GESELLSCHAFT
FÜR INFORMATIK

Berlin, 16. Juni 2021

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

zum Entwurf für die Cybersicherheitsstrategie 2021 (CSS) mit Stand 10.06.2021

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

Vorbemerkung: Angemessene Fristen für die Kommentierung von Gesetzesentwürfen und Strategiepapieren der Bundesregierung und ihrer Bundesministerien

Expertise benötigt Zeit. Unser Anspruch ist, Ihnen fundierte Rückmeldung aus unseren jeweiligen Fachgebieten zu den Gesetzgebungsvorhaben zu liefern. Die Einbeziehung unserer Fachexpert*innen benötigt jedoch immer einen ausreichenden Vorlauf. Dies gilt insbesondere für Organisationen wie die Gesellschaft für Informatik e.V. (GI), die auf dem Engagement Ehrenamtlicher fußen. Uns ist es rein organisatorisch nur schwerlich möglich, eine fundierte Stellungnahme innerhalb von vier Werktagen auszuarbeiten.

Im Sinne der in § 47 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) festgelegten „möglichst frühzeitigen“ Zuleitung an die Verbände, erwarten wir, künftig mindestens vier Arbeitswochen für die Anfertigung von Stellungnahmen eingeräumt zu bekommen. Die Bemessung der Frist sollte sich zudem an der Länge eines Entwurfes orientieren. Denkbar wäre eine Festschreibung von je einer Woche für je 50 Seiten Entwurfsdokument, nicht jedoch weniger als vier Wochen.

Aus den genannten Gründen beschränkt sich unsere Stellungnahme auf die folgenden zwei Feststellungen:

Zu 8.3.8 Den verantwortungsvollen Umgang mit 0-day-Schwachstellen und Exploits fördern

Die GI begrüßt, dass es ein ausdrückliches Ziel der CSS ist, ein „verbindliches Vorgehen [zu] etablier[en], das den verantwortungsvollen Umgang mit 0-day-Schwachstellen und Exploits regelt“ und den „Konflikt zwischen IT-Sicherheit und nachrichtendienstlicher Aufklärung, Gefahrenabwehr sowie Strafverfolgung“ (S. 89) adressiert.

Ein verantwortungsvoller Umgang mit 0-day-Schwachstellen im Sinne der IT-Sicherheit der deutschen Unternehmen und Bürgerinnen und Bürger kann jedoch nur darin bestehen, bekannt gewordene Sicherheitslücken im Sinne einer Responsible Disclosure schnellstmöglich zu veröffentlichen.

Das BSI sollte daher zu einer entsprechenden Veröffentlichung von Schwachstellen verpflichtet werden. Die genaue Verfahrensweise sollte sich an den etablierten Verfahrensweisen einer Responsible Disclosure orientieren, d.h. den verantwortlichen Stellen muss ausreichend Gelegenheit und umfassend Information zur umgehenden Beseitigung der Schwachstellen gegeben werden.

Zu 8.3.9 Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung gewährleisten

Mit Verweis auf die aktuelle Forschung im Bereich IT-Sicherheit lehnen wir die Formulierung „Sicherheit trotz Verschlüsselung“ als irreführend ab. Wie im selben Dokument unter 8.1.9 bemerkt, stellt Verschlüsselung die „Voraussetzung eines souveränen und selbstbestimmten Handelns“ dar und sollte daher auch nicht zu Gunsten anderer rechtmäßiger Ziele untergraben werden.

Eine absichtliche oder gar gesetzlich vorgeschriebene Schwächung von Sicherheitstechnologien zugunsten einer staatlichen Eingriffsmöglichkeit ist erstens nicht kontrollierbar, d.h. es darf davon ausgegangen werden, dass derartige „Hintertüren“ auch zu nicht legitimen Zwecken (Industriespionage, Ausspähen von Berufsgeheimnisträgern) von Privatpersonen und ggf. sogar Regierungen ausgenutzt werden können.

Zweitens führt insbesondere die Schwächung von kryptographischen Verfahren, die Grundlage der Verschlüsselung sind, zu einem Verlust an Integrität, Zurechenbarkeit und Unabstreitbarkeit, was zu einem gravierenden Verlust an Vertrauen in die digitale Kommunikation generell führen wird und nicht vereinbar ist mit dem Ziel, bis 2022 staatliche Verwaltungsleistungen im Kontext des Onlinezugangsgesetzes (OZG) den Bürgerinnen und Bürgern sicher und zuverlässig anzubieten.

Drittens ist es ungeachtet einer etwaigen staatlich angeordneten Schwächung von Verschlüsselung technisch heute unkompliziert und sehr unauffällig möglich, zusätzlich starke Verschlüsselung einzusetzen oder gar auf sogenannte steganographische Verfahren auszuweichen, welche nicht nur den Inhalt einer geheimen Nachricht, sondern sogar deren Existenz verschleiern. Kriminelle werden sich nicht scheuen, auch solche Verfahren einzusetzen, zumal diese heute auch ohne technischen Sachverstand frei verfügbar sind, wenngleich sie zumeist noch zusätzlichen Nutzungsaufwand verursachen. Eine staatliche Regulierung von Verschlüsselung würde Anreize zur Weiterentwicklung solcher Schutztechniken bis hin zu deren Integration in Messenger-Apps und vergleichbare Kommunikationsmittel setzen.

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.