhalb Jahren an. Zu einer Veröffentlichung einer ersten Entwurfsfassung kam es im April 2019, die zweite Fassung des Referentenentwurfs wurde im Mai 2020 publiziert. Zuletzt wurde das Gesetzgebungsverfahren immer wieder verzögert, was zuvorderst auf die politische Auseinandersetzung um „kritische Kernkomponenten" zurückzuführen ist, die eine erhebliche Relevanz für die öffentliche Sicherheit entfalten. Hierunter sind im Allgemeinen solche Komponenten zu verstehen, die für Kritische Infrastrukturen aufgrund ihrer Steuerungsfunktion eine besondere Relevanz besitzen.

Der gegenwärtige Entwurf zum IT-SiG 2.0 enthält eine Vielzahl begrüßenswerter Neuerungen, die das disziplin- und staatenübergreifende Zusammenwirken zur Verbesserung der IT-Sicherheit befördern sollen. Auch vor dem Hintergrund der in verschiedenen Wirtschaftszweigen teils „erzwungenen" Digitalisierung wird die politische, gesellschaftliche und wirtschaftliche Relevanz des Themas deutlich. Begrüßenswert ist überdies, dass insbesondere auch der verbraucherschützende Aspekt der Regelungsvorschläge im Vordergrund steht, um digitale Kompetenz zu fördern und digitaler Sorglosigkeit entgegenzuwirken.

Gerade aber mit Blick auf die digitale Souveränität und die IT-Sicherheitsregulierung in der Europäischen Union enthält der Referentenentwurf Verbesserungs- und Überarbeitungspotenzial. Begonnen beim Thema Verbraucherschutz stellt sich die Frage, inwieweit das freiwillige IT-Sicherheitskennzeichen gegenüber einer EU-Konformitätserklärung, die nach dem EU Cybersecurity Act ebenfalls freiwillig ausgestaltet ist, deutlich abgegrenzt werden kann. Durch die in diesem Zusammenhang zusätzlich vorgeschlagene Befugnis des BSI, eigenständige technische Richtlinien zu erlassen, wird der europäische Marktzugang fragmentiert und erschwert. Dies kann nicht im Sinne der Strategie eines einheitlichen digitalen EU-Binnenmarktes sein, und gerade für KMU wird es immer schwieriger, hier einen Überblick über den Regulierungsdschungel zur IT-Sicherheit zu behalten. Dadurch stellt sich nicht zuletzt die Frage, ob das freiwillige IT-Sicherheitskennzeichen in der Anwendungspraxis tatsächlich im rechtspolitisch beabsichtigten Maß von Unternehmen und Verbrauchern gleichermaßen angenommen wird – oder hier nicht im Gegenteil inflationär mit Gütesiegeln umgegangen wird, die damit letztlich wiederum an Wirkkraft verlieren.

Ein weiterer Aspekt betrifft die verschleppte Debatte um die digitale Souveränität, die als allgemeines politisches und technologierelevantes Problem zunehmend auch im Bereich der IT-Sicherheit ausgetragen wird. Zwar ist es grundsätzlich nachvollziehbar, wenn an den Einsatz der gesetzlich definierten „kritischen Komponenten" besondere

Sicherheitsanforderungen angelegt werden – in der Sache ist der vorgelegte Entwurf aber nicht zielführend, da mit dem Regelungsvorschlag ein vornehmlich politisch-volkswirtschaftliches Problem in das Recht und damit in die technisch-organisatorische Umsetzung übertragen wird. Der im Entwurf nach wie vor geforderte, uneingeschränkte Nachweis von Lieferketten betrifft damit letzten Endes auch keine Frage der digitalen Souveränität, da sie die Technologieentwicklung in Deutschland und der EU selbst nicht aufgreift.

Ein weiterer, schon in den zuvor enthaltenen Entwurfsfassungen aufgegriffener Kritikpunkt betrifft die Befugnis des BSI, aktiv nach Sicherheitslücken zu suchen. Hiervon umfasst sind beispielsweise Portscans oder das Überprüfen von Passwörtern. Wird durch eine Detektionsmaßnahme des BSI eine Sicherheitslücke erkannt und stehen überwiegende Sicherheitsinteressen nicht entgegen, sind grundsätzlich die für das informationstechnische System Verantwortlichen darüber zu informieren und auf Abhilfemöglichkeiten hinzuweisen. Berechtigte Kritik betrifft in diesem Zusammenhang die Frage, ob durch derartige Maßnahmen Systemausfälle und Beeinträchtigungen in zuvor ordnungsgemäß funktionierenden IT-Systemen hervorgerufen werden können. Angedacht werden sollte deshalb in jedem Falle eine Warn- und Hinweispflicht an den jeweiligen Betreiber vor Durchführung aktiver Detektionsmaßnahmen. Unerklärlich ist, dass dem BSI bekannt gewordene Sicherheitslücken nur veröffentlicht werden können, nicht jedoch müssen. Unverzichtbar für das Sicherheitsniveau von Unternehmen und Bürgern ist vielmehr die unverzügliche Veröffentlichung der dem BSI bekannt gewordenen Angriffspunkte (Sicherheitslücken). Diese Notwendigkeit ist erneut deutlich geworden bei Angriffen auf Einrichtungen des Gesundheitswesens.

Begründung und Gesetzestext sollten redaktionell überarbeitet werden; z.B. wird nicht deutlich, ob und wo der Gesetzgeber einen Unterschied zwischen dem umgangssprachlichen Begriff Schwachstelle und dem IT-Begriff Sicherheitslücke sehen soll.

Erneut fordern wir das Bundesamt für Sicherheit in der Informationstechnik (BSI) als weisungsunabhängige Behörde zu etablieren, um das IT-Sicherheitsniveau Deutschlands langfristig zu stärken.

Über den Präsidiumsarbeitskreis Datenschutz und IT-Sicherheit der Gesellschaft für Informatik (GI)

Sicherheits- und Datenschutzaspekte werden stark zunehmend von Gesellschaft, Unternehmen und auch der Politik adressiert. In der GI befassen sich eine Vielzahl von Fachbereichen (u.a. Sicherheit – Schutz und Zuverlässigkeit) mit diesen Themen, so dass das Präsidium den alle Fachbereiche übergreifenden Arbeitskreis Datenschutz und IT-Sicherheit mit der Bearbeitung beauftragt hat. Weitere Informationen finden Sie unter https://pak-datenschutz.gi.de/

GESELLSCHAFT
FÜR INFORMATIK

Über die Gesellschaft für Informatik e.V. (GI)

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.