Stellungnahme der Arbeitsgemeinschaft Kritische Infrastrukturen (AG KRITIS)

zur öffentlichen Anhörung im Ausschuß für Digitales zum Thema „Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“ am Mittwoch, 25. Januar 2023, 14:00 – 16:00 Uhr, Sitzungssaal Marie-Elisabeth-Lüders Haus (MELH) 3.101

Die AG KRITIS wird vertreten durch den Sachverständigen Manuel ‚HonkHase‘ Atug.
honkhase@ag.kritis.info

18.01.2023

AG KRITIS

Die AG KRITIS ist ein unabhängiger, ehrenamtlicher Zusammenschluss von Expertinnen und Experten, die sich täglich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (10) BSI-Gesetz i. V. m. BSI-Kritisverordnung beschäftigen, z. B. durch Planung, Bau, Betrieb, Beratung oder Prüfung der beteiligten IT-Systeme und Anlagen. Die Arbeitsgruppe ist vollständig unabhängig von Staat und Wirtschaft und vertritt keine Interessen von Unternehmen oder Wirtschaftsverbänden.

Inhaltsverzeichnis

Antworten auf die gestellten Fragen

Frage 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?

Wir begrüßen grundsätzlich das Bestreben, dem „Bundesamt für Sicherheit in der Informationstechnik" (BSI) mehr Unabhängigkeit zuzusprechen, wie es beim BStatistischen Bundesamt bereits umgesetzt ist. Die Dienstaufsicht verbleibt dann weiterhin beim Bundesministerium des Innern und für Heimat (BMI) und die Fachaufsicht erfolgt selbstständig nach Maßgabe wissenschaftlicher Grundlagen und nach Vorbild des Bundesamts für Statistik (Vgl hier: §1 BStatG).

Von einer bundeseinheitlichen Einrichtung von Landesämtern für die Sicherheit in der Informationstechnik (LSI) sollte man hingegen absehen. IT-Sicherheit kann nur dann gewährleistet werden, wenn das Vorgehen bundesweit harmonisiert und koordiniert ist, da das Internet keine Landesgrenzen kennt. So zeigte sich bereits in der Vergangenheit, dass für IT-Sicherheit zuständige Behörden in den Ländern dem Stand der Technik zum Teil Jahre hinterher hingen und nach veralteten wissenschaftlichen Kenntnissen handelten. Exemplarisch zeigt sich dies an bayerischen Behörden: Auf Anweisung des LSI wird dort weiterhin ein regelmäßiger Passwortwechsel durchgeführt, während des BSI diese Praxis längst nicht mehr empfiehlt.

Für eine Umsetzung der NIS2-Richtlinie wird es erforderlich sein, auch auf Ebene der Länder zuständige Behörden zu benennen. Wie oben dargestellt, erscheint der zusätzliche Aufbau von landeseigenen Verwaltungsbehörden mit entsprechender Zuständigkeit nicht zielführend zu sein. Stattdessen sollte vielmehr die grundgesetzliche Kompetenzverteilung dahingehend geändert werden, dass der Bund eine zuständige Behörde für die Wahrnehmung der Aufgaben auf Landesebene benennen darf.

Die ZITiS benötigt ein Gesetz, welches die Aufgaben klar definiert und juristische Leitplanken setzt, die die Entwicklungen von ZITiS verpflichtend an der grundgesetzlich gebotenen Schutzpflicht im Bereich der IT-Sicherheit und damit dem Grundsatz der Verteidigung orientiert.

Der Cybersicherheitsrat ist in seiner Zusammensetzung nicht in der Lage seinen Aufgaben nachzukommen. Weder die Wirtschaftsvertreter noch die Staatssekretäre der verschiedenen Ressorts haben eine Übersicht über aktuelle technische Entwicklungen. Dieses Wissen findet sich primär in akademischen Kreisen.

Eine weitere Aufgabe soll es sein, Impulse zur Weiterentwicklung der Cybersicherheitsarchitektur in Deutschland zu entwickeln. Auch wenn die im Cybersicherheitsrat vertretenen Staatssekretäre der verschiedenen Ressorts die aktuellen Verwicklungen, Abhängigkeiten und Doppelzuständigkeiten genau kennen, so fehlt ein unabhängiger, neutraler Blick von außen. Unter der Maßgabe, dass jedes Ministerium das Ziel hat, mehr Zuständigkeiten, mehr Stellen und mehr Budget zu erlangen, ist die aktuelle Zusammensetzung des Cybersicherheitsrat nicht in der Lage, ineffiziente Aspekte der Cybersicherheitsarchitektur in Deutschland zu finden oder gar zu beheben.

Damit der Cybersicherheitsrat in der deutschen Cybersicherheitsarchitektur in der Zukunft seinen Aufgaben gerecht werden kann, ist es unumgänglich, sowohl Vertreter der Wissenschaft, als auch Vertreter der Zivilgesellschaft in dieses Gremium zu berufen. Vertreter der Wirtschaft in diesem Gremium sind insbesondere aufgrund ihres technischen Sachverstands zu berufen, nicht jedoch aufgrund der Tatsache, dass sie in der Interessenvertretung des eigenen Verbands oder Arbeitgebers aktiv sind.

Frage 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?*

Die bestehenden Abhängigkeiten sind aus unserer Sicht politischer Natur. Insbesondere die zuständigen Referate im BMI versuchen die Kontrolle über das BSI zu erhalten, ohne dafür eine logisch nachvollziehbare oder wissenschaftlich korrekte Begründung zu haben. Die Verquickung mit der Aufsicht über die Sicherheitsbehörden sind hier dem Vertrauen, dass das BSI eigentlich haben müsste, abträglich.

Solange andere Geschäftsbereichsbehörden des BMI ein Interesse am Schaffen oder Offenhalten von Sicherheitslücken haben, bleiben in der IT-Sicherheitsszene Zweifel, ob dem BSI gemeldete

Schwachstellen wirklich dem Hersteller weitergemeldet oder aber auf Weisung des BMI zu Gunsten der anderen Sicherheitsbehörden zurückgehalten werden. Zudem ist dann auch die Standardisierungsarbeit des BSI dem Zweifel ausgesetzt, ob das BSI wirklich im Sinne der IT-Sicherheit gearbeitet hat, oder doch auch IT-Sicherheitslücken für die übrigen Sicherheitsbehörden eingebaut hat. Zusammengefasst geht es darum, ob der Arbeit des BSI vertraut werden kann, wenn nicht alleine das BSI seine Arbeit steuern kann, sondern auch das BMI, das nicht nur den Interessen der IT-Sicherheit verpflichtet ist.

Frage 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?*

Eine allgemein verbindliche Definition für “aktive Cyberabwehr” existiert nicht. Das sogenannte Stufenmodell für aktive Cyberabwehr des BMI wurde unserer Kenntnis nach von den Sicherheitsbehörden nicht offiziell veröffentlicht oder zur (politischen) Diskussion gestellt. Wir vermuten, dass hier Bezug genommen wird auf die Informationen zum Stufenmodell, wie diese auf netzpolitik.org veröffentlicht worden sind: https://netzpolitik.org/2019/aktive-cyber-abwehr-innenminister-schaltet-bei-it-sicherheit-schrittweise-von-verteidigung-auf-angriff/

Die Frage sollte aus Sicht der AG KRITIS nicht lauten “welche Stufen der aktiven Cyberabwehr existieren”, sondern “wo liegt die Grenze zwischen offensiver und defensiver Cyberabwehr”. Die Verwendung des Adjektivs “aktiv” ist hier unserer Ansicht nach irreführend. Die Schaffung von Stufen in diesem Kontext hat aus unserer Sicht das Ziel, im Rahmen einer politischen Salamitaktik über ein Stufenmodell erst eine abgeschwächte Form der defensiven Cyberabwehr gesetzlich zu erlauben und diese Befugnisse in den folgenden Jahren sukzessive auf offensive Maßnahmen zu erweitern.

Die Grenze zwischen offensiver und defensiver Cyberabwehr liegt in der Erhaltung der Integrität und Vertraulichkeit der entfernten Systeme, die am Angriff beteiligt sind. Im Stufenmodell ist schon das Verwenden eines Netzwerkscanner-Werkzeugs wie nmap eine offensive Maßnahme der Stufe 1 oder 2. Da der Einsatz eines solchen Werkzeugs die Integrität und Vertraulichkeit des angegriffenen Systems im Regelfall nicht gefährdet, ist dies zu den defensiven Maßnahmen zu zählen. Maßnahmen, deren Ziel es ist, fremden Quellcode auf dem Zielsystem auszuführen (Stufe 4), zählen dagegen zu den offensiven Maßnahmen. Auch der Einsatz eines Honeypots zählt zu den

defensiven Maßnahmen, wird aber im Stufenmodell als Stufe 3 beschrieben, sofern dabei auch Daten abfließen.

Die Maßnahme, einen sogenannten distributed Denial of Service Angriff (DDos) durchzuführen, lässt sich hingegen nicht eindeutig mit der Frage nach der Vertraulichkeit und Integrität klassifizieren. Zwar wird beides streng genommen nicht beeinträchtigt. Da Cyberangriffe aber oft von Systemen durchgeführt werden, deren Zweck eigentlich ein anderer ist und die für die Nutzung bei einem Angriff vom Angreifer übernommen worden sind, kann ein DDoS Angriff hier zu unerwünschten Kollateralschäden führen. Beispielsweise ist vorstellbar, dass Computer, die am Angriff mitwirken, im Leitstand eines Energieversorgers stehen oder in einem Krankenhaus eingesetzt werden. Würde man diese Systeme mit einem DDoS, oder anderen Maßnahmen der Kategorie 5 (“Hackback”) stören oder deaktivieren, so würde der erfolgte Ausfall auch andere Systeme beim Betreiber beeinträchtigen.

Einerseits fehlt im bestehenden Recht die explizite Erlaubnis, defensive Maßnahmen, wie in den vorstehenden Absätzen beschrieben, durchzuführen. Andererseits fehlt auch eine explizite Abgrenzung zwischen defensiven und offensiven Methoden. Eine solche Abgrenzung ist, wie am Beispiel DDoS beschrieben, oft nur schwer möglich.

Die Reduktion der Auswirkung eines Cyberangriffs kann nur gelingen, wenn alle Computersysteme, also sowohl solche in staatlichen Verwaltungen, in Unternehmen, aber auch der Bevölkerung, von vornherein grundlegend gegen Angriffe geschützt sind. Eine effektive Cyberabwehr fängt daher mit einer Meldepflicht für Sicherheitslücken an, die auch die Sicherheitsbehörden (einschließlich ZITiS) explizit und ausnahmslos zur unverzüglichen Meldung von bekannt gewordenen Sicherheitslücken verpflichtet. Dies inkludiert Sicherheitslücken, über die internationale Bündnispartner Kenntnis erlangen und diese Kenntnis mit deutschen Behörden teilen.

Systeme, die Sicherheitslücken enthalten, stellen ein signifikantes Sicherheitsrisiko für Deutschland dar. Von einem einmal kompromittierten System können Angreifer sich oft undetektiert horizontal in weitere Systeme verbreiten. Eine aktive Cyberabwehr muss fest auf rechtsstaatlichen Grundsätzen stehen. Die deutsche Bundeswehr ist als reine Verteidigungsarmee konzipiert und grundgesetzlich in ihrem Auftrag dahingehend eingeschränkt, dass sie keine offensiven Kriegshandlungen durchführen darf. Dennoch wendet sie Werkzeuge (im Sinne von Waffensystemen) an, die auch offensiv eingesetzt werden könnten. In Anlehnung hieran müssen auch offensive Maßnahmen der Cyberabwehr einfachgesetzlich oder sogar grundgesetzlich unterbunden werden, auch wenn die verwendeten Werkzeuge eine offensive Anwendung ermöglichen würden.

Zusätzlich ist die Ausweitung einer effektiven parlamentarischen Kontrolle der Nachrichtendienste anzumahnen. Denn sowohl der BND, als auch der Verfassungsschutz sollen - wenn es nach dem BMI geht - im Rahmen einer “aktiven Cyberabwehr” neue Befugnisse erlangen. Insbesondere in einem diffusen Cyber- und Informationsraum, der von politischen Konflikten geprägt ist, wird die Grauzone (unter der Schwelle eines bewaffneten Konfliktes), in welcher Nachrichtendienste operieren können, problematisch und ist daher zwingend mit Aufsichtsmaßnahmen zu belegen. Es ist wissenschaftlich längst belegt, dass Staaten und respektive ihre Sicherheitsbehörden versuchen Kompetenzen aufzubauen und gleichzeitig die (demokratische) Kontrolle gering halten, damit suggestive Handlungsspielräume gewahrt bleiben. Komplementär dazu darf bezweifelt werden, dass das sog. Attributionsproblem im Rahmen einer “aktiven Cyberabwehr” lösbar ist. Die Zurechnung eines Cyberangriffs auf den tatsächlichen Täter ist bestenfalls schwierig bis unmöglich. Bei dem Einsatz einer aktiven Maßnahme der Cyberabwehr, welche offensive Mittel einschließt, können Kollateralschäden nicht ausgeschlossen werden und sind deshalb abzulehnen.

Frage 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 umgesetzt werden, wo besteht aus Ihrer Sicht darüber hinausgehender Handlungsbedarf und wo bestehen insbesondere Defizite?*

Keine der gelisteten Punkte dürfen weiter verzögert werden, manche der Punkte werden allerdings früher eine Wirkung entfalten als andere. Alle in der Frage genannten Punkte sind wichtig. Aus fachlicher Sicht ist keine Priorisierung erforderlich, da diese Themen parallel und weitgehend unabhängig von einander umgesetzt werden könnten.

Im Sinne einer echten Cybersicherheitsstrategie sind die ersten beiden Punkte zusammen anzugehen. Ein Recht auf Verschlüsselung kann seine schützenden Eigenschaften nur dann bewirken, wenn es eine Meldepflicht für Sicherheitslücken gibt. Auch die Vorgabe "security-by-

design/default" dient dem selben Thema - der Stärkung der IT-Sicherheit des Staats, der Bürger und der Wirtschaft.

Eine Verbesserung der Rechtssicherheit für IT-Sicherheitsforschende ist dringend notwendig. Viele Lücken in wichtigen Programmen, wie z.B. dem BeA oder der IDWallet, wurden nicht von staatlichen Stellen entdeckt, sondern von IT-Sicherheitsforschenden. Diese sehen sich dann jedoch immer wieder der Bedrohung durch zivil- oder strafrechtliche Verfahren ausgesetzt. Zwar können sie sich bisher an das BSI als Clearingstelle wenden, das die Hinweise der Entdecker aufnimmt und an die Hersteller weiterleitet. Dieser Workaround kann jedoch kein sinnvoller Ersatz für einen sicheren Rechtsrahmen für IT-Sicherheitsforschende sein. Denn nur dieser bietet ihnen eine stabile Grundlage für ihre Arbeit. Sie hängen dann auch nicht davon ab, ob sie dem BSI wirklich vertrauen können, obwohl es dem BMI untergeordnet ist, das auch andere Interessen, nämlich die der Strafverfolgungsbehörden, verfolgt. Eine digitale Gesellschaft muss ein Interesse an der schnellen Entdeckung und Schließung von Sicherheitslücken haben und dann folgerichtig auch den entsprechenden rechtlichen Rahmen für die dabei tätigen Akteure schaffen.

In diesem Sinne wäre es, neben den dringend notwendigen Maßnahmen zur Unabhängigkeit des BSI, auch wichtig, die Strafgesetzgebung zu Computerkriminalität, z.B. in §202ff StGB, anzupassen und die Strafbarkeit ähnlich wie den Betrug an den Vorsatz einen Schaden zu bewirken, zu knüpfen. Dies ist eine erste wichtige Maßnahme um Rechtssicherheit für IT-Sicherheitsforscher zu erreichen, der weitere folgen müssen. Auch zivilrechtliche Reformen, bspw. im UWG und im UrhG müssen hier folgen, um IT-Sicherheitsforschende vor zivilrechtlichen Schikanen zu schützen.

Darüber hinausgehend dürfte strukturell die Klärung vordringlich sein, wie der Ausgleich zwischen IT-Sicherheit einerseits und den widerstreitenden Interessen der Sicherheitsbehörden aufgelöst wird. Wenn seitens des BMI von Sicherheit durch Verschlüsselung und "Sicherheit trotz Verschlüsselung" geschrieben wird, lässt das erhebliche technische und fachliche Defizite erahnen. Dies insbesondere, wenn im Sinne von "Sicherheit trotz Verschlüsselung" an den Grundfesten sicher verschlüsselter Kommunikation gesägt wird und auch auf europäischer Ebene an Rechtsakten gearbeitet wird, die Anbietern von Diensten die Implementierung von Hintertüren für Sicherheitsbehörden vorschreiben sollen.

Der Satz "Sicherheit trotz Verschlüsselung" ist kontradiktorisch. Jeder staatliche Versuch, Verschlüsselung zu schwächen ist, auch im Sinne unserer digitalen Souveränität, abzulehnen. Stattdessen gilt es, Vorgaben wie security-by-design/default zu stärken und ein Mindesthaltbarkeitsdatum für Sicherheitsupdates elektronischer Endgeräte einzuführen.

Auch kann kein ernsthafter Ausgleich zwischen dem Computergrundrecht (Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme) und den Interessen der

Sicherheitsbehörden gelingen, wenn ein Schwachstellenmanagement und damit das Verfahren zum Zurückhalten von Schwachstellen praktiziert wird. Denn bewusst offen gehaltene Schwachstellen oder eine eingebaute Hintertür in der Verschlüsselung sind faktisch eine Entscheidung gegen die IT-Sicherheit und gegen das Computergrundrecht der Bürger. Dahingehend gilt die Priorisierung und Stärkung der Bürgerrechte als maßgeblich. Ein Recht auf Verschlüsselung und die Rechtsdurchsetzung der Interoperabilität und Portierbarkeit sind längst überfällig, hier besteht dringend Handlungsbedarf. Regelmäßig begründet das Bundesverfassungsgericht seine Urteile mit dem Recht auf Informationelle Selbstbestimmung bzw. Computergrundrecht. Ein Grundrecht, das im Zeitalter der Digitalisierung immer mehr an Bedeutung gewinnt und vom Gesetzgeber nicht angemessen berücksichtigt wird. Es legen sogar viele Gesetzesentwürfe den gegenteiligen Verdacht nahe, dass insbesondere die Informationelle Selbstbestimmung der Bürger bewusst missachtet wird. Entsprechend würde ein Recht auf Verschlüsselung Klarheit bringen und den Fokus der Sicherheitsbehörden auf Maßnahmen lenken, die gezielter und grundrechtschonender sind.

Handlungsbedarf besteht auch bei der längst überfälligen Überwachungsgesamtrechnung, die empirisch beleuchten soll, über welche Überwachungsbefugnisse die deutschen Sicherheitsbehörden bereits verfügen und, ob das immer wieder angeführte Argument des "Going Dark" tatsächlich besteht. Mit Hilfe dieser Überprüfung lassen sich sowohl Befugnislücken und -redundanzen feststellen, als auch das grundrechtliche Prinzip der Verhältnismäßigkeit nachhaltig bewahren.

Vor dem Hintergrund des jahrzehntealten Reformstaus und der pathologischen Verweigerung, auf das "Neuland" angemessen zu reagieren, hat Deutschland nicht mehr den Luxus, Prioritäten setzen zu können. Es muss in allen relevanten Themenfeldern schnellstmöglich gehandelt werden. Lange bürokratische Prozesse sind dabei ebenso pragmatisch zu vermeiden, wie Alleingänge von Ländern oder Ministerien. Ansonsten sind ähnliche Misserfolge wie bei der termingerechten Umsetzung des OZG zu erwarten.

Frage 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?*

Diese Forderungen kommen primär aus zwei Richtungen: Unternehmen, die solche Werkzeuge entwickeln oder verkaufen möchten, sowie aktuelle oder ehemalige Angehörige der

Sicherheitsbehörden, des BMVg oder der Bundeswehr, die fachlich im Bereich der Informations- und Kommunikationssysteme geringe Kompetenzen haben und die Funktionsweise dieser Technologien weder durchdrungen haben, noch ihre Grenzen beschreiben können.

Experten der Informationssicherheit, die sowohl Informations- und Kommunikationssysteme auf technischer Ebene verstehen, als auch die Konzepte und Prinzipien der IT-Sicherheit, raten seit Jahrzehnten vom Einsatz solcher Systeme ab.

In Bezug auf die Zweckmäßigkeit können wir inzwischen mehrere Operationen betrachten und bewerten - sowohl die äußerst komplexe Operation Stuxnet, als auch die Operation Industroyer sowie die Operation Triton zeigen deutlich, dass Kosten und Nutzen in keinem Verhältnis stehen. Bei der Operation Industroyer wurde unter großem personellen Aufwand über viele Monate oder sogar Jahre eine spezielle Schadsoftware entwickelt, die das ukrainische Stromnetz lahmlegen sollte. Der so erzielte Ausfall dauerte nur wenige Stunden und erreichte nicht das gewünschte Ziel des Angreifers.

Bei der Operation Stuxnet wurde über mehrere Jahre und unter Beteiligung vieler tausend Personentage von mindestens den Geheimdiensten dreier Nationen (USA, Israel und Niederlande) eine spezielle Schadsoftware entwickelt, die iranische Zentrifugen zur Anreicherung von Uran schädigte. Diese aufwändig entwickelte Schadsoftware verbreitete sich selbsttätig und infizierte viele andere Industriesteuerungsanlagen weltweit, die gar nicht angegriffen werden sollten - und verursachte entsprechende Schäden bei internationalen Verbündeten und Partnern. Die Anreicherung von Uran wurde für einige Monate verzögert, die enormen internationalen Kollateralschäden und Risiken für Ausfälle von weltweiten Anlagen, die eingegangen wurden, stellen allerdings die Sinnhaftigkeit der gesamten Operation in Frage.

In der Operation Triton wurde bereits 2017 versucht, durch eine Schadsoftware eine Safety Schutzabschaltung in einer Petrochemiefabrik außer Kraft zu setzen und den Austritt von einem Schwefelwasserstoffgas zu provozieren, so dass es durch Funkenschlag zu einer Explosion auf der Fabrikanlage kommen sollte. Dass hier Menschen konkret geschädigt oder gar mit Todesfolge angegriffen werden sollten zeigt, welches Ausmaß offensive Angriffe inzwischen einnehmen können, wenn staatliche Akteure entsprechende Kompetenzen aufbauen und parlamentarisch nicht ausreichend demokratisch gesteuert werden, sowie wenn Sicherheitslücken nicht kontinuierlich behoben und die Sicherheitspatches eingespielt werden.

Ein weites Beispiel stellt der WannaCry Vorfall dar. Dabei wurde eine gravierende Schwachstelle von staatlichen Stellen jahrelang zurückgehalten, um darauf basierend eigene offensive Cyberangriffe zu entwickeln. Bei einem Einbruch in die betreffende US-Behörde wurde nicht nur die Schwachstelle den Angreifern bekannt sondern auch die als EternalBlue bezeichnete Angriffs-

Software entwendet. Diese wurde daraufhin für weltweite massive Angriffe missbraucht, die Milliardenschäden verursachten und zu Ausfällen Kritischer Infrastruktur führten.

Wir lehnen den Einsatz offensiver Instrumente im Cyberraum daher ab und empfehlen der Politik dringend, diesen Grundsatz zu übernehmen.

Frage 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?*

Cybersicherheitspolitik ist ein Instrument der staatlichen Sicherheitspolitik. Anders als in anderen Nationen, formuliert die deutsche Politik ihre Interessen im Bereich der Außen- und Sicherheitspolitik hingegen nicht ausreichend oder klar, und verfolgt ihre Ziele ebenso nicht stringent. Das Weißbuch der Bundeswehr kann nicht als gesamtstaatliche Sicherheitsdoktrin gelten. Eine klare gesamtstaatliche Sicherheitsstrategie der Bundesrepublik existiert seit jeher nicht und wird gerade erst auf dem strategischen Konzept der NATO und dem strategischen Kompass der EU aufbauend langwierig erarbeitet. Gerade in Zeiten zunehmend aufkommender Konflikte und der weiteren Verlagerung politischer Auseinandersetzungen in den Cyberraum, bedarf es einer gesamtstaatlichen Sicherheitsstrategie, die zwischen den Ressorts des Bundes und allen Ländern abgestimmt ist, und so Sicherheitspolitik im Inneren und Äußeren langfristig strategisch ausrichtet.

Eine staatliche Governance in der Cybersicherheit ordnet sich letztlich diesen strategischen Zielen unter. Auch der Aufbau und die Anwendung konkreter Instrumente und Kapazitäten in der Cybersicherheit müssen diesen strategischen Zielen folgen und somit abgestimmt zwischen den Akteuren des Bundes und der Länder aufgebaut werden. Damit einher geht vor allem das Ziel, die Anzahl parallel existierender Strukturen zu reduzieren - ein Blick in das “Wimmelbild der Verantwortungsdiffusion” der Cybersicherheitsarchitektur der SNV (https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur) zeigt, dass der derzeitige Aufbau an Kompetenzen in Form von Behörden und Zuständigkeiten unübersichtlich und mit begrenzter Wirkmöglichkeit zu erfolgen scheint. Hier wäre eine Fokussierung und Konsolidierung der beteiligten Behörden, Gremien und Rollen in den Ländern ein sinnvoller erster Schritt.

Uns liegen bisher zu wenige erfolgversprechende Ansätze aus anderen Ländern vor, um dazu eine Empfehlung abzugeben.

Frage 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“)?

Wenn das einzige Ziel ist, Schwachstellen zu schließen, so kann dies nur gelingen, wenn die meldenden Personen, also Forschung und Fachkräfte der IT-Sicherheit, unbedingtes Vertrauen haben, dass die Stellen, die die Meldung empfangen, diese Meldungen ausschließlich für das Schließen der Sicherheitslücken verwenden. Dies kann nur sichergestellt werden, indem die Verflechtungen der Aufsicht über die Sicherheitsbehörden und das BSI im BMI entflochten werden und das BSI an Unabhängigkeit gewinnt. Sicherheitsbehörden haben ein entgegenlaufendes Interesse und möchten Sicherheitslücken tendenziell eher geheim halten, um diese im Bereich der Kriminalitätsbekämpfung zu verwenden.

Sicherheitsforscher werden eine Meldung nur dann durchführen, wenn sie sich absolut sicher sein können, dass diese Meldung zur unverzüglichen Schließung der Sicherheitslücke führt. Besteht diese Sicherheit nicht, werden gefundene Sicherheitslücken nur zu einem deutlich geringerem Maße gemeldet werden.

Damit eine gesetzliche Meldepflicht für Sicherheitslücken Wirksamkeit entfalten kann, muss diese für alle, also auch die öffentliche Verwaltung, Sicherheitsbehörden, Nachrichtendienste und andere staatliche Akteure gelten. Jegliche Sicherheitslücke, von der Kenntnis erlangt wird, muss unverzüglich gemeldet werden.

Würde eine solche Gesetzgebung erlassen, ist davon auszugehen, dass die Nachrichtendienste und Sicherheitsbehörden die Dienstleistungen der Infektion eines Computersystems mit Schadsoftware extern einkaufen, ohne Kenntnis von den genau verwendeten Sicherheitslücken zu erlangen. Solche Angebote existieren bereits heute im Markt, z.B. bietet das in die Kritik geratene israelische Unternehmen NSO solche Services an. Da ein solches Vorgehen konträr zur Meldepflicht von Sicherheitslücken ist, muss dieses ebenso gesetzlich unterbunden werden.

Frage 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?

Der derzeitige Prozess der Gesetzgebung für das KRITIS-Dachgesetz ist zu weiten Teilen nicht zufriedenstellend: Die durch die Bundesregierung veröffentlichten Eckpunkte sind in der inhaltlichen Tiefe wenig aussagefähig und lassen dem wesentlichen Kern der Absicht des Gesetzgebers noch sehr viel Spielraum. Bis zum jetzigen Zeitpunkt ist die Befassung des KRITIS-Dachgesetzes ohne sichtbare Einbindung öffentlicher Expertise aus Wissenschaft oder Zivilgesellschaft erfolgt. Ein Entwurf des KRITIS-Dachgesetzes liegt noch nicht vor. Damit kann zum jetzigen Zeitpunkt auch nur unzureichend bewertet werden, wie sich das KRITIS-Dachgesetz in die bestehende Gesetzgebung aus IT-Sicherheitsgesetzen, BSI-Gesetz und Kritisverordnung einordnen soll.

Durch das Beschließen dieses recht wenig aussagenden Eckpunktepapiers hat die Bundesregierung bewirkt, dass nur noch über die Ausgestaltung dieser Eckpunkte diskutiert wird. Dies ist aus unserer Sicht nicht genügend. Um die Versorgungssicherheit der Bevölkerung nachhaltig zu steigern und die IT-Sicherheit in den Kritischen Infrastrukturen zu erhöhen, sind weitere Maßnahmen erforderlich als aktuell in den Eckpunkten festgelegt.

Sowohl der europäische Rahmen als auch die Erfahrung in den Ländern mit der vorhandenen KRITIS-Gesetzgebung legen nahe, ein KRITIS Dachgesetz ganzheitlich zu denken und weitere Maßnahmen zu ergreifen, als das Eckpunktepapier benennt.

Diese weiteren Maßnahmen sind mindestens:

- Umsetzung der Maßnahmen, die im Rahmen der überhasteten Schaffung des IT-SiG2.0 nicht mehr berücksichtigt wurden;

- Umsetzung der europäischen Vorgaben aus der NIS2 Richtlinie und der „Resilience of critical entities“ Richtlinie, damit diese fristgemäß und vor Ende der Legislatur umgesetzt werden können;

• Auflösung der bestehenden Regelungslücken für die Sektoren Staat und Verwaltung sowie Medien und Kultur, für die Stand heute kein Bundesland bisher eine KritisVO erlassen hat;

• wissenschaftliche Betrachtung und Analyse von Kaskadeneffekten, deren Ergebnis eine Anpassung der Sektoren, Schwellwerte, Anlagen- und Anlagenkategorien auf Basis der tatsächlich erbringbaren Ersatzversorgungsleistung ist;

• einheitliche und verbindliche Meldewege für alle Vorkommnisse (physisch und digital).

Kritiker mögen an dieser Liste zu Recht bemängeln, dass diese für ein Dachgesetz zu spezifisch ist. Der AG KRITIS wurde mündlich und glaubwürdig aus Kreisen des BMI versichert, dass die Planungen für gesetzliche Änderungen im Rahmen eines anstehenden IT-SiG 3.0 in das KRITIS-Dachgesetz integriert werden sollen, aber kein eigenes IT-SiG 3.0 geschaffen werden soll. Daraus folgt, dass die Debatte um regulatorische Änderungen und Erweiterungen, wie sie für ein IT-SiG 3.0 geführt werden müsste, zumindest vorerst zusammen mit der Debatte für das KRITIS-Dachgesetz geführt werden muss.

Das Aufkommen der politischen Diskussion des physischen Schutzes Kritischer Infrastrukturen korreliert zeitlich mit den Vorkommnissen rund um das Bahnfunksystem GSM-R und den Anschlägen auf die Pipeline Nord Stream 2. Der Wunsch, Kritische Infrastruktur physisch besser zu schützen, ist bei Netzen aller Art (Glasfaser, Pipelines, Strom usw. usf…) naiv. In der Fläche des Landes und der Ausdehnung an diversen Trassen, lassen sich solche Infrastrukturen nicht effektiv schützen - daraus folgt, dass diese Infrastrukturen so gebaut sein müssen, dass eine Störung oder ein Sabotageakt zwar erfolgreich sein kann, dann jedoch keine langanhaltenden oder großflächigen Störungen hervorruft.

Um in einem solchen Fall der Bewältigung erfolgreicher Sabotageakte adäquat zu unterstützen, bedarf es eines gut ausgeprägten Notfall- und Krisenmanagements bei allen Betreibern von Kritischen Infrastrukturen. Ziel muss es sein, binnen weniger Stunden aufgrund von Beschädigungen an Trassen auftretende Ausfälle beheben oder kompensieren zu können. Bei Systemen, Kraftwerken und anderen relevanten Kritischen Infrastrukturen ist darüber hinaus auch die Geschwindigkeit des Wiederanlaufens deutlich zu verbessern. Hierfür sind verbindliche Regularien durch das KRITIS-Dachgesetz zu schaffen.

Ein Regelungszweck des KRITIS-Dachgesetzes soll die klare Identifizierung von Kritischen Infrastrukturen sein. Hierfür ist der Vorschlag der AG KRITIS, sich von der bisherigen Systematik der Schwellwerte zu verabschieden: aus Sicht der Bevölkerung entscheidend ist, dass eine Versorgung mit den relevanten Gütern (Wasser, Strom, Heizung, Treibstoffe, Daten & Informationen, usw., vgl. auch BSIG Sektorenliste) stattfinden kann. Dabei ist unerheblich, wie viele andere Menschen durch

die gleiche physische Infrastruktur noch versorgt werden. Insbesondere für die Bereitstellung von leitungs- oder netzgebundenen Diensten (siehe weiter oben hier im Abschnitt) können also grundsätzlich keine Schwellwerte gelten, wenn diese eine monopolistische Stellung bspw. durch Betrieb der Netzinfrastruktur genießen.

Vor diesem Hintergrund muss dann bewertet und entschieden werden, ob bei Ausfall der Infrastruktur in einer Krise eine Ersatzversorgung sicher erbracht werden kann. Ist dies nicht möglich, muss die betrachtete Komponente oder Anlage als KRITIS gelten.

Auch für den Sektor Staat und Verwaltung kann die Frage der Anzahl der Menschen, die einen Dienst oder eine Dienstleistung in einer Verwaltungseinheit (Kommune, Land, Bund) nutzen nicht dafür entscheidend sein, ob dieser Dienst als kritische Infrastruktur zu gelten hat. Von wesentlich höherer Bedeutung ist die Fragestellung, ob die Aufrechterhaltung dieses Dienstes für den Erhalt der menschlichen Gesundheit und für den Schutz menschlichen Lebens kurz- und mittelfristig Relevanz hat. So ist die Auszahlung von Sozialleistungen oder der Betrieb von gesundheitlichen Diensten von höherer Relevanz, als beispielsweise die Anmeldung eines Kraftfahrzeuges.

Frage 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?*

Entscheidend ist nicht das verwendete Netzwerkprotokoll, sondern die Einrichtung des Routings: das TCP/IP ist eine Familie von Netzwerkprotokollen, welche auf der Entwicklung des DARPA-Net beruhen. Genau dieses ist dazu entwickelt worden, um einen Informationsaustausch zwischen mehreren Knoten auch bei Wegfall einzelner Verbindungen weiterhin aufrecht zu erhalten. Die Vermittlung von Paketen (“Daten”) erfolgt nicht mehr von Punkt zu Punkt, sondern über Gateways (“Router”) in einem Netzwerk.

Über bestehende Kontakte aus der AK KRITIS heraus haben wir von Beschäftigten der Deutschen Bahn erfahren, dass Evaluierungen und Ansätze zur Neukonzeption der Netzwerktopologie des GSM-R Systems sowohl vor, als auch nach den mutmaßlichen Sabotageakten intern durchgeführt wurden. Bei Fragen zu Details wenden Sie sich bitte an die DB Netze AG.

Spekulativ lässt sich hier vermuten, dass das Risiko eines Ausfalls der in Betrieb befindlichen Topologie durch den Netzbetreiber schlichtweg als betriebliches Risiko akzeptiert wurde.

Frage 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 nach dem Ausschluss einzelner Hersteller erübrigt sich, wenn ein definiertes Mindestsicherheitsniveau für alle Hersteller existiert. An einer öffentlichen Ausschreibung könnte dann nur teilgenommen werden, sofern der Hersteller dieses Mindestmaß an Sicherheit durch technische, operative und organisatorische Maßnahmen nachweislich erfüllt. Dieses Mindestsicherheitsniveau muss auch durch Reseller und Integratoren garantiert werden können.

Die NIS2 Direktive beinhaltet bereits eine Regelung, die auf Mindestanforderungen beruht.

Wir empfehlen daher die Streichung der Regelung, nach der einzelne Hersteller ausgeschlossen werden können und empfehlen stattdessen die Schaffung verbindlicher Mindestsicherheitsniveaus für alle Hersteller.

Gleichzeitig müssen technologische und digitale Souveränität politisch gewollt sein. Eine Verschärfung des Rechtsrahmens muss daher immer in Abwägung zu diesen beiden Punkten erfolgen.

Frage 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 Ausbildung derzeitiger Fachkräfte in der IT und IT-Sicherheit wurde jahrzehntelang verschlafen. Es bedarf hier Anpassungen im Bereich des Bildungssystems, sowohl in der schulischen Ausbildung als auch in der Berufsausbildung. Zusätzlich können Erleichterung bei der Zuwanderungspolitik

dafür sorgen, dass wir schnell und unbürokratisch Fachkräfte für IT und IT-Sicherheit aus dem Ausland nach Deutschland holen könnten.

Auch muss nachhaltig und sofort in das Basiswissen in Sachen IT und IT-Sicherheit vorallem bei Beschäftigten in Behörden des Bundes und der Länder investiert werden. Dies erfordert zunächst die Erkenntnis der Notwendigkeit, als auch die Bereitstellung von zeitlichen und finanziellen Ressourcen, um dies zu ermöglichen. Dies kann z.B. durch verpflichtende Weiterbildungen erfolgen.

Zusätzlich bedarf es der Erhöhung der Retention der entsprechend Fachkräfte. Weder die Arbeitsbedingungen, noch die Gehälter im öffentlichen Dienst sind derzeit angemessen, um entsprechende Fachkraft anzuziehen und langfristig zu binden.

Eine grundlegende Änderung der TVöD/TV-L sowie des BBesG o.ä. ist hier aus unserer Sicht notwendig, um Fachkräfte marktüblich bezahlen zu können. Auch müssen Eintrittsbarrieren abgebaut und Beschäftigungsmöglichkeiten nicht von einer formal vorhandenen, aber jahrzehntealten Qualifikation abhängig gemacht werden, sondern von tatsächlichen Kenntnissen und Fähigkeiten der sich bewerbenden Fachkräfte. Insbesondere im Höheren Dienst sollte neben Führungskräften ein Aufstieg auch für Fachkräfte in einer Expertenlaufbahn ermöglicht werden.

Durch bestehende Rahmenbedingungen, wie z.B. Haushaltsregeln, enge IT-Budgets und komplexeste Ausschreibungen für Beschaffung notwendiger Infrastrukturkomponenten, ist die Arbeit im Bereich IT in der öffentlichen Verwaltung strukturbedingt frustrierend. Eine technisch so unflexible Arbeitsumgebung, die gleichzeitig oft veraltet ist, sorgt für Desinteresse der besonders kompetenten Fachkräfte, die durch ihr Schaffen Dinge tatsächlich bewegen wollen.

Es entspricht der subjektiven Wahrnehmung der Mitglieder der AG KRITIS, dass sie, wenn sie ihre Fähigkeiten in der öffentlichen Verwaltung erbringen würden, auf 20-50% ihrer aktuellen privatwirtschaftlichen Vergütung verzichten müssten. Wir empfehlen, die tatsächlichen Unterschiede in der Vergütung von IT-Fachkräften zwischen der freien Wirtschaft und der öffentlichen Verwaltung wissenschaftlich zu analysieren und dies zur Grundlage der empfohlenen Reform von TVöD und BBesG zu machen.

Dabei gilt es zu beachten, dass hoch kompetente IT-Fachkräfte durch Remote-Arbeit auch international tätig sein können, und dabei trotzdem in Deutschland wohnen können. Der deutsche Staat konkurriert um IT-Fachkräfte eben nicht mehr im Umkreis von 30 km um einen Behördenstandort, sondern direkt auch mit ausländischen Unternehmen, deren Gehaltsniveaus oft einem Vielfachen der in der deutschen IT-Wirtschaft üblichen Gehälter entsprechen.

Frage 12

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

Der allgemeine IT-Fachkräftemangel stellt etwa zwei Drittel der Unternehmen vor erhebliche Schwierigkeiten, entsprechende Stellen zu besetzen (Statista 2020). So blieben zuletzt ca. 137.000 Stellen für IT-Fachkräfte unbesetzt (Bitcom Research, 2022).

Der Markt für IT-Cyberfachkräfte ist tendenziell noch deutlich angespannter. Es fehlt an Personen mit technischem Fachwissen, ebenso wie an Fachkräften für organisatorische Themen, wie Security-Governance und Business Continuity Management.

Gleichzeitig ist Informationssicherheit bei weitem kein reines Thema für Informatiker sondern ein Querschnittsthema. IT Kompetenz und Sensibilisierung für Cybersicherheit wird als Querschnittskompetenz in der Breite, und nicht nur von ein paar Fachkräften benötigt, denn Digitalisierung betrifft alle Menschen und Bereiche. Daher müssen in die schulischen Lehrpläne sowie in die Berufsausbildungen und Studiengänge aller Berufe und Abschlüsse grundlegendes Informatikwissen, Medienkompetenz, Programmierkenntnisse, IT-Sicherheitsfachkenntnisse sowie Algorithmen und Datenstrukturen aufgenommen werden.

Dazu braucht es ein einheitliches und hohes technisches Ausrüstungsniveau aller Schulen, Berufsbildungsstätten und Hochschulen im Bundesgebiet sowie ein einheitliches und hohes Wissensniveau in einem flächendeckend einzuführenden Pflichtfach Informatik. Diese Vereinheitlichung ist notwendig, um schnellstmöglich ausreichend Lehrpersonal aus- und fortzubilden sowie ausreichende Skalierbarkeit von IT-Lernkonzepten und Lösungen erreichen zu können. Die Grundlage für den Erfolg dieses Vorhabens wäre eine ausreichende Internetanbindung für alle Schulen und technisches Fachpersonal für Netzwerke und Computersystemen in Bildungseinrichtungen, selbst diese ist bisher nicht gelegt.

Eine systematische und einheitliche Bildungsoffensive ist notwendige Grundlage, um qualitativ und quantitativ ausreichenden Nachwuchs in den Ausbildungsbetrieben und Hochschulen zu erreichen.

Die weitere Ausbildung von Cyberfachkräften muss an Hochschulen sogar breiter aufgestellt sein, als es das heutige Studienfach Informatik ist. Die Ausbildung muss systematisch und interdisziplinär auch angrenzende Fachgebiete einschließen. Für Quantentechnologien braucht es zum Beispiel ein Zusammenspiel aus den Bereichen Informatik, Mathematik und Physik. Möchte man langfristig die Cybersicherheit von kritischen Infrastrukturen verbessern, so müssen IT-Cyberfachkräfte auch in den Fakultäten für Maschinenwesen und Mechatronik mit spezifischen Domänenwissen

ausgebildet werden. Für organisatorische Abläufe und Absicherungen sind auch Sozial- und Verhaltenswissenschaften einzubeziehen.

Die Cybersicherheitsstrategie geht mit dem Digitalführerschein für Anwenderinnen und Anwender nicht weit genug. Technische Fachkompetenzen müssen während der gesamten Bildungsbiografie, vom Kindergarten über die Hochschulen bis zur berufsbegleitenden Weiterbildung vermittelt werden. Dazu muss ein strategischer Rahmen entwickelt werden, der die Bürger bundesweit einheitlich befähigt, sowohl beruflich als auch privat im digitalen Raum sicher zu handeln.

Frage 13

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

Für die Abwehr von Angriffen auf die Systeme insbesondere der deutschen Verwaltung, wie zuletzt in Potsdam oder auch aus dem Landkreis Anhalt-Bitterfeld bekannt, bedarf es insbesondere der stringenten Umsetzung von security-by-design und privacy-by-design als Architekturprinzipien der Systeme. Weiterhin können derartige Angriffe, bspw. durch Ransomware, in der breiten Masse nicht durch eine aktive Komponente der “Cyberabwehr” abgewehrt werden. Wesentlicher ist es daher, den Abfluss von Daten zu verhindern, ein effizientes Notfallmanagement zu etablieren und Wiederherstellungsprozesse zu beschleunigen. Wenn dies erreicht wurde, so kann ein Angriff zwar erfolgreich sein, wird aber den Betrieb und damit die Versorgung der Bevölkerung entweder nicht, oder nur für kürzeste Zeiträume stören.

Maßnahmen der Cyberabwehr lassen sich in offensive und defensive Maßnahmen kategorisieren. Sofern unter dem Begriff der “aktiven Cyberabwehr” folglich offensive Maßnahmen gefasst werden, lehnen wir diese grundsätzlich ab. Defensive Maßnahmen, wie in der Antwort zu Frage 3 ausgeführt, sollten trotzdem und äußerst aktiv angegangen werden.

Der Wunsch nach offensiver Cyberabwehr leitet sich aus einem Täterdenken ab. Dieses Täterdenken impliziert, dass sobald der Täter feststeht, aktiv Maßnahmen unternommen werden könnten, um die Aktivitäten dieses Täters zu unterbinden. Selbst wenn es zuverlässig gelingen könnte, bei Cyberangriffen konkrete Täter zu bestimmen, würde dies nicht das Problem der Angreifbarkeit des jeweiligen Systems lösen. Bleiben bestehende Sicherheitslücken offen oder weisen fachliche Abläufe Anfälligkeiten auf, so könnten diese durch beliebige andere Angreifer ausgenutzt werden.

Um IT-Sicherheit effektiv und effizient auszugestalten, gilt es, die Systeme zu härten, also resilient gegen Angriffe zu machen, und zudem überall wo möglich Redundanzen aufzubauen. Das oberste Ziel, insbesondere staatlicher Infrastruktur, muss es sein, die Angreifbarkeit zu minimieren, sowie

Wahrscheinlichkeit und Folgen eines Ausfalls maßgeblich zu reduzieren, sodass keine Gefährdung für Staat und Bevölkerung entsteht.

Frage 14

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

Die Abhängigkeit der öffentlichen Verwaltungen in Deutschland von privaten Unternehmen ist im Bereich der Cybersicherheit grundsätzlich zu groß. Bereits die Kompetenzen und Kapazitäten zur Digitalisierung der öffentlichen Verwaltungen sind in der öffentlichen Hand unzureichend. Noch dramatischer trifft dies auf den Bereich der Cybersicherheit zu. Aus diesem Mangel heraus beauftragen Behörden aus Kostenstellen für Sachkosten heraus externe Dienstleister, um langanhaltend Personalmängel und fehlendes Fachwissen zu überbrücken. Sinnvoller wäre es aus unserer Sicht, langfristig Ausbildung und Arbeitsbedingungen für Cybersicherheit in der öffentlichen Hand grundlegend zu verbessern. Nur so kann sichergestellt werden, dass durch die öffentliche Hand ausgebildetes Personal auch langfristig gebunden bleibt.

Hiervon sind Bund und Länder, als auch Kommunen und Landkreise gleichermaßen betroffen.

Die fehlenden Kompetenzen und Kapazitäten der öffentlichen Hand werden verstärkt durch die daraus resultierenden Abhängigkeiten von externen Dienstleistern und Produzenten aus dem Ausland. So kann eine “digitale Souveränität” insbesondere im Bereich von Produkten aus der Cybersicherheit nicht erreicht werden, wenn seitens des deutschen Staates eigene Fachkompetenz fehlt. Die Nutzung ausländischer Produkte und Dienstleistungen sollte daher immer kritisch geprüft werden.

Relevante Anbieter im Bereich Cybersicherheit aus dem Ausland können nicht nur wirtschaftliche Eigeninteressen verfolgen, sondern auch politisch aus den Staaten ihres Unternehmenssitzes heraus gesteuert werden. Dies trifft auf verbündete Staaten gleichermaßen zu, wie auf wirtschaftlich oder politisch konkurrierende Nationen.

Beispielsweise ist das US-Unternehmen FireEye in den USA eine Ausgründung des US-Nachrichtendienstes CIA und kann daher nicht als politisch neutrales Unternehmen gelten. Ebenso ist die Cybersicherheitsindustrie in Israel maßgeblich geprägt von den Nachrichtendiensten und deren politischen Anforderungen an die nationalen Sicherheit. Auch der russische Staat nimmt üblicherweise großen Einfluss auf die Unternehmen im eigenen Land - und auch hier finden sich mehrere Unternehmen, die im Bereich der Cybersicherheit aktiv sind und ihre Dienstleistungen auch in westlichen Nationen anbieten.

Internationale Unternehmen sind im Bereich Cybersicherheit damit grundsätzlich zurückhaltend zu nutzen. Auch aus verbündeten Nationen oder solchen mit gemeinsamen Interessen sind in der Vergangenheit Fälle von Wirtschaftsspionage aufgetreten. Zudem sind Interessen im geopolitischen Raum nicht dauerhaft stabil. Partner und Verbündete von heute können in konkreten Konflikten von morgen abweichende oder eigene Interessen verfolgen.

Um also die nationale Resilienz zu erhöhen, sollte sich eine “Zeitenwende” nicht nur auf militärische Fähigkeiten beschränken, sondern auch und insbesondere den Schutz der Kritischen Infrastrukturen und der Cybersicherheit Deutschlands im Blick haben. Der Aufbau entsprechender Kompetenzen dient also letztlich auch der Steigerung und dem Erhalt der Souveränität des Staates.

Frage 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?*

Aus Sicht der Bürgerrechte und vor dem Hintergrund, dass die Integrität und Vertraulichkeit der persönlichen Computersysteme ein abgeleitetes Grundrecht ist, war diese Debatte vom ersten Tag an aus unserer Sicht hinfällig.

Spezifische IT-Schnittstellen für Sicherheitsbehörden sind Sicherheitslücken, denn diese wurden und werden eben nicht nur durch Sicherheitsbehörden genutzt, sondern können auch durch Kriminelle ausgenutzt werden. Seit den 1990er Jahren sind solche Sicherheitslücken in den Mobilfunksystemen, die explizit für und durch Sicherheitsbehörden geschaffen wurden, der Öffentlichkeit bekannt und werden aktiv ausgenutzt. Es besteht kein Grund zur Annahme, dass die geplanten Sicherheitslücken für Sicherheitsbehörden im 6G-Standard nicht auch binnen kurzer Zeit öffentlich bekannt werden und ebenfalls durch Kriminelle ausgenutzt werden.

Eine Schwachstelle, die für einen “befreundeten” Nachrichtendienst eingebaut worden ist, kann durch einen feindlichen Nachrichtendienst oder andere kriminelle Akteure gefunden und ausgenutzt werden.

Aus gesamtgesellschaftlicher sowie technischer Sicht gibt es keinen Grund, Software-Schwachstellen nicht unverzüglich zu schließen, um die Integrität und Vertraulichkeit der IT-Systeme für die Bevölkerung, der Wirtschaft und des Staates zu sichern.

Eine zur Verfügung stehende, grundrechtsschonende Maßnahme, welche Strafermittlungen ermöglicht, ohne Kollateralschäden zu verursachen, ist die richterliche Beschlagnahmung der Computersysteme und forensische Untersuchung selbiger.

Bezüglich des Frageteils nach Quantenkommunikation ist zunächst festzuhalten, dass auch nach Etablierung von Quantenkommunikation und Quantenkryptographie grundlegende Sicherheitseigenschaften von IT-Systemen bestehen bleiben werden, da die Quanten-Systeme in klassische IT-System eingebettet werden. Die bestehende Diskussion um IT-Sicherheit bleibt entsprechend vollumfänglich erhalten.

Die Sicherheit von Verfahren, die der Quantenverschlüsselung zuzurechnen sind, basiert im Gegensatz zu klassischen Verschlüsselungsverfahren nicht auf mathematischen Verfahren, sondern auf den physikalischen Eigenschaften der Informationsträger, sogenannter Qubits, bspw. Photonen. Diese sind im Informationstheoretischen Sinne Read-only-once-memory. Aufgrund dieser Eigenschaft und des No-Cloning Theorems - es ist nicht möglich Qubits vollständig zu kopieren - ist keine klassische Zwischenspeicherung von Quantenkommunikation möglich. Entsprechend ist asynchrone Kommunikation sowie die Umsetzung eines Analogon von klassischen Signaturen nicht möglich. Der Anwendungsbereich ist entsprechend stark eingeschränkt. Das Versenden einer “Quanten-E-Mail” ist nicht möglich.

Die Einbindung in klassische IT-Systeme für das Persistieren von Informationen bleibt notwendig. Daraus folgt, dass die Schwachstellen-Situation und Notwendigkeit von IT-Sicherheit durch die Etablierung von Quantenkommunikation qualitativ nicht verändert wird.

Qubits sind physikalisch gesehen höchst instabile Systeme. Die Dauer, für die diese Systeme Informationen speichern können, die sog. Kohärenzzeit, liegt bei den meisten Systemen im Bereich von Sekunden, der Weltrekord im Labor bei 3 Stunden. Da die Sicherheit von Quantenkryptographie auf physikalischen Eigenschaften der Informationsträger beruht und nicht auf mathematischen Verfahren, ist es zwar nicht möglich diese mit Quantencomputern zu brechen, dennoch stellt sie aufgrund der Instabilität der Speicherung der Informationen keine Alternative zur klassischen Kryptographie dar.

Die Entwicklung von Quantencomputern stellt bereits jetzt ein Risiko im Bereich der Informationssicherheit dar. Nachgewiesener Weise sind Quantencomputer in der Lage, klassische Verschlüsselungsalgorithmen zu überwinden. Dies ist eine Herausforderung für schwer zugängliche Systeme mit langer Lebensdauer, die jetzt in Dienst gestellt werden, von Systemen für kritische

Infrastrukturen bis hin zu Satelliten. Es finden bereits heute so genannte record-now-decode-later Angriffe auf Informationen mit langfristigem Schutzbedarf statt.

Wissenschaftliche Forschung im Bereich neuer quantensicherer kryptographischer Verfahren sollte daher verstärkt werden. Im Rahmen eines security-by-design und privacy-by-design Ansatzes ist es bereits best-practice, die eingesetzten kryptographischen Verfahren modular und austauschbar zu gestalten. Wir empfehlen daher dem Staat eine stringente Umsetzung und Rechtsdurchsetzung von Prinzipien des security-by-design und privacy-by-design.

Frage 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?*

Das einziges Ziel eines Schwachstellen-“Management” kann nicht die Verwaltung von Schwachstellen, sondern ausschließlich die Behebung von Schwachstellen sein.

Das Wort “Schwachstellenmanagement” wurde in der Vergangenheit in Sicherheitskreisen so verwendet, dass ein zu diesem Zweck eingesetztes Gremium darüber entscheiden solle, ob eine Schwachstelle zurückgehalten oder gemeldet und folglich geschlossen wird. Um eine solche Abschätzung vornehmen zu können, müsste eine Bewertung des Risikos zum Umgang mit dieser Schwachstelle erfolgen. Für die Bewertung des Risikos müsste diesem Gremium bekannt sein, in welchen Anlagen und Systemen diese Sicherheitslücke vorkommt. Dafür bedürfte es einer Datenbank, welche die präzise Softwareversion einer jeden Softwarekomponente in jedem informationstechnischen System in Deutschland kennt. Eine solche Datenbank existiert nicht. Die hypothetische Schaffung ist aus vielfältigen Gründen unrealistisch. Gäbe es eine solche Datenbank, so würde diese präzise dokumentieren, welche Systeme für welche Sicherheitslücken anfällig sind. Damit wäre diese Datenbank ein so wertvolles Angriffsziel, dass die Sicherheit dieser hochsensiblen Informationen nicht garantiert werden kann.

Gleichzeitig müsste jedes informationstechnische System auch jede Änderung und jedes Update an diese hypothetische Datenbank übermitteln, was enorme technische Schwierigkeiten bereiten würde. Alleine schon die Schaffung der gesetzlichen Grundlage für eine solche Datenübermittlung würde an vielfältiger Stelle durch vorhandene Gesetzgebung im Bereich des Wettbewerbsrechts,

des Datenschutzes, des Unionsrecht, durch technische Vorschriften und durch Grundrechte unserer Bürgerinnen verhindert werden.

Aus der faktischen Unmöglichkeit, das Risiko einer Sicherheitslücke objektiv zu bewerten, resultiert, dass jede Sicherheitslücke im Zweifel katastrophale Auswirkungen haben kann. Eine Abwägung welche Schwachstellen geschlossen werden, welche offen und vermeintlich geheim gehalten werden, darf nicht passieren.

Darüber hinaus ist auch die Zurückhaltung von Sicherheitslücken objektiv betrachtet, gescheitert. Selbst der uns technisch und finanziell enorm überlegene transatlantische Bündnispartner USA hat es nicht geschafft, Sicherheitslücken in Microsoft Windows geheim zu halten. Durch den unzureichenden Schutz dieser verheimlichten Sicherheitslücken durch die US-Geheimdienste wurde mindestens die Angriffswelle mittels der Schadsoftware “WannaCry” überhaupt erst ermöglicht.

Wenn es aber nicht mit hundertprozentiger Sicherheit gelingen kann, Sicherheitslücken nicht nur zurück- sondern auch geheim zu halten, dann ist die einzige logische Konsequenz daraus, Sicherheitslücken eben nicht zurück zu halten.

Zudem bleiben die Sicherheitsbehörden, die Schwachstellen zurückhalten wollen, eine empirisch fundierte Erklärung schuldig. Wir fragen uns, wieso es Cyber-Kriminellen möglich ist, erfolgreich längst öffentlich bekannte und patchbare Schwachstellen auszunutzen, um Systeme zu infiltrieren, den Sicherheitsbehörden dies angeblich jedoch nicht gelingt. Es ist aus unserer Sicht akzeptabel, gemeldete und bekannte Sicherheitslücken rechtsstaatlich nach einem Richtervorbehalt einzusetzen, um eine Strafverfolgung zu gewährleisten. Dies gilt natürlich nur solange, wie das BSI so unabhängig aufgestellt ist (vgl. Antwort zu Frage 7), dass gesetzlich sichergestellt ist, dass Maßnahmen zur Behebung und Schließung der Sicherheitslücken ungehindert erfolgen.

Damit eine Sicherheitslücke geschlossen werden kann, muss diese zuerst gemeldet werden, daraufhin muss die betroffene Software verändert werden und die aktualisierte Fassung auf den betroffenen IT-Systemen installiert werden. Zwischen der Meldung einer Sicherheitslücke und der Schließung selbiger liegen bedauerlicherweise oft Jahre. In diesen Zeiträumen kann mit Richtervorbehalt und einem zu schaffenden, starken rechtsstaatlichen Rahmen die gemeldeten Sicherheitslücken im Bereich der Strafverfolgung verwendet werden.

Daher darf das einzige Ziel eines Schwachstellen-“Management” nicht die Verwaltung von Schwachstellen, sondern ausschließlich die Behebung von Schwachstellen sein. In der Praxis lässt sich beobachten, dass oft viel Aufwand in das Etablieren und Betreiben von Schwachstellen-Datenbanken, -Übersichten und -Berichten fliesst. Da solche Aktivitäten dem Risiko-Management

ähnlich sind und mit vergleichbaren Kompetenzen und Personal betrieben werden können, lassen sich hier vermeintlich Synergieeffekte finden.

Das Beheben von Schwachstellen erfordert ganz andere technische Kompetenzen und Personal, welches die betroffenen IT-Komponenten im Detail beherrscht. Der personelle und organisatorische Aufwand zum Beheben von Schwachstellen hängt somit wesentlich von der Komplexität und dem Alter der im Einsatz befindlichen Informationstechnik ab.

Gerade im Bereich der Kritischen Infrastruktur, in der Anlagen zum Teil seit Jahrzehnten im Einsatz sind, ist somit mit einem überproportional hohen Aufwand zum Beheben von Schachstellen zu rechnen. Ein gute technische Ausstattung kann diesen Aufwand etwas verringern aber nicht kompensieren.

Bekannt gewordene Schwachstellen müssen geschlossen werden. Dazu müssen diese dem Hersteller, aber auch den Betreibern gemeldet werden. Das Zurückhalten von Schwachstellen steigert das Risiko und die Angriffsfläche und ist folglich abzulehnen.

Frage 17

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

Es fehlt nach wie vor an grundlegenden Bildungsangeboten zu allgemeiner Medienkompetenz sowie digitaler Souveränität.

Vergleichbar zu Verkehrserziehung und Verkehrssicherheitstrainings und -maßnahmen, die eine Risiko-orientierte Handlungsweise im Straßenverkehr etablieren, bedarf es Bildungsmaßnahmen, die ein Bewusstsein für digitale Souveränität, IT-Sicherheit und IT im Allgemeinen in allen Bevölkerungsgruppen schaffen. Die bestehenden Digitalisierungsinitiativen müssen genutzt werden, um nicht nur Möglichkeiten, sondern auch Risiken der Digitalisierung zu verdeutlichen und grundlegende IT-Sicherheits-Handlungsweisen zu vermitteln. Zudem muss IT-Sicherheit integraler Bestandteil der schulischen Bildung werden, angefangen im Grundschulbereich. Eine bundesweite Einführung des Pflichtfach Informatik in weiterführenden Schulen ist dringend geboten.

Jedem Wunsch nach Vermittlung von Kompetenz und Ausbildung liegt aber auch die Tatsache zugrunde, dass ausreichend ausgebildetes Personal sowie eine aktuelle und ausreichende Ausstattung zur Verfügung stehen müssen, um genannte Ausbildungen zu ermöglichen. Diese

Ausstattung muss nicht nur zur Verfügung gestellt werden, sondern es müssen Stellen zur Administration geschaffen werden, damit diese Ausstattung langfristig gepflegt und gewartet werden kann.

Weiterhin müssen wir anerkennen, dass wie immer in Kulturfragen, Zeit und Vorbildfunktion eine Rolle spielen. Kultur, wie auch Sicherheitskultur wird nicht in einem Haushaltsjahr etabliert und bedarf nachhaltiges Vorleben. Der Staat muss seine Organisationskultur, Fehlerkultur und Kommunikationskultur intern wie auch den Bürgerinnen gegenüber grundlegend überdenken.

Frage 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*

IT-Sicherheit betrifft alle Menschen gleichermaßen, unabhängig von Staatsbürgerschaft, Alter oder anderer Eigenschaften. Dementsprechend ist das Thema grundsätzlich ganzheitlich zu denken, also auf allen staatlichen und gesellschaftlichen Ebenen. Insofern sind Maßnahmen nicht nur an IT-Fachkräfte und Endnutzer (“Verbraucher”) von IT zu adressieren, sondern aufgrund der umfassenden Digitalisierung letztlich an jeden Berufszweig.

Sicherheit ist kein Selbstzweck, sondern dient gezielt dem Schutz von Menschen und ihren Lebensumständen. Deshalb müssen entsprechende Technologien, Werkzeuge und Regularien auch Menschen-zentriert entworfen und eingesetzt werden (“Usable Security”). Gemeinhin erhöhen Sicherheitsmaßnahmen die kognitive Last einer Aufgabe und werden schnell als lästig empfunden und im Ergebnis über Bord geworfen, wenn etwas nicht funktioniert (vgl. Adams & Sasse, Whitten & Tygar). Deshalb ist es wichtig, konsequent die Best Practices sowie aktuelle Forschungsergebnisse aus dem Bereich der Usable Security zu befolgen.

Insbesondere Organisationen, die Security Tools für Kritische Infrastrukturen entwickeln, müssen dafür konsequent mit den betroffenen Fachkräften in engem Dialog stehen und ihre Entwicklung von den konkreten Bedürfnissen, Nutzungskontexten und -erfordernissen leiten lassen. So kann der “Faktor Mensch” als integrale Stärke der Informationssicherheit und nicht als “schwächstes Glied” agieren. Gerade Beinahe-Vorfälle im Bereich KRITIS, wie z.B. der Angriff auf eine Trinkwasseraufbereitungsanlage im US-Bundesstaat Florida in 2021 zeigen, dass oft nur die menschliche Aufsicht eine Katastrophe verhindern kann. Damit dies gelingt, muss die Technik den Menschen in die Hände spielen und sie nicht durch Überkomplexität oder umständliche Bedienung behindern.

Damit einhergehend sind die Themen Bildung und Schulung in Informationssicherheit ebenfalls von höchster Wichtigkeit, wie bereits in den Antworten der Fragen 12 und 17 zum Ausdruck gebracht. Bestehende Informations- und Bildungsmaßnahmen zielen vor allem auf die Vermittlung von derzeit sicheren Handlungsweisen ab (zum Beispiel beim Thema Passwortsicherheit), vernachlässigen allerdings die Vermittlung von Kompetenz und dem selbstständigen Beurteilen von IT-Sicherheitsaspekten. Dadurch wird eine reaktive Handlungsweise verstärkt, statt digitale Souveränität zu fördern. Die IT-Sicherheit würde davon profitieren, wenn gerade im Bereich Digitalisierung besonders “vorausschauend gefahren” würde.