Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)127

25.01.2023

Öffentliche Anhörung, Bundestagsausschuss für Digitales

„Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“

Ammar Alkassar
Ehemaliger Bevollmächtigter des Saarlandes für Innovation und Strategie
sowie CIO der Landesregierung

Berlin, den 25. Januar 2023

1) **Im Koalitionsvertrag haben die Regierungsparteien vereinbart, dass sie „einen strukturellen Umbau der IT-Sicherheitsarchitektur“ einleiten und das „Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger“ aufbauen und es als „zentrale Stelle im Bereich IT-Sicherheit“ ausbauen wollen.**

Wie sollte die Cybersicherheitsarchitektur auf nationaler und europäischer Ebene ausgestaltet werden, um effektiver, wirksamer und widerspruchsfreier aufgestellt zu sein und wo bedarf es einer Neuordnung oder auch Bündelung der Kompetenzen zwischen Bund, Ländern und der Europäischen Union und bedarf es auch angesichts der aktuellen Herausforderungen einer Diskussion über innere und äußere Sicherheit und der diesbezüglichen Kompetenzen und Grenzen? Welche anderen Akteure neben dem BSI (also etwa Cyber-Abwehrzentrum, Nationaler Cyber-Sicherheitsrat, ZITiS), die in Deutschland für Cybersicherheit zuständig sind, sollten reformiert werden und wie?

Zunächst kann festgehalten werden, dass die Aufstellung der deutschen Cybersicherheitsarchitektur sich im Grundsatz weitestgehend bewährt hat und sich auch im internationalen Vergleich als Erfolgsmodell sehen lassen kann.

Dies betrifft insbesondere das BSI, das sich seit seiner Gründung vor 30 Jahren zu einem international und national anerkannten Kompetenzträger für IT-Sicherheit entwickelt hat.[1] Insbesondere die strategische Trennung der nationalen Cybersicherheitsbehörde von nachrichtendienstlichen Aufgaben hat ganz wesentlich zu einer starken Vertrauensstellung und zu einer hohen Wertschätzung auch innerhalb der Zivilgesellschaft beigetragen. Gerade diese Vertrauensstellung und die zweifelsfreie Integrität der Behörde ist eine ganz wesentliche Grundlage für die erfolgreiche Erfüllung der Aufgaben einer Cybersicherheitsbehörde. Das zeigt sich besonders deutlich im Vergleich mit anderen nationalen Cybersicherheitsbehörden, die einer anderen Tradition folgen, beispielsweise in den Vereinigten Staaten oder im Vereinigten Königreich.

Daher sollte die Weiterentwicklung der Cybersicherheitsarchitektur die Erfolgsgrundpfeiler nicht verlassen und hierauf aufbauen.

Der im Koalitionsvertrag angestrebte Ausbau des BSIs zu einer zentralen Stelle wird nachdrücklich begrüßt, auch die damit einhergehende stärke Selbständigkeit in den Zentralstellenfunktionen. Ziel muss die eigenständige Erbringung von Leistungen für Bund und Länder sowie ihre nachgeordneten Einrichtungen sein. Eine Dezentralisierung oder Dopplung der Aufgaben des BSI auf Landesebene, beispielsweise durch die flächendeckende Errichtung von Landesämtern für die Sicherheit in der Informationstechnik erscheint hingegen kontraproduktiv.

Eine effiziente Gewährleistung von IT-Sicherheit kann nur in einem bundesweit harmonisierten Vorgehen sichergestellt werden. Die regionale Stärkung des BSI durch regionale

[1] Martin Schallbruch: "Mehr Unabhängigkeit für das BSI? Aufgaben und Steuerung des Bundesamtes für Sicherheit in der Informationstechnik", DuD • Datenschutz und Datensicherheit 4 | 2021, https://doi.org/10.1007/s11623-021-1424-3

Standorte mit dedizierten Fokusgebieten (wie Künstliche Intelligenz im Saarland[2]) kann den Wissenstransfer, die Talentakquise und die gesellschaftliche Verankerung stärken.

Die ebenfalls seit geraumer Zeit diskutierte und im Koalitionsvertrag aufgegriffene Frage nach einer Stärkung der **„Unabhängigkeit des BSI“** ist hingegen schwieriger zu bewerten.

Grundsätzlich gab es in der Frage der Führung des BSI durch das BMI auch in der Vergangenheit immer wieder Konfliktlinien, vornehmlich, wenn die Position des BSI-Präsidenten durch starke externe Persönlichkeiten besetzt werden. Aber gerade diese Persönlichkeiten haben maßgeblich zur positiven Entwicklung des BSI beigetragen, zu einer gewachsenen (politischen) Rolle und zu einer Stärkung des Vertrauens in die Institution durch Wirtschaft und Zivilgesellschaft.

Gleichzeitig hat das BMI als Aufsicht führendes Ministerium die Stärkung des BSI aktiv begleitet, maßgeblich unterstützt und politisch verantwortet. Die beständig erweiterten und gesetzlich festgeschrieben Zuständigkeiten des BSI und infolge dessen auch das Ausweiten von Haushaltsmitteln und Planstellen wären ohne ein starkes und fachlich versiertes BMI vermutlich nicht in dieser Geschwindigkeit möglich gewesen. Und was in der politischen Diskussion oftmals unberücksichtigt bleibt: Das BMI hat das BSI auch durch eine Vereinnahmung durch Interessen anderer Sicherheitsbehörden geschützt und die breite Ausrichtung der IT-Sicherheit als gesamtgesellschaftliche Aufgabe nachhaltig unterstützt.

Die in der Diskussion um eine größere Unabhängigkeit des BSI verbleibenden Argumente beziehen sich auf ein (tatsächliches oder vermeintliches) Mikromangement der nachgeordneten Behörde durch die vorgesetzte sowie ein (vermeintlicher) Vertrauensverlust, da die vorgesetzte Behörde auch die (Fach-)Aufsicht über Behörden führt, zu deren Auftragserfüllung die Schwächung von IT-Sicherheit gehöre. Gerade letzteres lässt sich nicht bestätigen und das BMI führt gleichzeitig auch Behörden, die gegenseitig einem Trennungsgebot unterliegen.

Vorschläge, das BSI ähnlich zum Modell des Bundesbeauftragten für den Datenschutz aus der Exekutive herauszulösen, sind skeptisch zu sehen, da die Cybersicherheitspolitik heute schon kein rein fachlich-administrative Aufgabe ist, sondern Gegenstand demokratisch-politischer Willensbildung ist und in der Verantwortung von (politischem) Regierungshandeln steht. Mehr noch: In Zukunft wird die Digitalisierung und die Cybersicherheit als wichtige Gestaltungselemente politischen Handelns eine noch größere Bedeutung erlangen und zu einem Kernbestandteil des Ressorts werden, in dem diese Aufgaben politisch verantwortet werden. Die Frage nach dem „richtigen“ Ressort ist dabei weniger maßgeblich, viel gewichtiger ist es, die Kompetenzen nicht weiter zu verteilen und deren starke Bündelung und eine Konzentration zentraler Entscheidungsverantwortung in wenigen Ressorts.

[2] https://www.bsi.bund.de/DE/Das-BSI/BSI-Standorte/Stuetzpunkt/saarbruecken_node.html

Nationale Stiftung Cybersicherheit: Eine Möglichkeit, den Konflikt um eine unabhängigere Cybersicherheitsbewertung zu erhalten ist die Schaffung einer eigenständigen Institution[3], die nur einer Rechtsaufsicht unterliegt und ähnlich zur Stiftung Wissenschaft und Politik (BK) oder zum Bundesinstitut für Risikobewertung (BMEL) eigenständige und fachlich unabhängige Bewertungen im Zusammenhang mit der Cybersicherheit erbringt.

Nationaler Cyberabwehrzentrum (NCAZ): Das NCAZ ist derzeit im Wesentlichen eine Informationsdrehscheibe aller mit der Cyberabwehr befassten Einrichtungen des Bundes und einiger Länder. Das NCAZ hat keine operativen Befugnisse. Der im Jahr 2020 mit der „AG Zukunftsbild“ gestartete Weiterentwicklungsprozess orientiert sich dabei an der „Stärkung der Lagefähigkeit des NCAZ, Intensivierung der interdisziplinären, operativen Fallbearbeitung, Forcierung der operativen und strategischen Berichterstattung, Optimierung von Abläufen und Prozessen inklusive Controlling und Wirkungskontrolle, die Etablierung neuer Zusammenarbeitsformate, die weitere Stärkung der Krisenreaktionsfähigkeit des NCAZ sowie die Einbindung weiterer Stellen.“[4] Damit ist auch weiterhin keine operative Rolle vorgesehen.

Dies scheint den Anforderungen angemessen. Allerdings sollte im Krisenfall eine Behörde die operative Leitung übernehmen. Dies kann nach hiesiger Einschätzung nur das BSI sein. Derzeit stellt der BND den Koordinator, BSI und KdoCIR[5] jeweils die Stellvertreter.

Nationales IT-Lagezentrum: Das beim BSI 24/7 betriebene IT-Lagezentrum erfasst kontinuierlich für die Cybersicherheit relevante Entwicklung und bewertet diese. Die Bundeswehr ist hier systematisch eingebunden. Ein weiterer Ausbau des Lagezentrums mit dem Ziel ein Echtzeitlagebild für alle staatlichen Ebenen und kritischer Infrastrukturen, erscheint geboten.

Nationaler Cyber-Sicherheitsrat (NCSR): Gerade im Hinblick auf die fortschreitende Digitalisierung in Staat, Wirtschaft und Gesellschaft und deren Bedeutung für die weitere Entwicklung Deutschlands in nahezu allen Lebensfeldern, ist die Cybersicherheit schon lange kein technologisches Trendthema mehr. Die langfristige strategische Aufstellung auf den Ebenen des Schutzes digitaler Werte und deren Infrastrukturen sowohl im staatlichen Bereich, der Wirtschaft aber auch unmittelbar der Bürger sind genauso zu berücksichtigen wie deren industrie- oder verteidigungspolitische Bedeutung.

Hierfür fehlt es an einem übergreifenden Gremium, in dem Politik, Verwaltung, Industrie, Wissenschaft und die IT-Sicherheitswirtschaft gemeinsame Ziele vereinbaren und in ihren jeweiligen Bereichen umsetzen.

Spätestens mit der Cyber-Sicherheitsstrategie von 2016 wird dieser Anspruch für den NCSR formuliert, allerdings bleibt das jetzige Gremium weit hinter diesen eigenen Ansprüchen zurück.

[3] Martin Schallbruch: "Mehr Unabhängigkeit für das BSI? Aufgaben und Steuerung des Bundesamtes für Sicherheit in der Informationstechnik", DuD • Datenschutz und Datensicherheit 4 | 2021, https://doi.org/10.1007/s11623-021-1424-3

[4] https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html

[5] Bundeswehr Kommando Cyber- und Informationsraum

Vorstellbar ist ein einmal jährlich tagendes Gremium auf Chef-Ebene, dass von Arbeitsgruppen vorbereitet wird und neben einer systematisierten Bestandsaufnahme eine gemeinsame, nationale Cybersicherheitsstrategie fortschreibt. Ähnlich zum Digitalgipfel der Bundesregierung könnten die unterschiedlichen Dimensionen der Herausforderungen in Plattformen organisiert und gemeinsam von den jeweils relevanten Stakeholdern verantwortet werden.

Sollte ein Nationaler Sicherheitsrat wie seit 2021 diskutiert geschaffen werden, sollte der NCSR dort als ein wesentlicher Pfeiler integriert werden.

Verbleibt der Nationale Cyber-Sicherheitsrat in der jetzigen Form ist dieser möglicherweise als internes Abstimmungsgremium innerhalb der Bundesregierung (und einigen Ländern) weiterhin hilfreich, erscheint aber als Grundpfeiler einer Cybersicherheitsarchitektur entbehrlich.

CISO Bund: Das BMI plant gemäß ihrer Cybersicherheitsagenda[6] die Schaffung der Position eines Chief Information Security Officers (CISO) für den Bund. Damit würde der Bund der in Unternehmen und zwischenzeitlich auch in mehreren Ländern[7] üblichen Praxis folgen. Zwingende Voraussetzungen für einen sinnvollen Mehrwert ist allerdings, dass der CISO-Bund in Personalunion mit dem BSI-Präsidenten besetzt wird und über mindestens ein Vortragsrecht beim für die IT der Bundesregierung zuständigen Ministers/Ministerin erhält. Das BSI ist bereits heute die „CISO-Organisation“ des Bundes, erfüllt ihre Aufgaben erfolgreich, eine personelle Trennung von CISO und BSI wäre in hohem Maße nachteilig.

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS): Der Koalitionsvertrag sieht die Schaffung einer gesetzlichen Grundlage auch für die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) vor. Ein eigenes ZITiS-Gesetz soll Verantwortlichkeiten klarer definieren und bietet eine Chance Vertrauen und Transparenz in deren Arbeit weiter zu erhöhen und mögliche Vorbehalte abzubauen. Dies erscheint für eine Behörde, die bei teils sehr weitgehenden Grundrechtseingriffen unterstützt, zwingend geboten. Ferner bietet ein solches Gesetz und die damit einhergehende parlamentarische Beratungsprozess gleichzeitig die Chance, die ZITiS weiterzuentwickeln. Ein Ausbau der ZITiS erscheint im Hinblick auf die weiter steigenden Bedarfe der Sicherheitsorgane und deren Handlungsfähigkeit im digitalen Raum dringend geboten.

Vor dem Hintergrund des Ziels ‚Digitaler Souveränität der deutschen Sicherheitsbehörden‘, wie es in der aktuellen Cybersicherheitsagenda des Bundesinnenministeriums definiert wurde, sollte ferner ein Rollenwechsel der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) hin zu einer Behörde mit einem zentralen bundesweiten Koordinierungsauftrag in Betracht gezogen werden. Ein Blick auf die Behördenstrukturen unseren westlichen Partner zeigt, dass solche „Zentralstellen“ nicht nur mehr Effizienz bringen,

[6] Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode. Juli 2022. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf

[7] Leitlinie zur Informationssicherheit der Landesverwaltung des Saarlandes, veröffentlicht im Amtsblatt des Saarlandes Teil I vom 15. Dezember 2016. http://www.vorschriften.saarland.de/verwaltungsvorschriften/vorschriften/ads_49_2016_teil_i_1192b_leitlinie_informationssicherheit.pdf

sondern auch Kosten und Ressourcen eingespart werden können. Statt, dass jede Sicherheitsbehörde ihre eigenen Forschungen und individuellen Anlangen betreibt, könnte dies etwa durch die ZITiS zentral gesteuert werden.

Zwar leistet die ZITiS schon jetzt einen wesentlichen Beitrag dazu, indem sie für die Aufrechterhaltung der Cyberfähigkeiten von Sicherheitsbehörden Werkzeuge und Methoden prüft, erforscht und evaluiert, Fachwissen sammelt sowie ggf. zentrale Dienstleistungen zur Verfügung stellt. Dies ist allerdings in der Regel nur für ausgewählte Bedarfsträger auf Bundesebene der Fall. Ein bundesweiter Auftrag zur Evaluation und Forschung sowie letztlich auch zur Festlegung, welche Systeme zukünftig durch die Sicherheitsbehörden zum Einsatz kommen, würde die Parallelität von Prozessen bei staatlichen Stellen verhindern. Fener könnte durch eine zentrale Bündelung von Investitionen und nationalen Entwicklungsfähigkeiten bei der ZITiS unter anderem die Abhängigkeit der Sicherheitsbehörden von außereuropäischen Herstellern noch weiter reduziert werden.

Die Weiterentwicklung der ZITiS ist damit eine wichtige Säule der vieldiskutierten „Digitalen Souveränität“ Deutschlands, will man nicht bei Maßnahmen der Strafverfolgung (und andere Maßnahmen der Inneren Sicherheit) innerhalb des nationalen Rechtsrahmens auf Unternehmen und Produkte zurückgreifen, die einer anderen Rechtstradition und Sicherheitskultur unterliegen.

In diesem Zusammenhang und in Anbetracht der Geschwindigkeit, mit der sich Technologien im digitalen Raum entwickeln, ist einer solchen Behörde ausreichend Spielraum zu geben, auch an Grundlagen für Technologien und Fähigkeiten zu arbeiten, deren Einsatz sich noch in einer gesellschaftlichen und politischen Diskussion befinden.

Cybersicherheitsstrategie: Die Formulierung und Fortschreibung einer kohärenten Strategie ist Voraussetzung für die zielgerichtete Weiterentwicklung der Cybersicherheitsarchitektur. Die aktuelle Strategie von 2021 ist bereits methodisch sinnvoll aufgebaut, bleibt aber in den Handlungsfeldern in wesentlichen Punkten in der Definition messbarer Ziele zu wage („wird sich verbessern“, „… steigt“, „…werden angenommen“). Hier sollten wenige aber zeitlich, quantitativ und qualitativ messbare Ziele vereinbart werden. (z.B. „Der Anteil an entdeckten Sicherheitslücken, die gemeldet werden, steigt von derzeit x% über y% in 2024 auf z% in 2026“ oder „Die Anzahl der Downloads und Installationen der Ausweis-App2 auf dem Smartphone steigt von derzeit x% über y% in 2024 auf z% in 2026“). Auch eine Differenzierung in Kurzfrist- und Langfristziele kann zu einer besseren Zielerreichung führen.

.

2) Wie kann das Ziel, das BSI unabhängiger aufstellen zu wollen, konkret erreicht werden und wo bedarf es neben der Rechtsaufsicht seitens des BMI auch einer Fachaufsicht – oder anders herum gefragt: wo sind die bestehenden Abhängigkeiten das größte Hemmnis mit Blick auf die Akzeptanz und das Vertrauen in das BSI und welche Möglichkeiten sehen Sie, diese abzubauen?

Wie in Frage 1 beschrieben, ist die Cybersicherheit zunehmend Gegenstand politisch-verortetem Regierungshandeln und das BSI diesbezüglich ein wichtiges Instrument der Exekutive. Ein von der Exekutive weitestgehend losgelöstes BSI erfüllt diesen Anspruch nicht.

Trotzdem ist denkbar, die Fachaufsicht des BSI breiter aufzustellen und bestimmte Entscheidungen, die grundsätzlich technisch-fachlicher Natur sind, durch das BSI in Eigenverantwortung zu bescheiden und einem Ministervorbehalt zu unterstellen, wie es beispielsweise für das Kartellamt bei der Untersagung von Unternehmenszusammenschlüssen geregelt ist. In wie weit ein solches Vorgehen praktikabel ist, müsste geprüft werden.

Für die zunehmend breite Bedeutung der Cybersicherheit für Staat, Wirtschaft und Gesellschaft kommt dem BSI-Präsidenten eine besondere Rolle zu und bedarf nicht eines ausreichenden eigenen Handlungs- und Gestaltungsspielraum im Rahmen grundsätzlicher politischer Vorgaben. Daher ist es nachvollziehbar die Position und dessen Ausübung unter dem Vorbehalt der „fortdauernden Übereinstimmung mit den grundsätzlichen politischen Ansichten und Zielen der Regierung“ zu stellen. Für die Erfüllung der Aufgaben sind hohe Anforderungen an die Qualifikation zu stellen, die für ein fachlich in höchstem Maße anspruchsvolle, stark in der politischen Öffentlichkeit stehende und in verwaltungsrechtliche Prozesse eingebundene Behörde mit sich bringen. Eine rein politische besetzte Position ist auszuschließen.

3) **Könnten Sie bitte den Begriff der aktiven Cyberabwehr und die unterschiedlichen Stufen und Möglichkeiten der aktiven Cyberabwehr (auch vor dem Hintergrund einer allein defensiv ausgerichteten bzw. einer offensiv ausgerichteten Cyberabwehr) definieren und wo sehen Sie konkrete Defizite im geltenden Recht und in den geltenden Kompetenzen, die einer wirksamen Cyberabwehr entgegenstehen?**

Der Begriff „aktive Cyberabwehr“ erscheint aus fachlicher Sicht unglücklich gewählt. Grundsätzlich erfordern die meisten Maßnahmen zur Cyberabwehr aktive Komponenten: So trennt eine Firewall aktiv zu schützende Netze vor schädlichem oder gefährlichem Netzverkehr und das Patchen von Systemen greift beispielsweise aktiv in die Integrität von IT-Komponenten ein.

Ein wesentliches Unterscheidungsmerkmal, das eine Abstufung ermöglicht und in der Diskussion bereits Einzug gefunden hat, ist, die Maßnahmen zur Cybersicherheit nach dem Ort ihrer Wirksamkeit zu staffeln: (1) Im eigenen, unmittelbaren Verfügungsbereich (z.B. eigene Firewall, Netze, Rechner), (2) in einem Bereich Dritter, über den aufgrund gesetzlicher oder vertraglicher Regelungen Maßnahmen verfügt werden kann (z.B. Providernetze) und (3) in einem Bereich, in dem gegen den Willen oder mindestens ohne explizite Zustimmung von Betroffenen Maßnahmen zur Cybersicherheit durchgeführt werden (entspricht z.B. in der analogen Welt dem Aufbrechen einer Türe durch Durchsetzung einer rechtlichen Maßnahme). Der hierfür erforderliche Rechtsrahmen ließe sich analog anwenden (Richtervorbehalt, Maßnahmen bei Gefahr in Verzug etc.)

Alle drei Maßnahmenbereiche sind für eine effiziente Cyberabwehr unerlässlich und alle drei Maßnahmenbereiche erfordern eigene Fähigkeiten und Werkzeuge. Die beiden ersten Fähigkeiten und Werkzeuge sind vergleichbar, der dritte Maßnahmenbereich hat technische Überschneidungen mit aktiven Cyberoperationen und wird deutlich seltener zur Anwendung kommen. Auch hier lohnt sich der Vergleich zur „analogen Welt“: Mit der GSG9 verfügt die Bundespolizei und mit den SEKs der Landespolizeien Einheiten, die über besondere polizeiliche Fähigkeiten verfügen und deren Anwendung in einem besonderen Maße der Verhältnismäßigkeit unterliegen müssen.

Eine Durchführung solcher Maßnahmen außerhalb der eigenen gesetzlichen Reichweite (z.B. im Ausland) wird nur mit angemessener Amtshilfe möglich sein. Aktive Maßnahmen in Drittstaaten gegen den Willen dieser ist kaum vorstellbar. Graubereiche wie Maßnahmen in Staaten, die über keine funktionierenden staatlichen Strukturen verfügen, werden ähnliche rechtliche und politische Implikationen mit sich bringen wie „analoge“ polizeiliche Maßnahmen in solchen Kontexten.

Hiervon abzugrenzen sind Aktive Militärische Cyberoperationen (AMCO). Diese sind – obgleich vielfach das mildere Wirkmittel – militärischen Mitteln zuzuordnen und außerhalb von kriegerischen Situationen nicht anzuwenden.

Die für Gefahrenabwehr im Cyberraum erforderlichen Befugnisse der beiden ersten Maßnahmenbereiche sind bereits dem BSI zugeordnet (Bsp. In §7c BSIG) und sollten auch bei einer Ausweitung weiterhin beim BSI verortet bleiben.

Die Grundsätzliche Zuständigkeit für die Gefahrenabwehr im Cyberraum kann langfristig sinnvoll nur in einer zentralen Einrichtung erfolgen, entweder durch die Verlagerung in die Zuständigkeit des Bundes oder durch eine Bund-Länder Einrichtung (was aber wieder Redundanzen schaffen würde).

4) Weitere Instrumente, die der Koalitionsvertrag adressiert, sind etwa auch

- das Recht auf Verschlüsselung,
- ein Schwachstellenmanagement und die Pflicht, Sicherheitslücken zu melden,
- die Stärkung der digitalen Souveränität und die Beachtung der Vertrauenswürdigkeit von Unternehmen,
- die Vorgaben „security-by-design/default“ als Standard,
- Stärkung der Produkthaftung und der IT-Sicherheitsforschung,
- das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme, etwa bei 5G oder KI.

Welche dieser Maßnahmen sollten mit welcher Priorität ungesetzt werden, wo besteht aus Ihrer Sicht darüberhinausgehender Handlungsbedarf und wo bestehen insbesondere Defizite?

Entscheidend ist, dass die Begriffe nicht inhaltsleer bleiben, sondern in den jeweiligen Handlungsfeldern konkrete und messbare Ziele vereinbart werden, die in der Praxis relevant werden. So wurde aus Deutschland heraus maßgebliche Standards beispielsweise für elektronische Signaturen erarbeitet, die aufgrund ihrer Komplexität keine Verbreitung fanden und später durch (meist geschlossene) Verfahren großer Anbieter ersetzt wurden.

Recht auf Verschlüsselung: Diese Diskussion ist zwischenzeitlich ein Vierteljahrhundert alt und an der technischen Unmöglichkeit Verschlüsselung wirksam zu verbieten hat sich nichts verändert. Hier wird empfohlen, den politischen Raum vor weiteren Diskussionen zu schonen und Ressourcen und Energie auf die weiteren Herausforderungen bei Cybersicherheit und Kriminalitätsbekämpfung zu legen.

Produkt- und Dienstehaftung: Eine nachhaltige Sicherheit von IT-Systemen kann nur durch die stärkere Einbeziehung von Herstellern und Betreibern in die Haftung gelingen: Genauso wie es bei öffentlich zugänglichen Gebäuden oder Wegen eine Verkehrssicherungspflicht gibt, für die der Eigentümer haftet, muss es eine Haftung beispielsweise für Schäden durch Schadsoftware geben, die durch ungepatchte, öffentlich zugängliche Server verbreitet werden. Während bei Kritischen Infrastrukturen die IT-Sicherheit gesetzlich geregelt wird, erscheint die Regulierung der anderen Wirtschaftsbereiche durch ein Haftungsregime zielführender.

Open-Source: Hier ist zu erwarten, dass der Angriffsfläche und die Abhängigkeiten sich weiter ausweiten (siehe Log4Shel/j), da open-source Code in unterschiedlichster Weise weit verbreitet ist und genutzt wird. Eine einfache Applikation besteht schonmal teils aus hunderten open-source Bibliotheken & Komponenten mit mehreren Millionen Zeilen Code. Deswegen wird das Thema sichere Lieferketten und eine „Software Bill of Material (SBOM)“ bei Software insgesamt und insbesondere bei Open-Source Komponenten sowie die Evaluierung und Zertifizierung von Open-Source Komponenten zunehmend wichtig. Gerade letztere ist oftmals ressourcenintensiv und ohne einen wirtschaftlichen Sponsor gerade bei Open-Source Projekten auf staatliche Unterstützung angewiesen. Wichtig dabei ist, dass es sich nicht um einmalige Aufwände handelt, sondern um einen Prozess, der sicherstellt, dass auch bei kontinuierlichen Versionsanpassungen ein Qualitätssicherungsprozess eingehalten und nachevaluiert wird.

5) Vor dem Hintergrund des hybriden Angriffskrieges Russlands gegen die Ukraine sind erneut Forderungen nach Instrumenten der sogenannten offensiven Cyberabwehr laut geworden. Wie beurteilen Sie diese Forderungen und die Argumentation, offensive Instrumente vermeintlich unterhalb der Schwelle von Hackbacks einzusetzen, im Hinblick auf ihre Recht- und Zweckmäßigkeit?

Es ist unklar was mit „offensive Cyberabwehr“ gemeint ist. Angesichts der weltweiten Sicherheitslage wird man auch zunehmend die eigenen Fähigkeiten zur Offensive Militärische Cyberoperationen[8] signifikant ausbauen. Dabei handelt es sich letztlich um

[8] Matthias Schulze: Militärische Cyber-Operationen: Nutzen, Limitierungen und Lehren für Deutschland. SWP-Studie 2020/S 15, 10.08.2020, doi:10.18449/2020S15

militärische Maßnahmen. Für die Maßnahmen im zivilen Bereich wird auf die Beantwortung von Frage 3 verwiesen.

6) **Was kann die Bundesrepublik Deutschland in ihrer nationalen und internationalen Cybersicherheitspolitik von anderen Ländern und internationalen best practices konkret lernen, insbesondere im Hinblick auf staatliche Stellen, Governance, verfügbare Instrumente, Fokus und Kapazitäten?**

Ein Aspekt, der immer wieder auffällt, ist die aktive Industriepolitik, die in vielen Ländern, auch in Bezug auf Cybersicherheitsprodukte aus nationaler Entwicklung verfolgt wird. Dabei wird nicht nur in der Beschaffung von Cybersicherheitsprodukten (als Schlüsseltechnologien) proaktiv nationales Sourcing betrieben und der Export solcher Produkte administrativ und politisch aktiv gefördert.

Darüber hinaus fördern einzelne Länder im Rahmen von millionenschweren „Security Capacity Building Programs“ den Aufbau der IT-Sicherheit in anderen Ländern. Die Gelder fließen ausschließlich an nationale Hersteller des fördernden Staates zurück, die sich so Referenzkunden schaffen oder Industrien mit ihren Produkten und Standards dominieren.

In Deutschland haben hingegen die Restriktionen und der bürokratische Aufwand für den Export nach Einschätzung der Industrie in den vergangenen Jahren zugenommen.

7) **Welche politischen und rechtlichen Herausforderungen stellen sich bei der Schaffung eines Regelwerks für eine Meldepflicht für Sicherheitslücken (zero days) und einen gesetzlich strukturierten Umgang mit Schwachstellen („wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen“)?**

Hier wird auf Fragen 15 und 16 verwiesen.

8) **Die Bundesregierung hat Eckpunkte eines KRITIS-Dachgesetzes verabschiedet und will dabei insbesondere eine bessere Verschränkung des Schutzes digitaler und physischer Infrastruktur erreichen: Welche organisatorischen und rechtsdogmatischen Ansatzpunkte sind denkbar, um physische und digitale Komponenten kritischer Infrastruktur gemeinsam und kohärent zu regulieren und inwiefern kann der Gesetzgeber hier insbesondere auf geltendem Recht und Regulierungsvorschlägen aus der Vergangenheit (etwa rund um das IT-Sicherheitsgesetz 2.0) aufsetzen?**

Von der Beantwortung dieser Frage wird abgesehen.

9) **Mit Blick auf Redundanzen in der Kommunikationsinfrastruktur der Deutschen Bahn könnte das Netzwerkprotokoll TCP/IP als Rückfallebene bei etwaigen Sabotageakten verwendet werden. TCP/IP müsste dabei aber nicht über Mobilnetze, sondern kabelgebunden verwendet werden. Dafür müsste die DB-Netze ein kleines Matrix-Netz an den Knoten aufbauen, das bspw. mit der Kabelinfrastruktur einzelner Netzbetreiber verbunden ist. Dann läuft das System weiter, auch wenn**

die Infrastruktur punktuell beschädigt, oder zerstört würde. Was könnten Gründe dafür sein, dass ein solches Matrix-Netz nicht bereits existiert?

Von der Beantwortung dieser Frage wird abgesehen.

10) Wenn in Deutschland entscheidende Bestandteile für kritische Infrastrukturen (KRITIS) beschafft werden – etwa für Telekommunikationsnetzwerke –, dann können Produzenten unter bestimmten Bedingungen davon ausgeschlossen werden. Die Hürden hierfür sind jedoch hoch. So kann dies erst nach wiederholten Verstößen gegen die Vertrauenswürdigkeit geschehen (bspw. wenn ein Hersteller falsche Angaben gemacht hat, Sicherheitsüberprüfungen nicht unterstützt oder IT-Schwachstellen nicht unverzüglich meldet und beseitigt). Sehen Sie in Anbetracht der sog. „Zeitenwende“ Anlässe den geltenden Rechtsrahmen zu verschärfen (etwa in einem IT-Sicherheitsgesetz 3.0) und, falls ja, wie?

Die Frage bezieht sich offensichtlich auf §9b BSIG. Dabei handelt es sich im Wesentlichen um eine politische Prüfbefugnis als ultima ratio zum Ausschuss von Herstellern kritischer Komponenten soweit eine Vorabprüfung Sicherheitsbedenken für die öffentlichen Interessen der Bundesrepublik Deutschland ergibt. Obgleich diese Regelung seine Berechtigung in Ausnahmesituationen hat (auch zur Abschreckung), trägt sie wenig zur Erhöhung der objektiven IT-Sicherheit in der Fläche bei.

Hier erscheint es zweckdienlicher, mit dem Instrument definierter Mindeststandards einen hohen Standard bei der Vertrauenswürdigkeit von kritischen Komponenten festzulegen und diesen um prozessuale Kriterien und solchen nach Lieferketten der Komponenten zu erweitern.

Die geeignete Ausgestaltung von Mindeststandards kann auch ein wirtschaftspolitischer Beitrag zur Stärkung der nationalen und europäischen Cybersicherheitsindustrie sein und damit einen Beitrag zur Stärkung der Digitalen Souveränität leisten.

11) Wie bewerten Sie die Lage von IT-Fachkräften – insbesondere für Cybersicherheit – auf dem Arbeitsmarkt und was müssten staatliche (Sicherheits)-Behörden verbessern, um noch mehr kompetente IT-Fachkräfte zu gewinnen?

Die Lage von IT-Fachkräften – insbesondere für Cybersicherheit auf dem Arbeitsmarkt wird von Behörden und Unternehmen als äußerst angespannt angesehen – und vermutlich bleiben, wenn keine Maßnahmen ergriffen werden. Dies hat unmittelbar negative Auswirkungen auf das Cybersicherheitsniveau in Deutschland und muss sofern es langfristig bestehen bleibt als ernstes Risiko der nationalen Sicherheit betrachtet werden.

Ursache hierfür ist der exponentiell gestiegene Bedarf und die anspruchsvolle Ausbildung im Bereich der IT-Sicherheit. Auch wenn weiterhin Maßnahmen zur Erhöhung der Fachkräfte in diesem Bereich wie eine frühe Motivierung in Schulen, spezialisierte Studiengänge

für Cybersicherheit und die gezielte Anwerbung von Bewerbern hierfür erforderlich sein werden, eine adäquate Cybersicherheit wird sich nicht alleine mit einer quantitativen Erhöhung der Fachkräfte erzielen lassen.

Erforderlich ist eine qualitative Weiterentwicklung von Werkzeugen zur Cyberabwehr, ja ein Quantensprung in den Technologien, die dafür Sorge tragen, dass ein hoher Automatisierungsgrad erreicht wird.

Grundsätzlich gilt: Derzeit haben wir einen „Vulnerablen Cyberraum“, ein Raum, in dem Cyberangriffe deutlich weniger Ressourcen benötigen als die Abwehr derselbigen. Daher ist eine weiterhin hohe Intensität der Forschungsinvestitionen beim Thema Cybersicherheit zwingend erforderlich. Ziel muss es sein, langfristig das Verhältnis umzudrehen. Hierfür werden vor allem die Verknüpfung von Cybersicherheit und Methoden des Maschinellen Lernens eine wesentliche Rolle spielen.

Speziell im Bereich der öffentlichen Verwaltung spielen zwei weitere Faktoren eine Rolle: Das Vermeiden von Doppelstrukturen mit dem gegenseitigen Abwerben von Fachkräften und die Schaffung von adäquaten Besoldungen für Spezialisten (dies betrifft vielfach eine deutliche Ausweitung von Befreiungen vom Besserstellungsverbot). Auch hierfür bietet es sich an, das fachliche Knowhow auf ziviler Seite im BSI und auf militärischer Seite im Org-Bereich CIR zu konzentrieren.

Neben den finanziellen Rahmenbedingungen spielen für viele Talente die Arbeitsbedingungen, Flexibilität, aber auch wie spannend und abwechslungsreich die Tätigkeit ist, eine nicht unerhebliche Rolle. Auch hier konnte das BSI in den vergangenen beiden Jahrzehnten sich als attraktiver Arbeitgeber positionieren – eine Voraussetzung dafür, dass es dem Amt gelang, das politisch vorgegebene Wachstum trotz der angespannten Fachkräftesituation zu erreichen.

12) Wie könnte die Ausbildung von IT-Cyberfachkräften sowohl in quantitativer als auch in qualitativer Hinsicht in Deutschland weiter verbessert werden?

Siehe Frage 11. In qualitativer Hinsicht bietet sich eine weitere Differenzierung an: Nicht alle IT-Sicherheitsfachkräfte müssen Informatiker sein. Viele Aufgaben im Bereich der Cybersicherheit haben die Schwerpunkte in der Prozessorganisation. Hier könnten auch in anderen Studiengängen (z.B. BWL) entsprechende Schwerpunktprogramme aufgelegt werden.

13) Wie bewerten Sie die vorhandenen technischen Fähigkeiten in Deutschland für eine wirksame Cyberabwehr – auch mit aktiven Cyberabwehr-Instrumenten?

Grundsätzlich haben sich die (staatlichen) technischen Fähigkeiten in Deutschland für eine wirksame Cyberabwehr in den vergangen zehn Jahren signifikant verbessert und weiterentwickelt. Das BSI verfügt über umfassende eigene Fähigkeiten und Werkzeuge.

Deutschland verfügt im militärischen Bereich sowohl in der Eigensicherung als auch für Offensive Militärische Cyberoperationen über erfahrene Kräfte und umfassende eigene Fähigkeiten.

Für beides gilt jedoch: Die technische Entwicklung geht mit einer hohen Geschwindigkeit weiter und erfordert weiter kontinuierliche Investitionen auf hohem Niveau in diesem Bereich in Menschen, Technologien und Werkzeugen.

14) Welche Rolle spielen private Cybersicherheits-Unternehmen für eine effektive staatliche Cyberabwehr im internationalen Vergleich?

(Private) Cybersicherheitsunternehmen spielen sowohl für eine effektive staatliche als auch für die Cyberabwehr bei Unternehmen und Bürgern eine ganz essentielle Rolle. Dies gilt sowohl bei der Bereitstellung sicherer IT-Infrastrukturen, bei IT-Sicherheitsdienstleistungen (wie der Evaluierung von Software), vor allem aber bei der Bereitstellung effektiver Werkzeuge zur Cybersicherheit. Eine effektive Cyberabwehr ohne eine starke, forschende Cybersicherheitsindustrie ist ausgeschlossen.

Deutschland investiert seit mindestens zwei Jahrzehnten erhebliche Mittel in die Cybersicherheitsforschung mit soliden Ergebnissen. Trotzdem stammen – in der Gesamtschau betrachtet – nur ein geringer Teil der verwendeten Werkzeuge aus nationaler Wertschöpfung. Dies erscheint im Hinblick der Bedeutung dieser Schlüsseltechnologien nicht angemessen. Abhilfe könnte eine aktive Industriepolitik bringen, die das Ziel hat, leistungsfähige, weltweit wettbewerbsfähige Anbieter aufzubauen und den Anteil aus Drittstaaten eingeführter Cybersicherheitsprodukte zu reduzieren. Der Staat kann hier mit seiner Beschaffungspolitik wichtige Stellschrauben bedienen.

15) Inwieweit sind aus technischer Sicht sog. Software-Schwachstellen (nicht gemeint sind spezifische IT-Schnittstellen für Sicherheitsbehörden, wie sie z. B. derzeit im Rahmen des 3GPP-Gremiums für den künftigen 6G-Mobilfunkstandard unter Beteiligung von ZITiS und Cyberagentur entwickelt werden) erforderlich, um Sicherheitsbehörden Zugriff auf Kommunikationsendgeräte im Rahmen von Strafermittlungen zu verschaffen oder gibt es mittlerweile hinreichend wirksame Technologien, wie z. B. kryptographische Verfahren, die weniger Kollateralschäden aufweisen und inwieweit ist diese Schwachstellen-Diskussion auf mittlere Sicht hinfällig, wenn wir an Entwicklungen wie Quantenkommunikation denken?

Schwachstellen in Softwareprodukten sind derzeit der wesentliche Grund für einen „Vulnerablen Cyberraum“ in dem Cyberangriffe deutlich weniger Ressourcen benötigen als die Abwehr derselbigen. Die Konsequenz ist, dass solche Schwachstellen zu einem grundlegenden Risiko für digitalisierte Gesellschaften und deren Funktionsfähigkeit werden. Die

weltweite Bedeutung für die Zukunft digitaler geopolitischer Konflikte wurde in einer interessanten Szenarioentwicklung der Stiftung Wissenschaft und Politik und Deloitte erarbeitet.[9]

Ziel von IT-Sicherheitsforschung und angewandter Cybersicherheit ist es, Architekturen zu entwickeln, die die Vulnerabilität durch Schachstellen nachhaltig reduziert. Dazu gehören sichere Entwicklungssprachen und -umgebungen und moderne Betriebssystemarchitekturen (auf Basis von Mikrokern/Hypervisor-Isolierung).

Aus fachlicher Sicht sind solche Schwachstellen unbedingt und schnellstmöglich zu schließen um ein Risiko für Staat, Wirtschaft und Bürger zu vermeiden. Denn es kann nicht ausgeschlossen werden, dass vorhandene Schwachstellen nicht auch durch unberechtigte Angreifer genutzt werden.

Daher darf die Nutzung von Schwachstellen im Rahmen der Strafverfolgung, beispielsweise um sich Zugang zu einem Kommunikationsendgerät zu verschaffen, nicht dazu führen, dass dadurch das Schließen der Sicherheitslücke (unbillig) verzögert wird.

16) **Wie sollte ein Schwachstellen-Management technisch, personell und organisatorisch aufgesetzt werden, sind dafür z. B. Risiko Management-Standards als ein Vorbild denkbar und welche Ziele kann sich ein Schwachstellen-Management setzen, angesichts von über 20.000 Software-Schwachstellen, wie sie zuletzt der BSI-Lagebericht festgestellt hat und inwieweit ist für die Konzeptionierung und Implementierung eines solchen Schwachstellen-Managements tatsächlich ein unabhängiges BSI zwingend erforderlich?**

Derzeit existiert kein zentrales Schwachstellenmanagement, weder im Sinne einer Coordinated Vulnerability Disclosure (CVD) Richtlinie noch im Sinne eines strukturierten Prozesses zur Bewertung und der weiteren Behandlung von kritischen Schwachstellen. Die Schaffung einer CVD-Richtlinie ist als Ziel in der aktuellen Cybersicherheitsstrategie[10] aufgeführt.

Die Nutzung von bereits offen gelegten Schwachstellen in Werkzeugen zur Strafverfolgung bzw. während der Behebung der selbigen erscheint im Sinne von Frage 15 akzeptabel. Will man den Zeitraum zwischen Entdeckung einer Zero-Day Schwachstelle und deren Behebung – und damit eine mögliche Nutzung in solchen Werkzeugen – verlängern, entsteht ein Zielkonflikt zwischen Cybersicherheit und Strafverfolgung. Das Risiko für die Cybersicherheit kann dabei erheblich sein und auch staatliche Schutzgüter umfassen. Erschwerend kommt hinzu, dass es objektiv äußerst schwierig ist das individuelle Risiko einer Sicherheitslücke zu bewerten.

Hier könnte ein Lösungsansatz sein, das allgemeine Risiko in (groben) Risikokategorien durch eine Fachbehörde zu bewerten und mit einer gesetzlich festgelegten maximalen Laufzeit (z.B. in drei Kategorien 6, 9 oder 12 Monate) zu kombinieren, nach der eine Schwachstelle für einen Zeitraum vom Tag der Kenntnisnahme bis zur weiteren Meldung an einen nationalen CVD-Prozess für Zwecke der Strafverfolgung genutzt werden kann.

[9] https://www2.deloitte.com/de/de/pages/strategy/articles/zukunft-digitaler-geopolitischer-konflikte.html
[10] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf

Damit würde sichergestellt, dass auch für die Zwecke der Strafverfolgung erforschte oder beschaffte Schwachstellen zeitnah geschlossen werden und ein beständiger Beitrag zur Erhöhung der Cybersicherheit geleistet werden kann.

Die Bewertung der Schwachstellen und die Governance darüber sollte nicht durch das BSI erfolgen, sondern durch eine andere Fachbehörde, beispielsweise die ZITiS. Die kürzere Nutzungsdauer von Schwachstellen wird allerdings zu einem erhöhten Ressourcenbedarf zur Erforschung/Beschaffung von Schwachstellen führen und sofern eine systematische Verbesserung der Softwareprodukte erfolgt, vermutlich exponentiell steigen. Daher erscheint es zwingend notwendig weitere Mittel für die Erforschung von effizienten, alternativen Werkzeugen zur Strafverfolgung im digitalen Raum bereitzustellen (ZITiS, Cyberagentur).

Es erscheint außerordentlich wichtig für die Vertrauenswürdigkeit des BSI, hier eine strikte Trennung beizubehalten und das BSI aus dem Nutzungsregime von Schwachstellen vollständig herauszuhalten. Das BSI sollte den nationalen CVD-Prozess verantworten und auf gesetzlicher Grundlage jede zur Kenntnis erlangte Sicherheitslücke unmittelbar in den CVD-Prozess zur Schließung der Schwachstelle zu überführen.

Insgesamt ist darauf zu achten, dass keine Regulierung dazu führen darf, dass Behörden zur Erfüllung ihrer Aufgaben auf die Beschaffung ausländischer Software ausweichen. So könnte beispielsweise bei einem Prozess, der eine temporäre maximale Nutzungsdauer vorschreibt, diese auch für die in beschafften Werkzeugen ausgenutzten Schwachstellen gelten.

17) **Anhand welcher Maßnahmen und/oder Methoden kann das Sicherheitsverständnis und -verhalten von IT-Nutzer*innen effektiv in den Mittelpunkt gerückt, eine höhere IT-Sicherheitskultur aufgebaut und das individuelle Vertrauen in die digitale Umgebung gestärkt werden?**

Die Anfälligkeit von IT-Systemen nimmt mit der Diversität der eingesetzten Hard- und Softwareanwendungen, der Vielfältigkeit von Versionen, der Anzahl von Schnittstellen erheblich zu, der Aufwand, der für eine wirksame Cybersicherheit in einer Einrichtung zu leisten ist, unterschreitet eine gewisse Mindestschwelle nicht – auch bei kleinen Einrichtungen. Dies führt dazu, dass vielfach kleine Einheiten – und dazu gehören die übergroße Anzahl der Kommunen – wirtschaftlich keine ausreichende Cyberabwehr implementieren können.

Abhilfe kann nach hiesiger Sicht nur in der weiteren Standardisierung und Zentralisierung von Anwendungen (beispielsweise cloud-basierte Ausführung, die in sicheren Rechenzentren betrieben werden), geschlossenen Anwendungen und einer an „Zero Tust“ orientierten Infrastruktur erfolgen.

18) **Wer bzw. was muss alles in den Blick genommen werden, wenn wir über Zuständigkeiten und Instrumente zur Verbesserung der IT-Sicherheit nachdenken, wo liegen die jeweiligen Defizite sowie Verbesserungsmöglichkeiten und wie bewerten Sie die Effektivität aktueller Informations- und (Weiter-)Bildungsmaßnahmen?**

Von der Beantwortung dieser Frage wird abgesehen.