GESELLSCHAFT
FÜR INFORMATIK

Berlin, 15. Juli 2022

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

zur Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat vom 12.07.2022

Die Gesellschaft für Informatik e.V. (GI) begrüßt, dass das Bundesministerium des Inneren und für Heimat mit der Ausarbeitung der Cybersicherheitsagenda das Thema Cybersicherheit strategisch und mit konkreten Maßnahmen operationalisiert angehen möchte.

In dieser Stellungnahme sollen die einzelnen Arbeitsabschnitte der Agenda bewertet und kommentiert werden. Grundsätzlich lässt die Agenda in vielen Fragen jedoch die nötige Konkretheit vermissen, sodass eine präzise Bewertung und Einordnung kaum möglich sind.

Ad 1. Cybersicherheitsarchitektur modernisieren und harmonisieren

Die geplante Bündelung von Zuständigkeiten für Cybersicherheit auf Bundesebene in den Aufgabenbereich des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist grundsätzlich ein sinnvoller Schritt in Richtung einer verantwortlicheren Gefahrenabwehr. Gleichzeitig sollte ein Kapazitätsaufbau auch auf Seiten der Länder vorangetrieben werden, um die vielschichtige Bedrohungslage zu adressieren.

Ebenso ist die unabhängigere Aufstellung des BSI zu begrüßen. Die Formulierung in der Agenda bleibt hierbei jedoch äußerst vage, sodass unklar bleibt, wie die konkreten Aufgaben verteilt werden sollen. Die Unabhängigkeit des BSI von politischer Einflussnahme ist zudem wichtig, um die Glaubwürdigkeit der Tätigkeiten des BSI, insbesondere auch von Warnungen nach §7 BSI-Gesetz zu gewährleisten. Deshalb plädieren wir dafür, das BSI als unabhängige Behörde ähnlich dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) aufzustellen und aus der Aufsicht des BMI zu herauszulösen.

Ad 2. Cyberfähigkeiten und digitale Souveränität der Sicherheitsbehörden stärken

Die GI begrüßt die Etablierung eines wirksamen Schwachstellenmanagements. Dieses sollte zwingend den verantwortungsvollen Umgang mit 0-Day-Schwachstellen und -Exploits im Sinne einer Responsible Disclosure beinhalten.

Der Ausbau und die Stärkung technischer Ermittlungs- und Analysefähigkeiten und -instrumente bei den Sicherheitsbehörden sollte sich auf nicht-intrusive Maßnahmen beschränken. Zwar betonte Ministerin Faeser auf der Pressekonferenz zur Cybersicherheitsagenda, dass „Hackbacks“ ungewollt seien. Die entsprechenden Formulierungen der Agenda bleiben in diesem Punkt jedoch zu vage. Weitere Ausarbeitungen sollten klarstellen, dass der Fokus der anvisierten Befugnisse auf Aufklärung liegt und diese keine intrusiven Maßnahmen umfassen.

Dies sollte auch Berücksichtigung finden, wenn die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) endlich auf eine gesetzliche Grundlage gestellt werden sollte.

Bei Ausbau und Modernisierung der Ermittlungsfähigkeiten und -instrumente des Bundeskriminalamtes (BKA) und der Bundespolizei gilt es darauf zu achten, dass diese tatsächlich zu den mit der Agenda anvisierten Verbesserungen der Cybersicherheit im Sinne der Gefahrenabwehr beitragen. Befugnisse in der Datensammlung- und Auswertung könnten hier kontraproduktiv wirken.

Ad 3. Cybercrime und strafbare Inhalte im Internet bekämpfen

Schweren Straftaten wie sexualisierter Gewalt gegen Kinder und Jugendliche sowie Erpressung mithilfe von Ransomware ist entschieden entgegenzutreten. Sie sind allerdings sowohl technisch als auch rechtlich völlig unterschiedlich zu bewerten und zu behandeln. Ebenso wie die Bekämpfung von Hasskriminalität und Extremismus in sozialen Medien hat sexualisierte Gewalt gegen Kinder und Jugendliche im digitalen Raum wenig mit Cybersecurity zu tun.

Bei der Arbeit an diesen Zielen, insbesondere im Zusammenhang mit dem geplanten EU-weiten Rechtsrahmen ist darauf zu achten, dass neue Befugnisse nicht die Cybersicherheit der europäischen Wirtschaft, Verwaltung und Bürger*innen gefährden, etwa indem wirksame Verschlüsselungstechnologien umgangen werden. Wirksame Verschlüsselung stellt einen zentralen Baustein einer effektiven Cybersicherheitsarchitektur dar.

Ad 4. Cybersicherheit der Behörden des Bundes stärken

Die GI begrüßt ausdrücklich die Etablierung des Grundsatzes „security by design and by default“ in der Bundesverwaltung. Auch hier bleibt allerdings unklar, wie dies operationalisiert werden soll.

Auch hinsichtlich der Investition in Quantencomputing beim BSI bleibt unklar, was genau gemeint ist. Während Investitionen in eine Quantencomputer-resistente Post-Quanten-Kryptographie grundsätzlich sinnvoll erscheinen, sollte auch die Quantentechnologie nicht für intrusive Maßnahmen eingesetzt werden.

Ad 5. Cyber-Resilienz Kritischer Infrastrukturen stärken

Hinsichtlich der Resilienz der Kritischen Infrastruktur fehlt es an konkreten Erläuterungen, wie die IT-Lieferketten besonders geschützt werden sollen. Ebenso bleibt unklar, was unter der der Einrichtung von Awareness und Cyber-Resilienz-Projekten zu verstehen ist.

Ad 6. Schutz ziviler Infrastrukturen vor Cyberangriffen

Eine zentrale Informationsplattform „BSI Information Sharing Portal“ kann ein sinnvoller Baustein zur Bündelung der Informationsangebote sein. Zielsetzung und Konzeption des „zivilen Cyberabwehrsystems“ (ZCAS) sind jedoch zu unkonkret, als dass das Vorhaben bewertet werden könnte.

Mit Blick auf den Schutz ziviler Infrastrukturen sollte insbesondere auf die zunehmende Verbreitung von Internet-of-Things-Geräten ein größeres Augenmerk gelegt werden. Hier gilt es die langfristige Unterstützung der Geräte mit Sicherheitsupdates regulatorisch sicherzustellen.

Ad 7. Digitale Souveränität in der Cybersicherheit stärken

Die Stärkung der deutschen Cybersicherheitsforschung zur Erhöhung der Resilienz ist zu begrüßen. Gleichzeitig sollte anerkannt werden, dass das Thema der digitalen Souveränität zu lange vernachlässigt wurde, um nun allein durch Fördermittel die notwendigen Innovationen für Cybersicherheit erzielen zu können.

Technologiesouveränität im 5G- und 6G-Bereich kann ausschließlich mittel- bis langfristig erreicht werden, wenn jetzt in den dafür notwendigen Kompetenzaufbau von Fachkräften durch die universitäre Ausbildung investiert wird. Die entsprechende Lehre sollte durch die Förderung von Open-Source-Hardwarefertigung unterstützend flankiert werden, die eine praxisnahe Beschäftigung mit der Materie erlaubt und Innovation unterstützt.

Eine Erweiterung von Prüfmöglichkeiten im Hinblick auf die Vertrauenswürdigkeit von Herstellern und kritischen Komponenten bei KRITIS-Betreibern könnte grundsätzlich unterstützend wirken, müsste dafür jedoch konkretisiert werden.

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

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. 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.